



ICLG

The International Comparative Legal Guide to: **Fintech 2019**

3rd Edition

A practical cross-border insight into fintech law

Published by Global Legal Group, with contributions from:

A&L Goodbody
AEI Legal LLC
Anderson Mōri & Tomotsune
Anjarwalla & Khanna
Appleby
BAHR
Bär & Karrer
BBA
BonelliErede
Bonn Steichen & Partners
Bredin Prat
De Brauw Blackstone Westbroek
Democritos Aristidou LLC
ENSafrica
Erciyas Law Office
Evriss Law Firm
FINREG PARTNERS
Galicia Abogados, S.C.

Gilbert + Tobin
Glæss Lutz
Goldfarb Seligman & Co.
Gorriceta Africa Cauton & Saavedra
Gorrißen Federspiel
GVZH Advocates
Hajji & Associés
Hudson Gavin Martin
Kim & Chang
König Rebholz Zechberger Attorneys at Law
Lee and Li, Attorneys-at-Law
Links Law Offices
Lloreda Camacho & Co
Mannheimer Swartling
Mattos Filho, Veiga Filho, Marrey Jr e
Quiroga Advogados
McMillan LLP
PFR Attorneys-at-law

QUORUS GmbH
Schoenherr
Shearman & Sterling LLP
Shearn Delamore & Co.
Silk Legal Co., Ltd.
Slaughter and May
Stanford Law School
The Blockchain Boutique
Trape Konarski Podrecki & Partners
Triay & Triay
Trilegal
Udo Udoma & Belo-Osagie
Uría Menéndez
Uría Menéndez – Proença de Carvalho
Vodanovic Legal
Walalangi & Partners (in association
with Nishimura & Asahi)
Walkers Bermuda



Contributing Editors
Rob Sumroy and Ben Kingsley, Slaughter and May

Publisher
Rory Smith

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Senior Editors
Caroline Collingwood
Rachel Williams

Sub Editor
Amy Norton

Group Consulting Editor
Alan Falach

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Stephens & George
Print Group
May 2019

Copyright © 2019
Global Legal Group Ltd.
All rights reserved
No photocopying

ISBN 978-1-912509-70-6
ISSN 2399-9578

Strategic Partners



General Chapters:

1	Artificial Intelligence in Fintech – Rob Sumroy & Ben Kingsley, Slaughter and May	1
2	Cross-Border Financing of Fintech: A Comparison of Venture and Growth Fintech Financing Trends in Europe and the United States – Jonathan Cardenas, Stanford Law School	7

Country Question and Answer Chapters:

3	Australia	Gilbert + Tobin: Peter Reeves	14
4	Austria	PFR Attorneys-at-law: Bernd Fletzberger	21
5	Bermuda	Walkers Bermuda: Natalie Neto & Rachel Nightingale	26
6	Brazil	Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados: Larissa Lancha Alves de Oliveira Arruy & Fabio Ferreira Kujawski	31
7	Canada	McMillan LLP: Pat Forgione & Anthony Pallotta	37
8	Cayman Islands	Appleby: Peter Colegate & Anna-Lise Wisdom	44
9	China	Llinks Law Offices: David Pan & Xun Yang	49
10	Colombia	Lloreda Camacho & Co: Santiago Gutierrez & Juan Sebastián Peredo	55
11	Cyprus	Democritos Aristidou LLC: Christiana Aristidou	60
12	Czech Republic	FINREG PARTNERS: Ondřej Mikula & Jan Šovar	67
13	Denmark	Gorrissen Federspiel: Morten Nybom Bethe & Tue Goldschmieding	72
14	France	Bredin Prat: Bena Mara & Vincent Langenbach	78
15	Germany	Gleiss Lutz: Dr. Stefan Weidert & Dr. Martin Viciano Gofferje	85
16	Gibraltar	Triay & Triay: Javi Triay & Jay Gomez	91
17	Hong Kong	Slaughter and May: Benita Yu & Jason Webber	97
18	Iceland	BBA: Stefán Reykjálín & Baldvin Björn Haraldsson	105
19	India	Trilegal: Kosturi Ghosh & Adhunika Premkumar	112
20	Indonesia	Walalangi & Partners (in association with Nishimura & Asahi): Luky I. Walalangi & Hans Adiputra Kurniawan	119
21	Ireland	A&L Goodbody: Claire Morrissey & Peter Walker	124
22	Israel	Goldfarb Seligman & Co.: Ariel Rosenberg & Sharon Gazit	134
23	Italy	BonelliErede: Federico Vezzani & Tommaso Faelli	140
24	Japan	Anderson Mōri & Tomotsune: Ken Kawai & Kei Sasaki	146
25	Kenya	Anjarwalla & Khanna: Sonal Sejpal & Dominic Rebelo	152
26	Korea	Kim & Chang: Jung Min Lee & Samuel Yim	157
27	Liechtenstein	König Rebholz Zechberger Attorneys at Law: Dr. Helene Rebholz & MMag. Degenhard Angerer	164
28	Luxembourg	Bonn Steichen & Partners: Pierre-Alexandre Degehet	169
29	Malaysia	Shearn Delamore & Co.: Timothy Siaw & Christina Kow	174
30	Malta	GVZH Advocates: Dr. Andrew J. Zammit & Dr. Kurt Hyzler	181
31	Mexico	Galicia Abogados, S.C.: Claudio Kurc & Arturo Portilla	186
32	Morocco	Hajji & Associés: Nihma Elgachbour & Ayoub Berdai	192
33	Netherlands	De Brauw Blackstone Westbroek: Björn Schep & Willem Röell	197
34	New Zealand	Hudson Gavin Martin / The Blockchain Boutique: Andrew Dentice & Rachel Paris	204

Continued Overleaf →

Further copies of this book and others in the series can be ordered from the publisher. Please call +44 20 7367 0720

Disclaimer

This publication is for general information purposes only. It does not purport to provide comprehensive full legal or other advice. Global Legal Group Ltd. and the contributors accept no responsibility for losses that may arise from reliance upon information contained in this publication. This publication is intended to give an indication of legal issues upon which you may need advice. Full legal advice should be taken from a qualified professional when dealing with specific situations.



Country Question and Answer Chapters:

35	Nigeria	Udo Udoma & Belo-Osagie: Yinka Edu & Tolulope Osindero	210
36	Norway	BAHR: Markus Nilssen & Vanessa Kalvenes	216
37	Peru	Vodanovic Legal: Ljubica Vodanovic & Alejandra Huachaca	223
38	Philippines	Gorriceta Africa Cauton & Saavedra: Mark S. Gorriceta	229
39	Poland	Traple Konarski Podrecki & Partners: Jan Byrski, PhD, Habil. & Karol Juraszczyk	234
40	Portugal	Uría Menéndez – Proença de Carvalho: Pedro Ferreira Malaquias & Hélder Frias	242
41	Russia	QUORUS GmbH: Maxim Mezentsev & Nikita Iovenko	250
42	Singapore	AEI Legal LLC: Andrea Chee & Law Zhi Tian	258
43	Slovenia	Schoenherr: Jurij Lampič	265
44	South Africa	ENSafrica: Angela Itzikowitz & Ina Meiring	271
45	Spain	Uría Menéndez: Leticia López-Lapuente & Isabel Aguilar Alonso	278
46	Sweden	Mannheimer Swartling: Anders Bergsten & Martin Pekkari	286
47	Switzerland	Bär & Karrer: Dr. Daniel Flühmann & Dr. Peter Ch. Hsu	292
48	Taiwan	Lee and Li, Attorneys-at-Law: Robin Chang & K. J. Li	300
49	Thailand	Silk Legal Co., Ltd.: Dr. Jason Corbett & Don Sornumpol	306
50	Turkey	Erciyas Law Office: Nihat Erciyas & Miraç Arda Erciyas	311
51	Ukraine	Evris Law Firm: Sergii Papernyk & Alexander Molotai	317
52	United Kingdom	Slaughter and May: Rob Sumroy & Ben Kingsley	322
53	USA	Shearman & Sterling LLP: Reena Agrawal Sahni & Eli Kozminsky	329

EDITORIAL

Welcome to the third edition of *The International Comparative Legal Guide to: Fintech*.

This guide provides corporate counsel and international practitioners with a comprehensive worldwide legal analysis of the laws and regulations of fintech.

It is divided into two main sections:

Two general chapters. These chapters provide an overview of artificial intelligence in fintech, and of the recent trends and challenges in the financing of cross-border fintech start-ups.

Country question and answer chapters. These provide a broad overview of common issues in fintech laws and regulations in 51 jurisdictions.

All chapters are written by leading fintech lawyers and industry specialists and we are extremely grateful for their excellent contributions.

Special thanks are reserved for the contributing editors Rob Sumroy and Ben Kingsley of Slaughter and May for their invaluable assistance.

Global Legal Group hopes that you find this guide practical and interesting.

The *International Comparative Legal Guide* series is also available online at www.iclg.com.

Alan Falach LL.M.
Group Consulting Editor
Global Legal Group
Alan.Falach@glgroup.co.uk

Artificial Intelligence in Fintech

Rob Sumroy



Ben Kingsley



Slaughter and May

1 Introduction

“AI” has been the fintech buzzword of the past couple of years. But what is AI, why is it so relevant to fintech, and what legal issues might be raised by its use? This chapter examines these questions, setting out a brief history and description of AI, followed by a review of its current use in fintech and why this is a growing area. We then briefly discuss the legal issues which may be raised by the use of AI and, in particular, its use in a financial context.

AI represents a hugely exciting tool and framework with which, and within which, actors in all sectors have new potential to engage with their customers and counterparties. The World Economic Forum, for instance, reported in its Global Risks Report for 2017 that global investment in AI start-ups had risen from \$282 million in 2011 to just shy of \$2.4 billion in 2015 (World Economic Forum, 2017), and worldwide spending on cognitive and artificial intelligence systems is forecast to reach \$77.6 billion in 2022, according to a new IDC Spending Guide. It is distinctly possible that more money will be invested in the next decade into AI research than has been invested in the entire history of the field to this point. One of the most visible examples of this sort of innovation has been in the financial services and asset management sectors.

2 What is AI?

2.1 A brief history

In 1987, Warren Buffett wrote in his letter to the shareholders of Berkshire Hathaway: “In my opinion, investment success will not be produced by arcane formulae, computer programs or signals flashed by the price behaviour of stocks and markets.” Thirty years on, he may be proved wrong. Since 2016, Aidyia, the Hong-Kong based investment company, has managed a hedge fund that is entirely automated, requiring no supervision or intervention by humans. At the heart of these new developments lies artificial intelligence (AI).

Marvin Minsky, one of the founders of the field of AI, defined AI as “the science of making machines do things that would require intelligence if done by man” (Minsky, 1968). It is generally agreed that AI as an academic and research discipline, and indeed even as a term, can be traced to a formal beginning in 1956 at the US Dartmouth College. Academics at Dartmouth College at the time proposed a two-month study of AI with a bold and exciting vision, “to proceed on the basis of the conjecture that every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it”

(McCarthy *et al.*, 1955). The academics at Dartmouth College considered that a two-month period would be enough to achieve this “general AI”, but 60 years later this is still elusive.

The 1990s and 2000s brought major advances in AI through improvements in machine learning and the use of “neural networks”, driven by developments in algorithms and the increasing availability of large sets of training data. This led, in the early 2010s, to the concept of “deep learning”, involving complex neural networks (designed to mimic the brain’s activity), which have led to successes such as defeating human agents in chess, Go and reading comprehension.

2.2 Different types of AI

While there is some disagreement over the most appropriate manner and the level of granularity with which to categorise AI, here we adopt the four categories of AI that are entering the financial industries, which were used by the consultancy firm Deloitte in an article on intelligent automation in the business world.

Machine learning

This refers to a computer system where the performance of a given task improves through experience and exposure to a variety of data. The key element here is that machine learning represents the ability to perform a task, and improve, without the need to follow explicitly programmed instructions.

This frees up the capacity to perceive and exploit subtle correlations within a massive set of seemingly unconnected data. It does not rely on the boundaries of a human mind attempting to delineate every logical if/then rule that might apply to a given task.

Some examples of applications in the financial sector may include the prediction of fraud, or recognition of rogue trading.

Autonomics

Autonomics refers to a system that is capable of not only learning about and identifying new patterns within a set of data, but of executing a task or operation that is usually carried out by a human actor.

The system here is therefore not only capable of recognising an incident or a pattern of incidents, but can also implement the appropriate routine to resolve such an incident.

Concrete examples could therefore include troubleshooting software or the execution of credit risk analysis.

Machine vision

Machine vision refers to the ability of a computer to recognise and identify discrete objects, or even themes or activities, in images.

The machine may also be able to classify the identified object as something which is already known to the machine; this could be anything from recognising an approved user, or confirming a given “watermark” which attaches to a certain asset or currency.

Natural language processing

This is where a machine or computer is able to process and interpret human language and respond appropriately.

General versus narrow

Notwithstanding the functional distinctions that have been drawn above, it may also be useful to conceptualise AI using another spectrum: narrow AI to general AI. All of the functions set out above are broadly capable of being ascribed general problem-solving capabilities. However, it is important to note that even where a machine has taken great steps on its own, technology at present is at the stage wherein all systems fall within the “narrow” category, meaning that for any given problem, there is a specific AI design to try to solve it, rather than a generic AI able to solve any problem. General AI is usually what is portrayed in science fiction literature and films, but has not, yet, been achieved.

3 The Benefits of AI

Broadly, computers with artificial intelligence are clearly capable of making decisions much faster than their human counterparts, and with reference to much larger sets of data. We consider that these benefits can be further analysed using the following generic categories.

3.1 Personalisation

For services which are provided to individual customers, AI has the potential (and indeed has already begun) to massively expand the limits of that interface. This can start at the beginning of a customer interaction through intelligent identification using machine vision. Certain products or parts of a service can then be recommended to the customer based on past behaviour within the given service, much like Netflix alters its user interface based on each customer’s previous use. At base, this is simply the potential for AI to give rise to a better customer experience.

But this element can be stretched even more imaginatively. If a computer has access to larger sets of data in relation to the customer’s circumstances – for example, spending habits linked to fluctuating commodities such as fuel, or consumption of certain utilities such as water – then products and even advice can be altered or recommended in a much more streamlined fashion than if mere past usage of the given app or service is taken into account.

At a higher level than pure customer experience, where the machine is able to learn what those idiosyncratic, highly personalised requirements or behaviours of its customers are, and has access to a multitude of information about the use of its services and products at any given moment, it is much easier to detect where behaviour deviates from the norm. This again can feed back into providing more bespoke advice or products to an individual, but the more obvious application is to the detection of fraudulent activity.

3.2 Adaptability

Previously, computer-based services or tools have been very logic-based. Exhaustively designed inputs are tied to a delineated set of outputs. Where AI has the ability to break new ground is the capacity to make seemingly imaginative leaps to accommodate

unexpected shifts in the broad market, or even to respond sensibly and effectively to novel customer behaviours on a more granular level.

One of Michael Lewis’ memorable examples of the imaginativeness of Wall Street traders is the buying of potato futures in the immediate aftermath of Chernobyl: “A cloud of fallout would threaten European food and water supplies, including the potato crop, placing a premium on uncontaminated American substitutes” (Lewis, 2000). But, of course, this is merely the recognition of established patterns and a calculation of the likelihood that a given cause will entail a given effect. Machines are able to perform the exact same function but with vastly larger data sets; the interesting element is that computers now have the capacity to receive such data in a variety of different ways and also learn from how that data changes over time. One can now conceive, for instance, of a computer listening to the words of an important economic speech from a UK Chancellor or an ECB president whilst simultaneously digesting headlines and formulating a real-time trading strategy, even where something dramatic or paradigm-shifting arises. This adaptability benefit feeds well into the third benefit of AI: automation.

3.3 Automation

Automation is currently widely utilised, especially in segments of a business that are more rules-based. Simple examples include the use of ATMs at banks or self-service checkouts in supermarkets.

A lot of the time, such machines will be carefully configured so that recognised inputs will lead to a given output. Where an input is not recognised, human intervention is required. The leap from adaptability to automation is an obvious one; a machine that can learn how to process new data and situations will require less human intervention.

Businesses therefore have a huge opportunity to begin optimising those more routine, or scale-based, areas of its function, thus lowering costs and increasing efficiency. In 2016, JP Morgan reported that they already had line of sight to savings of more than \$30 million in 2017 due to the automation of system access administration, and research published by PwC suggests that by the mid-2030s, 30 per cent of UK jobs could be automated.

This would of course change the way in which responsibility and accountability is allocated within certain segments of a given business, and especially so in an industry such as financial services. The ways in which roles begin to change will impact on our thinking around the regulation of AI, particularly as focal points of responsibility begin to shift within the financial services industry.

4 Why are We Talking About AI in Fintech?

4.1 Disruptive capability

The banking industry’s larger players are increasingly facing disruption in the marketplace, fuelled by the innovation of fintech companies. Investments in global fintech have grown at an exponential rate over the past decade. The global fintech sector saw over \$50 billion of investment between 2010 and 2016 (Accenture, 2016), and the *Forbes Fintech 50 report* (Forbes, 2019) reports that overall investment in fintech “surged” in 2018, hitting \$55 billion worldwide (double the year before). Big fintechs are also getting bigger, with 19 of the 2019 Fintech 50 being valued at \$1 billion or more.

While the Western banking market is still in the earlier stages of this disruption cycle, traditional players are starting to recognise the importance of embracing change (JP Morgan noting in its 2017 Annual Report that fintech forms the bank's "backbone"). And the forecast is eye-widening: Citi predicts that, by 2023, as much as 17 per cent of consumer banking revenue in North America will be derived from new digital models (Ghose, 2016). AI, as the newest frontier of technological advances in business and in the financial sector, will be at the heart of the momentum.

An interesting example of how larger-footprint, established players are being undercut is through the ubiquity of mobile devices as compared to "typical" bank accounts. M-Pesa is a prime example, the mobile money initiative which first launched in Kenya in 2007, enabling person-to-person mobile payments. At its 10th anniversary, M-Pesa boasts usage in 96 per cent of households in Kenya (Collins, 2017). This level of market penetration is remarkable, but the social inclusion effect is also important: reportedly, M-Pesa is responsible for lifting two per cent of Kenyan households out of poverty (*ibid.*). The fintech space is therefore exciting not only from the business side, but also from a societal side, as it represents a tool for financial inclusion.

The capacity of AI to fine-tune the interface with the customer itself feeds well into this dynamic. "Cleo", a London-based fintech which developed an artificially intelligent "chatbot", is a notable example. Cleo is a financial assistant with which the customer can interact via text messaging or voice to help present, and assist, in organising his or her financial information. For instance, Cleo can let its user know how much they have spent in coffee shops in a month as well as set up alerts if such spending goes over a certain limit. Having built a successful UK business, it was reported at the start of 2018 that Cleo had expanded into the US market and that further global expansion was planned (techcrunch.com, 2018).

As customers demand instant forms of communication, smarter and more intelligent chatbots in financial services are on the rise, with many organisations now using them.

4.2 Mainstream fintech

However, more established players in the financial services and investment sectors have not been slow on the take-up of artificial intelligence. As early as 2012, Bridgewater poached IBM's head of AI, and in 2018 JP Morgan made headlines, hiring a leading AI specialist from Google.

Mainstream financial institutions, with their sprawling and complex data landscapes, have not been slow to implement AI in different sectors of their business. This has been borne out both in their adoption of technology (JP Morgan noted in its 2017 Annual Report that it benefits from the expertise of 50,000 technologists, and its 2018 technology budget totalled \$10.8 billion, with more than \$5 billion earmarked for new investments) and in the willingness of these bigger players to collaborate with fintech start-ups. Citigroup, for example, invested in Behavox, which uses artificial intelligence to monitor the phone calls, emails and electronic chats of bankers. Other interesting examples are Nasdaq's acquisition of London-based software company, Sybenetix, which uses artificial intelligence software to track the behaviour patterns of individual traders and spot rogue trading, and HSBC's announcement that it will employ the artificial software of Quantexa to assist with detecting money laundering (Arnold, 2017).

The more established companies in the banking sphere have also recognised quickly that AI has massive potential to drive down costs. Compliance, for example, is an area where financial institutions continue to dedicate huge amounts of budget and resources, and the

volume of regulation continues to increase. Duff and Phelps estimate that regulatory costs will rise from 4% to 10% of revenue by 2021 (Forbes, 2018) and financial institutions (and regulators such as the FCA) are looking at ways fintech and RegTech (much of which is underpinned by AI) can help.

5 What Could Be Some Legal/Regulatory Challenges?

Attempting to marry something as technical and, as Warren Buffett put it, arcane as AI with robust and successful regulation presents novel challenges. One root of the problem is the dislocation between, on the one hand, the need for transparency in financial regulation and, on the other hand, the impenetrability for the majority of people of the inner workings of an AI system. Indeed, the more advanced that certain types of AI become, the more they become "black boxes", where the creator of the AI system does not really know the basis on which the AI is making its decisions, which means that ensuring accountability for, and compliance in, the behaviour of an AI becomes very difficult.

One well-known example of this was the 2016 game of AlphaGo between Google's DeepMind and Lee Sedol. The move played by the machine to beat its human opponent was so unusual that it prompted match commentators to assume that AlphaGo had malfunctioned. Humans were unable to fully understand or unpick its rationale for the move, and AlphaGo (like many AI systems) was not designed to provide reasons for its decisions and so could not explain why it made the move.

5.1 Regulatory issues

Currently, one very interesting area of discussion in which we have been engaged in the UK and Europe is the extent to which existing regulatory systems and structures are adequately able to supervise and control the risks involved in deploying AI-based products, services and approaches. These risks, and the ability to manage them, are a challenge both for the firms concerned and the regulators tasked with protecting consumer interests and the integrity of the financial system; as with many new technologies, to date there has perhaps been less appetite to analyse the risks of AI than to contemplate the potential gains.

Regulators tend to take a technology-neutral approach to rule-making today, at least in Europe, choosing to focus on activities and outcomes rather than the means of delivery. So, in principle, AI methods of performing existing activities or achieving existing outcomes should fall neatly within existing legal and regulatory frameworks. In some cases this is evidently true, and thus there should be no need for new laws or regulations, just new understandings of business models, of risks and of the effectiveness of risk management responses.

That said, it is equally quite evident that the introduction of autonomous non-human actors in customer-facing discretionary decision-making processes, such as the provision of financial advice, wealth management, credit assessment and the like, could give rise to some more complex questions around the attribution of responsibility (and liability) for risks, particularly when risks crystallise into harm. In the UK, the House of Lords recommended, in a wide-ranging AI report, that there was no need for new general AI regulation, but that any new rules should be approached on a sector by sector basis.

At this stage in the lifecycle of AI's pairing with financial services, it is probably unhelpful to draw conclusions about any need for future

legal or regulatory architecture on the basis of generic concepts – and fortunately for the time being, there seems to be limited need, or indeed appetite, to make rules in this area. The more entrepreneurial policy approach, which we are fortunate to see practised in the UK, is to provide a safe space – a sandbox – in which to live-test specific concepts and use cases so that unanticipated and unaddressed risks and harms can hopefully be identified, and an appropriate policy discussion and consultation can then take place to ensure that laws and regulation buffer rather than smother innovative AI models.

The achievable aim of regulation can and should be to facilitate the safe deployment of beneficial new technologies, such as AI.

5.2 Intellectual property and AI

A key consideration for companies seeking to use AI in their business is how they can protect and exploit the investment they make into this powerful new technology.

The classification and protection of the intellectual property surrounding any AI model is an interesting and developing area. This may need to include not only the algorithms on which the AI model is based, but also any ideas or inventions which the AI itself creates.

The analysis of what intellectual property rights arise in respect of an AI model will require an individual assessment of the type of AI and how it has been implemented by its developers.

The algorithm and AI processes which sit behind an AI may be patentable inventions in and of themselves, though this will vary from jurisdiction to jurisdiction. IBM is reported to be the largest owner of AI patents. It received 9,100 patents in 2018 alone, and nearly half of these related to emerging areas of technology (including AI). Of course, the downside of a patent is that the applicant is required to disclose the patentable material (e.g., the algorithm), which may be disadvantageous, giving competitors an opportunity to design around the patented invention.

Most jurisdictions will also protect the expression of the algorithm and AI processes in the form of software through copyright law. However, there is more of a challenge where the AI continues to “learn” and so make changes to its own software structure – again, there is variation between jurisdictions as to whether they will recognise copyright in works created by a computer, and the ownership of those works.

The concept of computer authorship is already legislated for in English law; section 9(3) of the Copyright, Designs and Patents Act 1988 provides that “in the case of a literary, dramatic, musical or artistic work which is computer-generated, the author shall be taken to be the person by whom the arrangements necessary for the creation of the work are undertaken”.

This wording may be simple enough to navigate through a more pedestrian instance of one engineer designing a simple algorithm; actively inputting a given set of data with the express purpose of eliciting the creation of a new computer program. On the other hand, it is unclear how this wording might be stretched in order to accommodate more complex scenarios involving multi-faceted models, capable of learning and expanding their input and output without human supervision. It is conceivable that we may reach a point where human “arrangement” is many steps removed, and perhaps not capable of being traced. It will require careful thinking and testing of the law; questions of ownership feed importantly into how responsibility and accountability is framed.

Where it is not possible to establish from the output of an AI how the AI model in question works, then the best form of protection may just be to protect the confidentiality of the algorithms and AI model.

Most jurisdictions will have laws which protect trade secrets or confidential information, and the best investment in protecting a valuable AI asset may be in enhancing your organisation’s conventional and cyber security protections and procedures.

Like most intangible assets, it is possible to license a proprietary AI model to others, and how this licensing is to be structured will again vary depending on the type of AI and the use to which it is put. Where the AI model is static and is not continuing to be trained, this is relatively similar to licensing any other software product. However, where it is anticipated that the AI model will continue to be trained after deployment, and where the benefit of this training is expected to be shared with all licensees of the relevant AI, then a bespoke approach will need to be taken to feeding back any “improvements”.

5.3 Data protection

The key risk areas for data protection in AI are: (i) the training of an AI model using personal data, and whether that processing of the personal data is lawful; and (ii) the way in which an AI model itself processes personal data when it is deployed.

Data protection authorities around the world are now focussing on AI. The Information Commissioner’s Office (ICO) stated in November 2018 that AI is one of its three top priorities, given the “ability of AI to intrude into private life and affect human behaviour by manipulating personal data”. This statement highlights some of the tensions that exist between AI and data protection regulation. Some of the key principles enshrined in EU and UK data protection law which are challenging for AI are set out below.

Purpose specification and use limitation – personal data used by an AI model may not originally have been collected for that purpose.

Unintentional bias and fairness – the potentially inscrutable way in which an AI model processes personal data can mask, and even lead to, unexpected and unfair outcomes by reflecting unintended biases. For example, in pre-GDPR guidance from 2017, the ICO draws attention to research which suggested that internet searches for “black-identifying” names generated advertisements associated with arrest records far more often than those for “white-identifying” names (ICO, 2017).

Transparency and intelligibility – AI that cannot easily be explained is very likely to be too opaque to be fair. The ICO has also touched on the problem of the obscurity of AI models in terms of relying on consumers’ “informed consent” to the processing of their personal data. The high threshold for consent set out in EU and UK data protection law also mean that consent may not be the most appropriate ground to rely on to justify the processing of personal data by an AI model. This is compounded by the fact that a binary yes/no approach to consent may by its very nature be incompatible with an AI model that is able to find entirely new uses for sets of data. The ICO has helpfully pointed out that a more dynamic approach may be possible, with a “process of graduated consent, in which people can give consent or not to different uses of their data throughout their relationship with a service provider, rather than having a simple binary choice at the start” (ICO, 2017). As mentioned at the beginning of this chapter, transparency underpins all regulation.

Data minimisation and data retention limitations – these may be difficult to comply with when using certain AI models (e.g., an AI model may continuously keep learning to use personal data in slightly different ways or for different purposes).

Upholding the exercise of individual rights (including rights of access, rights to data portability, rights of rectification and erasure, etc.) – the GDPR also recognises that “the data subject shall have

the right not to be subject to a decision based solely on automated processing". This right and the restrictions that flow from it are designed to counter some of the problems identified above around unintentional bias.

Risk profile of data protection compliance – the consequences of non-compliance, or of a cyber/data breach are significant. They include fines of up to €20 million or 4% of annual worldwide turnover (whichever is greater), potential follow-up litigation from consumers and reputational damage. The GDPR suggests various tools and mechanisms to help identify and mitigate privacy risks, such as data protection impact assessments and privacy by design and default. However, without further guidance from regulators, this will remain a challenging area.

6 Conclusion

AI has the potential to change the way businesses function across all sectors in the economy, and finance is at the forefront of this change. Both existing businesses looking to innovate to keep up with competition, and start-ups seeking to disrupt, need to be aware of the legal and regulatory issues which they face in implementing these new technologies, and how they can mitigate the key risks which arise.

Bibliography

1. Books

- 1.1 Minsky, M. 1968. *Semantic Information Processing*. Cambridge, MA: MIT Press.
- 1.2 Lewis, M. 2000. *Liar's Poker*. London: Penguin.

2. Government & regulator publications

- 2.1 House of Commons Science and Technology Committee (2016). *Robotics and artificial intelligence* [online]. Available at: <https://www.publications.parliament.uk/pa/cm201617/cmselect/cmsctech/145/145.pdf>. [Accessed 15 February 2018.]
- 2.2 UK Information Commissioner's Office (2017). *Big data, artificial intelligence, machine learning, and data protection* [online]. Available at: <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>. [Accessed 15 February 2018.]
- 2.3 House of Lords Select Committee on AI Report: *AI in the UK: ready, willing and able* [online]. Available at: <https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf>.

3. Newspaper articles

- 3.1 Arnold, M. (2017). *Banks' AI plans threaten thousands of jobs*. Financial Times [online]. Available at: <https://www.ft.com/content/3da058a0-e268-11e6-8405-9e5580d6e5fb>. [Accessed 15 February 2018.]

4. Websites & online articles

- 4.1 PwC (2017). *Sizing the prize* [online]. Available at: <https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf>. [Accessed 15 February 2018.]

- 4.2 World Economic Forum (2017). *Assessing the Risk of Artificial Intelligence* [online]. Available at: <http://reports.weforum.org/global-risks-2017/part-3-emerging-technologies/3-2-assessing-the-risk-of-artificial-intelligence/>. [Accessed 15 February 2018.]
- 4.3 McCarthy, M. *et al.* (1955). *A PROPOSAL FOR THE DARTMOUTH SUMMER RESEARCH PROJECT ON ARTIFICIAL INTELLIGENCE* [online]. Available at: <http://jmc.stanford.edu/articles/dartmouth.html>. [Accessed 15 February 2018.]
- 4.4 PwC (2017). *Will robots really steal our jobs? An international analysis of the potential long term impact of automation* [online]. Available at: <https://www.pwc.co.uk/economic-services/assets/international-impact-of-automation-feb-2018.pdf>. [Accessed 15 February 2018.]
- 4.5 Accenture (2016). *Fintech and the evolving landscape: landing points for the industry* [online]. Available at: https://www.accenture.com/t00010101T000000Z_w/_gb-en/_acnmedia/PDF-15/Accenture-Fintech-Evolving-Landscape.pdf. [Accessed 15 February 2018.]
- 4.6 Ghose, R. *et al.* (2016). *DIGITAL DISRUPTION: How FinTech is Forcing Banking to a Tipping Point* [online]. Citi GPS: Global Perspective & Solutions. Available at: <https://www.citivelocity.com/citigps/ReportSeries.action?recordId=51>. [Accessed 15 February 2018.]
- 4.7 Collins, K. (2017). *Kenya's been schooling the world on mobile money for 10 years* [online]. Available at: <https://www.cnet.com/news/kenya-mobile-money-vodafone-mpesa-10-years/>. [Accessed 15 February 2018.]
- 4.8 IBM (2018). *IBM Breaks Records to Top U.S. Patent List for 25th Consecutive Year* [online]. Available at: <https://www-03.ibm.com/press/us/en/pressrelease/53581.wss>. [Accessed 15 February 2018.]
- 4.9 *Forbes Fintech 50 Report*. Available at: <https://www.forbes.com/fintech/2019/#98b0acf2b4c6>.
- 4.10 *JPMorgan Chase's 2017 Annual Report*. Available at: <https://www.jpmorganchase.com/corporate/investor-relations/document/annualreport-2017.pdf>.
- 4.11 *IDC Spending Guide*. Available at: <https://www.idc.com/getdoc.jsp?containerId=prUS44291818>.
- 4.12 PwC. *How will automation impact jobs?* Available at: <https://www.pwc.co.uk/services/economics-policy/insights/the-impact-of-automation-on-jobs.html>.
- 4.13 Forbes (2018). *Taming The High Costs of Compliance with Tech* [online]. Available at: <https://www.forbes.com/sites/tomgroenfeldt/2018/03/22/taming-the-high-costs-of-compliance-with-tech/#359a85035d3f>.
- 4.14 techcrunch.com (2018). *Cleo, the chatbot that wants to replace your banking apps, has stealthily entered the U.S.* [online]. Available at: https://techcrunch.com/2018/03/20/cleo-across-the-pond/?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=tTILM-9gtYCrAVJTL-fAoQ.

Acknowledgments

The authors would like to acknowledge their colleagues Matthew Harman, Harry Vanner, Natalie Donovan and Cindy Knott for their invaluable contributions to the preparation of this chapter.

**Rob Sumroy**

Slaughter and May
1 Bunhill Row
London EC1Y 8YY
United Kingdom

Tel: +44 20 7090 4032
Email: rob.sumroy@slaughterandmay.com
URL: www.slaughterandmay.com

Rob is Head of Slaughter and May's Technology practice and co-heads the firm's Fintech Team and Data Privacy practice. He advises on all aspects of IT, outsourcing, e/m-commerce, big data, data protection, cyber security and IP, as well as assisting organisations with their digital strategies. Rob is ranked in the IT and Outsourcing sections of *Chambers UK*, recognised as a leading individual for Commercial Contracts in *The Legal 500* and is listed in Super Lawyers.

**Ben Kingsley**

Slaughter and May
1 Bunhill Row
London EC1Y 8YY
United Kingdom

Tel: +44 20 7090 3169
Email: ben.kingsley@slaughterandmay.com
URL: www.slaughterandmay.com

Ben is a partner in Slaughter and May's Financial Regulation practice and co-heads the firm's Fintech Team. His clients span the full spectrum from established global financial and TMT groups to high growth start-up challengers. He advises on all aspects of UK and EU financial regulation, including in the areas of banking, insurance, asset management, payments, mobile banking, e-money, and digital financial services. Ben is recognised in *The Legal 500* as a leading individual in the area of fintech.

SLAUGHTER AND MAY

Slaughter and May is a full-service international law firm headquartered in London with first-class European technology and fintech practices. We are pleased to have been retained as UK and EU legal advisers to a broad range of investors, entrepreneurs, high growth start-ups, established businesses and multi-national corporations. Among our many tech and fintech sector clients we are delighted to have supported Stripe, Euroclear, Equinix, WorldRemit, Aviva, Arm Holdings, Google and Vodafone.

Cross-Border Financing of Fintech: A Comparison of Venture and Growth Fintech Financing Trends in Europe and the United States

Stanford Law School

Jonathan Cardenas



Cross-border financing of early-stage technology companies is increasingly recognised as a driver of innovation and national industrial competitiveness.ⁱ In the financial technology (“Fintech”) sector alone, cross-border flows of venture and growth stage investment have skyrocketed to unprecedented levels in recent years, contributing to a proliferation of innovative Fintech start-ups on both sides of the Atlantic. This chapter will provide an overview of recent trends and challenges in venture and growth-stage financing of Fintech start-ups in Europe and the United States (“U.S.”), highlighting the importance of these investments for the transatlantic economy.ⁱⁱ

I. Global Fintech Investment in Context

Overall global investment in the Fintech sector amounted to \$55.3B in 2018, spread over a total of 3,251 deals globally, more than doubling the \$26.7B invested in 2017.ⁱⁱⁱ Of this total, venture capital-backed Fintech start-ups raised more than \$39B across 1,707 deals, including 52 “mega” rounds each exceeding \$100M.^{iv} Within this funding landscape emerged 16 Fintech unicorns (those valued at over \$1B) in 2018,^v including Circle (\$3B),^{vi} UiPath (\$3B),^{vii} DevotedHealth (\$1.8B),^{viii} Brex (\$1.1B),^{ix} Dataminr (\$1.2–1.6B),^x Tradeshift (\$1B)^{xi} and Root (\$1B)^{xii} in the U.S., together with Revolut (\$1.7B)^{xiii} and Monzo (\$1.27B)^{xiv} in the United Kingdom (“UK”), among others located elsewhere.^{xv}

Although the U.S. was home to the highest number of Fintech investment transactions in 2018 with over 1,100 deals executed, China accounted for 46% of all Fintech investment volume.^{xvi} The largest Fintech financing transaction in 2018 was that of Hangzhou-based Ant Financial Services Group, which raised a record-breaking \$14B in a financing round co-led by the Singaporean Government’s GIC Private Limited and Temasek Holdings.^{xvii} In the U.S., the total value of Fintech deals increased by 46% in 2018 to \$16.6B, with LendingPoint’s \$600M credit facility financing standing as the largest U.S. Fintech transaction of the year.^{xviii} The total value of Fintech deals also increased in the UK by 50% in 2018 to \$3.9B,^{xix} with the largest transactions including Prodigy Finance’s \$1B financing round,^{xx} Revolut’s \$250M round,^{xxi} Atom Bank’s \$200M round^{xxii} and Monzo’s \$100M round.^{xxiii} In contrast to other regions of the world, however, the total volume of Fintech financing in Europe declined in 2018, yielding a total of approximately \$3.5B.^{xxiv}

A. Corporate Venture Capital Investment in Fintech

Corporate venture capital investment in Fintech also increased significantly in 2018, with corporate venture capital investors participating in 33% of all Fintech deals globally, amounting to a five-

year high.^{xxv} The leading Fintech corporate venture capital investors in 2018 were American Express Ventures, CapitalG (Alphabet’s growth equity investment fund), Citi Ventures, Goldman Sachs Principal Strategic Investments, Google Ventures, ING Ventures, Munich RE Ventures and Santander InnoVentures.^{xxvi} Among the most significant Fintech corporate venture capital transactions in 2018 were ABN AMRO Digital Impact Fund’s investment in solarisBank,^{xxvii} BBVA’s investment in Atom Bank,^{xxviii} CapitalG’s investment in Robinhood^{xxix} and Morgan Stanley Tactical Value Fund’s investment in Dataminr.^{xxx}

In addition to direct corporate venture capital investment in Fintech start-ups, 2018 also saw a growing number of indirect investments by way of incubator and accelerator programmes housed within banks, commonly referred to as “Fintech innovation labs”.^{xxxi} Examples include the Barclays Accelerator, BBVA Innovation Labs, Citi Innovation Labs and Innovation at Rabobank.^{xxxii} Corporate venture capital investment in European and U.S. Fintech start-ups is projected to continue to grow in 2019.^{xxxiii}

II. Early-Stage Venture Financing Challenges in Europe

In contrast to the U.S., which has historically been regarded as the strongest market worldwide for the provision of venture capital to early-stage technology companies,^{xxxiv} Europe is widely regarded as a region that faces major obstacles in early-stage venture funding.^{xxxv} The German Private Equity and Venture Capital Association (the *Bundesverband Deutscher Kapitalbeteiligungsgesellschaften* or “BVK”), for example, has recognised that early-stage German technology start-ups face barriers in obtaining domestic venture capital funding due, in part, to the relatively low number of large venture capital funds in Germany combined with a lack of interest from institutional investors in the small German venture capital funds that currently exist.^{xxxvi} In addition, the German venture capital ecosystem is constrained by an overall culture of financial risk aversion that produces an inclination towards debt financing rather than equity financing.^{xxxvii} Similar views have been expressed with respect to the venture capital environment in the European Union (“EU”) as a whole by the European Commission and Invest Europe (formerly known as the European Private Equity & Venture Capital Association).^{xxxviii}

European venture financing constraints, which are present across all industries, directly impact Fintech start-ups and are one reason for the relative decline in total volumes of Fintech financing in Europe in 2018. As described in further detail below, various public sector initiatives have been implemented in Europe to stimulate pan-European venture capital investment in early-stage European

technology start-ups. Each of these initiatives is likely to increase the amount of capital that is available to early-stage European Fintech start-ups in the future.

A. Public-Private Partnership Model in German Venture Capital

The combination of a risk-averse financial culture in Germany^{xxxix} with an overall shortage of large-scale venture capital funds has led to the implementation of the public-private partnership model – traditionally deployed in the financing of public infrastructure projects – in the venture capital sphere. The Bonn-based High-Tech Gründerfonds (“HTGF”), for example, which is Germany’s largest seed investor,^{xi} is structured as a public-private partnership venture capital firm. HTGF’s investor base includes major public sector institutions, such as the German Federal Ministry for Economic Affairs and Energy, the German state-owned development bank Kreditanstalt für Wiederaufbau (“KfW”), and the Fraunhofer Society for the Advancement of Applied Research (“Fraunhofer-Gesellschaft”), as well as private sector actors, such as BASF, Deutsche Post DHL and Robert Bosch, among others.^{xii} HTGF has invested approximately €892M in more than 500 seed-stage German technology start-ups,^{xiii} and is considered a significant player in the German Fintech sector. Recent HTGF seed financings in Fintech include Berlin-based insurtech start-up remind.me in May 2018,^{xiiii} North Rhine-Westphalia-based digital debt collection start-up troy in September 2018,^{xiv} Frankfurt-based crypto asset management firm Iconiq Holding in January 2019,^{xlv} and Frankfurt-based blockchain services provider Agora Innovation in February 2019.^{xlvi} While the public-private partnership model has proven to be successful in the German context, the level of funding that it has provided is simply not enough to enable German and European start-ups to compete on a global scale.

B. EU Venture Capital Fund-of-Funds Programme

In an effort to “bridge the gap” that exists between small European venture capital funds and large institutional investors,^{xlvii} the European Commission and the European Investment Fund (“EIF”) launched a pan-European venture capital fund-of-funds programme known as VentureEU in April 2018.^{xlviii} Developed under the auspices of the European Commission’s Capital Markets Union Action Plan, VentureEU is expected to stimulate €6.5B of investment in “start-up and scale-up” companies across the EU by way of six fund-of-funds that will invest public and private sector capital in small venture capital funds, each of which is required to focus on investment projects in at least four European jurisdictions.^{xlix} Funding into each of the six VentureEU fund-of-funds consists of an initial “cornerstone” investment of up to €410M from EU institutions, including the European Investment Fund, the Horizon 2020 InnovFin Equity initiative, COSME (the EU programme for the Competitiveness of Enterprises and SMEs), and the European Fund for Strategic Investments, with the remainder provided by private investors in matching amounts.¹

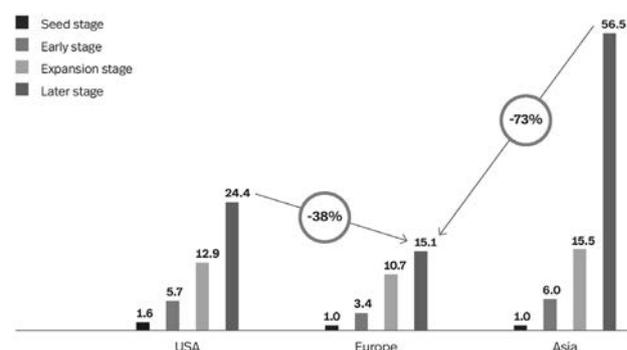
The VentureEU programme has sparked the creation of similar initiatives at the EU Member State level. In March 2019, for example, the EIF and Axis, the wholly-owned venture capital arm of Spanish credit institution Instituto de Crédito Oficial, jointly launched a €40M angel investment fund geared toward Spanish early-stage technology start-ups.ⁱⁱ The fund, which forms part of EIF’s European Angels Fund initiative,ⁱⁱⁱ will provide funding to angel investors who invest in the Spanish market. In addition, the EIF and Germany’s Fraunhofer-Gesellschaft established a joint

technology transfer fund in February 2019 under the auspices of the European Commission’s EU Finance for Innovators (“InnovFin”) programme.ⁱⁱⁱⁱ This €60M Fraunhofer Tech Transfer Fund will help to commercialise intellectual property generated by researchers at the Fraunhofer-Gesellschaft’s 72 research institutes, with the intent of catalysing spin-offs that will transfer technology “from the laboratory to the economy”.^{lv} The launch of these initiatives is projected to stimulate deeper investment in early-stage technology start-ups across Europe and is likely to provide further impetus for venture capital investment in the European Fintech sector.

III. Growth Equity Investment in Fintech

In addition to venture capital financing barriers that exist at the nascent stage of development, European technology start-ups wrestle with financing obstacles at the growth stage, which is commonly referred to as the “turning point” for market entry.^{lv} As the below graph illustrates, Europe trailed behind Asia and the U.S. in 2018 with respect to levels of venture capital invested in both expansion and later-stage start-ups:^{lvi}

Average venture capital investment per company by phase in the startup lifecycle in Q2 2018 [EUR m]



Source: German Private Equity and Venture Capital Association (BVK), Roland Berger; Internet Economy Foundation, CB Insights and PwC. Figures have been rounded.

In recent years, however, an increasing amount of capital has been invested in growth-stage start-ups through growth private equity (“growth equity”) investment vehicles, which attract limited partners that seek exposure to technology start-ups with potentially lower risk profiles than those at earlier stages of development.^{lvii} In 2018, overall growth equity investment reached record levels, with \$66.1B invested across 1,057 deals in the U.S. alone.^{lviii} 2018 also saw the largest ever growth equity fundraising with the close of New York-based Insight Venture Partners’ \$6.3B technology-focused growth equity fund.^{lix} This trend may help to fill at least some of Europe’s growth-stage funding gap.

A. Defining Growth Equity

Growth equity (also known as “growth capital” or “expansion capital”) is often referred to as the intersection between venture capital and leveraged buyouts.^{lx} To date, there is no universally accepted definition of growth equity due, in part, to its similarity to other forms of alternative investment. The U.S. National Venture Capital Association (“NVCA”) and its Growth Equity Group have described growth equity as a “critical component” of the venture capital industry, and have defined growth equity investments as those that exhibit some, if not all, of the following characteristics: investors

typically acquire a non-controlling minority interest in the company; investments are often unlevered or use only light leverage; the company is founder-owned and/or founder-managed with a proven business model, positive cash flows and rapidly growing revenues; and invested capital is geared towards company expansion and/or shareholder liquidity, with additional financing rounds typically not expected until the growth equity investor's exit.^{lxi} The European Bank for Reconstruction and Development has defined growth equity in a similar way, but has specifically included mezzanine financing within its definition as a result of private equity investment patterns in the emerging Europe and Central Asia regions, which typically consist of combinations of venture, growth and buyout strategies.^{lxii}

Growth equity investors include, but are not limited to, traditional private equity and venture capital firms that offer growth equity as one of several strategies, specialist growth equity firms, strategic corporate investors, and non-traditional institutional investors, such as pension funds and single family offices, which historically have not invested in emerging companies. In 2018, the 10 most active growth equity investors were Business Growth Fund, Bpifrance, Foresight Group, Warburg Pincus, Kohlberg Kravis Roberts, The Blackstone Group, CM-CIC Investissement, Caisse de dépôt et placement du Québec, TPG Capital and General Atlantic.^{lxiii} Of the 24 most active growth equity investors in 2018, the majority were concentrated in the U.S., France and the UK, respectively.^{lxiv}

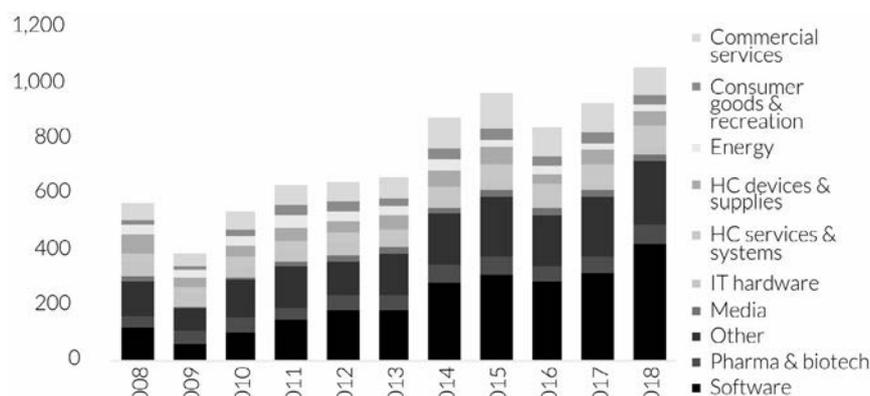
From the company perspective, growth equity investment, in its varying shapes and sizes, fuels later-stage expansion into new product and/or geographic markets, often in preparation for a future merger, acquisition or initial public offering. In contrast to multi-investor early-stage venture financing rounds, growth equity investment may provide the company with the benefit of a higher-stake single investor who can provide strategic business and operational guidance that can translate into greater market share and profitability. This benefit, however, can become a double-edged sword for founders as a result of the growth equity investor's potentially more significant influence over management decisions.

B. Fintech as a Growth Equity Investment Target

From the investor perspective, technology start-ups are considered attractive growth equity investment targets as a result of their perceived revenue stability and high growth potential.^{lxv} Software start-ups in the Fintech sector, in particular, attract strong interest from growth equity investors.^{lxvi} Pitchbook-NVCA Venture Monitor data in the below graph evidences this trend.^{lxvii}

Growth equity deals in software startups increase in 2018

US growth equity deals (#) by industry



Source: Pitchbook-NVCA Venture Monitor (2019)

In the UK alone, growth equity investment in the Fintech sector rose by 57% in 2018 to \$1.6B.^{lxviii} Among the largest UK growth equity investments in Fintech in 2018 were General Atlantic's \$250M investment in lending start-up Greensill Capital^{lxix} and BBVA's £85.4M investment in mobile-banking platform Atom Bank.^{lxx}

The number of growth equity funds that have been formed in Europe has also grown in recent years,^{lxxi} and includes Atlantic Labs' Growth I Fund, Citizen Capital II Fund, Digital+ Partners Digital Growth Fund I and Verdane Capital's ETF III Fund.^{lxxii} Recent examples of European growth equity investments in Fintech include Bridgepoint Capital's lead investment in Kyriba,^{lxxiii} and Vitruvian Partners' lead investments in Deposit Solutions^{lxxiv} and smava.^{lxxv} In the U.S., recent examples of growth equity investments in Fintech include DST Global's lead investment in Chime Bank,^{lxxvi} Edison Partners' lead investment in YieldStreet,^{lxxvii} Great Hill Partners' lead investment in Mineral Tree^{lxxviii} and Goldman Sachs Principal Strategic Investments' lead investment in Nav Technologies.^{lxxix}

With injections of growth equity, Fintech start-ups can deepen their domestic market share, as well as their international reach. Growth equity investment in UK Fintech start-ups, in particular, has fuelled their ambitions to expand into the U.S. market. One such example is UK-based small and medium-sized enterprise lending platform Oak North, which plans to launch in the U.S. in 2019 following a \$440M growth equity investment from Softbank Vision Fund and the Clermont Group.^{lxxx}

Growth equity is projected to continue its upward trend as an investment strategy of choice for later-stage investors in the Fintech sector. With higher levels of growth equity invested in promising Fintech start-ups on both sides of the Atlantic, the transatlantic investment relationship in the Fintech sector is likely to deepen and the strength of the European and U.S. Fintech ecosystems is likely to augment.

IV. Conclusion

With record-breaking levels of Fintech investment in 2018, the European and U.S. Fintech ecosystems continue to grow at remarkable speeds. Notwithstanding the early- and growth-stage financing obstacles that currently limit the scale of the European Fintech financing market, cross-border Fintech investment between the EU and U.S. continues to drive innovation and stimulate economic growth on both sides of the Atlantic. With a rapidly evolving transatlantic Fintech market, cross-border Fintech M&A and IPO activity is likely on the way. Attorneys on both sides of the Atlantic should therefore pay close attention to developments in this space.

Endnotes

- i. For an academic perspective, see Bradley, W. *et al.*, *Cross-Border Venture Capital Investments: What is the Role of Public Policy?*, University of Oxford Saïd Business School WP 2019-02, European Corporate Governance Institute (ECGI) – Finance Working Paper No. 591/2019 (January 2019). Available at: <https://www.law.ox.ac.uk/business-law-blog/blog/2019/02/cross-border-venture-capital-investments-what-role-public-policy>. See also Andrea Schertler, A. and Tykrová, T., *What Lures Cross-Border Venture Capital Inflows?*, Leibniz-Zentrum für Europäische Wirtschaftsforschung (ZEW) Discussion Paper No. 10-001 (January 2010). Available at: <ftp://ftp.zew.de/pub/zew-docs/dp/dp10001.pdf>. For a German industry perspective, see German Private Equity and Venture Capital Association (BVK) *et al.*, *Venture Capital: Fueling innovation and economic growth* (June 2018). Available at: https://www.bvkap.de/sites/default/files/publication/rb_pub_18_019_cop_ief_bvk_online_en_with_publication_date.pdf. For a European industry perspective, see Investment & Pensions Europe (IPE) International Publishers Ltd. (2019), *Venture capital: Venturing further in Europe* (February 2019). Available at: <https://www.ipe.com/investment/asset-class-reports/private-equity/venture-capital-venturing-further-in-europe/10029270.article>. See also Invest Europe, *Innovation boosts Europe's lead as global investment destination* (5 November 2018). Available at: <https://www.investeurope.eu/news-opinion/newsroom/press-releases/2018-global-investment-decision-makers-survey/>.
- ii. See European Commission Directorate-General for Research and Innovation, *Study on Transatlantic Dynamics of New High Growth Innovative Firms* (2016). Available at: <https://publications.europa.eu/en/publication-detail/-/publication/a9b6ac9d-31cc-11e7-9412-01aa75ed71a1/language-en>. See also The German Marshall Fund of the United States, *What do High-Growth Firms in the United States and Europe Teach Policymakers?* (August 2012). Available at: <http://www.gmfus.org/file/2729/download>. For a high-level overview of the economic value of venture capital, see Strebulaev, I. and Gornall, W., *The Economic Impact of Venture Capital: Evidence from Public Companies*, Stanford University Graduate School of Business Research Paper No. 15-55 (2015). Available at: <https://www.gsb.stanford.edu/faculty-research/working-papers/economic-impact-venture-capital-evidence-public-companies>.
- iii. Accenture, *Global Fintech Investments Surged in 2018 with Investments in China Taking the Lead, Accenture Analysis Finds; UK Gains Sharply Despite Brexit Doubts* (25 February 2019). Available at: <https://newsroom.accenture.com/news/global-fintech-investments-surged-in-2018-with-investments-in-china-taking-the-lead-accenture-analysis-finds-uk-gains-sharply-despite-brexit-doubts.htm>.
- iv. CB Insights, *Fintech Trends to Watch in 2019* (February 2019). Available at: <https://www.cbinsights.com/research/report/fintech-trends-2019/>. See also CB Insights, *These Are The Most Active Fintech Investors in 2018* (18 February 2019). Available at: <https://www.cbinsights.com/research/top-fintech-investors-2018/>.
- v. CB Insights, *Fintech Trends to Watch in 2019* (February 2019).
- vi. Fortune, *Cryptocurrency Exchange Circle Valued at Nearly \$3 Billion After Poloniex Deal* (15 May 2018). Available at: <http://fortune.com/2018/05/15/crypto-exchange-circle-bitmain-value/>.
- vii. TechCrunch, *'Software robot' startup UiPath expands Series C to \$265M at a \$3B valuation* (14 November 2018). Available at: <https://techcrunch.com/2018/11/14/software-robot-startup-uipath-expands-series-c-to-265m-at-a-3b-valuation/>.
- viii. CNBC, *Devoted Health, a start-up selling health insurance to seniors, is worth \$1.8 billion* (17 October 2018). Available at: <https://www.cnbc.com/2018/10/17/devoted-health-is-valued-at-1-point8-billion-in-funding-led-by-andreessen.html>.
- ix. Forbes, *Brex Has Amassed A Valuation Of \$1.1 Billion In Under Two Years* (5 October 2018). Available at: <https://www.forbes.com/sites/donnafusco/2018/10/05/brex-has-amassed-a-valuation-of-1-1-billion-in-under-two-years/#15425bbd65a1>.
- x. The Wall Street Journal, *Morgan Stanley Leading Dataminr Round at \$1.2 Billion Pre-Money* (6 June 2018). Available at: <https://www.wsj.com/articles/morgan-stanley-leading-dataminr-round-at-1-2b-pre-money-1528284601>.
- xi. Bloomberg, *Tradecraft Valuation Hits \$1.1 Billion After Pre-IPO Fundraising* (29 May 2018). Available at: <https://www.bloomberg.com/news/articles/2018-05-29/goldman-psp-lead-250-million-funding-round-for-tradecraft>.
- xii. TechCrunch, *A new unicorn is born: Root Insurance raises \$100 million for a \$1 billion valuation* (22 August 2018). Available at: <https://techcrunch.com/2018/08/22/a-new-unicorn-is-born-root-insurance-raises-100-million-for-a-1-billion-valuation/>.
- xiii. CNBC, *Revolut becomes latest fintech unicorn after \$250 million funding gives it a \$1.7 billion valuation* (26 April 2018). Available at: <https://www.cnbc.com/2018/04/26/revolut-raises-250-million-in-funding-at-1-point-7-billion-valuation.html>. See also Reuters, *Revolut becomes Britain's first digital bank unicorn* (26 April 2018). Available at: <https://www.reuters.com/article/us-fintech-revolut-funding/revolut-becomes-britains-first-digital-bank-unicorn-idUSKBN1HX0MZ>.
- xiv. TechCrunch, *Monzo, the UK challenger bank, raises £85M Series E at a £1B pre-money valuation* (30 October 2018). Available at: <https://techcrunch.com/2018/10/30/monzocorn/>.
- xv. CB Insights, *Fintech Trends to Watch in 2019* (February 2019).
- xvi. Accenture (25 February 2019).
- xvii. Wall Street Journal, *Jack Ma's Ant Financial Valued Around \$150 Billion After Funding Round* (7 June 2018). Available at: <https://www.wsj.com/articles/jack-mas-ant-financial-raises-14-billion-1528428455>. See also Accenture (25 February 2019).
- xviii. Accenture (25 February 2019).
- xix. *Id.*
- xx. Forbes, *Cross-Border Student Loan Lender Prodigy Finance Raises \$1B In Debt Financing* (24 September 2018). Available at: <https://www.forbes.com/sites/donnafusco/2018/09/24/cross-border-student-loan-lender-prodigy-finance-raises-1b-in-debt-financing/>. See also Prodigy Finance, *US\$1 billion in debt financing supports accelerated international student growth* (24 September 2018). Available at: <https://prodigyfinance.com/resources/blog/1-billion-debt-financing-2018>.
- xxi. CNBC, *Revolut becomes latest fintech unicorn after \$250 million funding gives it a \$1.7 billion valuation* (26 April 2018). Available at: <https://www.cnbc.com/2018/04/26/revolut-raises-250-million-in-funding-at-1-point-7-billion-valuation.html>.
- xxii. Financial Times, *Atom Bank in £149m capital raising* (7 March 2018). Available at: <https://www.ft.com/content/9dd3f234-21e3-11e8-add1-0e8958b189ea>. See also Finextra, *BBVA raises Atom Bank stake to 39% as part of £149 million funding round* (7 March 2018). Available at: <https://www.finextra.com/newsarticle/31778/bbva-raises-atom-bank-stake-to-39-as-part-of-149-million-funding-round>.
- xxiii. TechCrunch, *Monzo, the UK challenger bank, raises £85M Series E at a £1B pre-money valuation* (30 October 2018).

- Available at: <https://techcrunch.com/2018/10/30/monzocorn/>. See also The Telegraph, *Monzo raises £85m to become UK's latest tech 'unicorn'* (31 October 2018). Available at: <https://www.telegraph.co.uk/technology/2018/10/31/monzo-raises-85m-become-uks-latest-tech-unicorn/>.
- xxiv. CB Insights, *Fintech Trends to Watch in 2019* (February 2019). See also Accenture (25 February 2019).
- xxv. CB Insights, *Fintech Trends to Watch in 2019* (February 2019).
- xxvi. Financial Technology Partners, *Annual 2018 Fintech Almanac: Financing & M&A Statistics* (February 2019). Available at: <https://www.ftpartners.com/Fintech-research/almanac>.
- xxvii. ABN AMRO, *ABN AMRO Digital Impact Fund invests in German fintech solarisBank* (8 March 2018). Available at: <https://www.abnamro.com/en/newsroom/press-releases/2018/abn-amro-digital-impact-fund-invests-in-german-fintech-solarisbank.html>.
- xxviii. BBVA, *BBVA backs UK banking disruptor Atom with further investment* (7 March 2018). Available at: <https://www.bbva.com/en/bbva-backs-uk-banking-disruptor-atom-further-investment/>.
- xxix. Robinhood Blog, *Robinhood Raises \$363 Million to Expand Product Lineup* (10 May 2018). Available at: <https://blog.robinhood.com/news/2018/5/9/robinhood-raises-363-million-to-expand-product-lineup>.
- xxx. New York Business Journal, *This week in NYC funding news: The top VC rounds of 2018* (28 December 2018). Available at: <https://www.bizjournals.com/newyork/news/2018/12/28/this-week-nyc-funding-news-the-top-vc-rounds-2018.html>.
- xxxi. CB Insights, *30 Corporate Innovation Labs in Finance* (2018). Available at: <https://www.cbinsights.com/research/report/finance-corporate-innovation-labs/>.
- xxxii. *Id.*
- xxxiii. CB Insights, *The 2018 Global Corporate Venture Capital Report* (28 March 2019). Available at: <https://www.cbinsights.com/research/report/corporate-venture-capital-trends-2018/>. See also The American Banker, *Why Venture Capitalists Love Fintechs* (10 February 2019). Available at: <https://www.americanbanker.com/list/why-venture-capitalists-love-fintechs>.
- xxxiv. See Kaplan, S. and Lerner, J., *It Ain't Broke: The Past, Present, and Future of Venture Capital*, Journal of Applied Corporate Finance, Vol. 22, No. 2 (Spring 2010). Available at: <http://www.people.hbs.edu/jlerner/kaplanlerner.jacf.pdf>.
- xxxv. Financial Times, *European Venture Capital Groups Struggle to Attract Investors* (7 February 2008). Available at: <https://www.ft.com/content/845f5cb0-0c19-11e8-839d-41ca06376bf2>. See also Bloomberg, *Why Can't Europe Do Tech* (15 August 2018). Available at: <https://www.bloomberg.com/news/features/2018-08-16/inside-europe-s-struggle-to-build-a-truly-global-tech-giant>.
- xxxvi. German Private Equity and Venture Capital Association (BVK) *et al.* (June 2018).
- xxxvii. German Private Equity and Venture Capital Association (BVK) *et al.* (June 2018).
- xxxviii. European Commission, *VentureEU: €2.1 billion to boost venture capital investment in Europe's innovative start-ups* (10 April 2018). Available at: http://europa.eu/rapid/press-release_IP-18-2763_en.pdf. See also Invest Europe, *EU venture capital programme a 'great step forward', says Invest Europe* (10 April 2018). Available at: <https://www.investeurope.eu/news-opinion/newsroom/press-releases/vc-fof/>.
- xxxix. See Quartz, *Germans don't do tech startups — more access to capital might change that* (30 September 2018). Available at: <https://qz.com/1404647/germans-dont-do-tech-startups-more-access-to-capital-might-change-that/>.
- xl. PitchBook, *The top 11 VC investors in German startups* (14 June 2018). Available at: <https://pitchbook.com/news/articles/the-top-11-vc-investors-in-german-startups>.
- xli. High-Tech Gründerfonds, *A powerful motor for innovation and the economy: High-Tech Gründerfonds makes its 500th investment* (28 June 2018). Available at: <https://high-tech-gruenderfonds.de/en/a-powerful-motor-for-innovation-and-the-economy-high-tech-gruenderfonds-makes-its-500th-investment/>.
- xlii. High-Tech Gründerfonds, *Coinlend receives HTGF seed funding for its AI-based lending platform tailored to the cryptocurrency market* (27 March 2019). Available at: <https://high-tech-gruenderfonds.de/en/coinlend-receives-htgf-seed-funding-for-its-ai-based-lending-platform-tailored-to-the-cryptocurrency-market/>. See also EU-Start-ups.com, *High-Tech Gründerfonds makes and celebrates its 500th investment (Sponsored)* (18 June 2018). Available at: <https://www.eu-startups.com/2018/06/high-tech-gruenderfonds-makes-and-celebrates-its-500th-investment-sponsored/>.
- xliii. High-Tech Gründerfonds, *Berlin-based Fintech start-up remind.me secures seed financing* (24 May 2018). Available at: <https://high-tech-gruenderfonds.de/en/berlin-based-Fintech-start-up-remind-me-secures-seed-financing/>.
- xliv. High-Tech Gründerfonds, *New HTGF Fintech investment troy revolutionizes the debt collection process and combines machine learning with friendliness* (3 September 2018). Available at: <https://high-tech-gruenderfonds.de/en/new-htgf-fintech-investment-troy-revolutionizes-the-debt-collection-process-and-combines-machine-learning-with-friendliness/>.
- xlv. High-Tech Gründerfonds, *Iconiq Holding closes a seven-figure financing round as FinLab increases its stake and Germany's largest VC, High-Tech Gründerfonds, invests* (22 January 2019). Available at: <https://high-tech-gruenderfonds.de/en/iconiq-holding-closes-a-seven-figure-financing-round-as-finlab-increases-its-stake-and-germanys-largest-vc-high-tech-gruenderfonds-invests/>.
- xlvi. High-Tech Gründerfonds, *Frankfurt blockchain start-up Agora Innovation secures high six-figure investment from High-Tech Gründerfonds* (25 February 2019). Available at: <https://high-tech-gruenderfonds.de/en/frankfurt-blockchain-start-up-agera-innovation-secures-high-six-figure-investment-from-high-tech-gruenderfonds/>.
- xlvii. European Commission, *VentureEU: Pan-European Venture Capital Funds-of-Funds Programme: Frequently asked questions* (10 April 2018). Available at: https://europa.eu/rapid/press-release_MEMO-18-2764_en.pdf.
- xlviii. European Commission, *VentureEU: €2.1 billion to boost venture capital investment in Europe's innovative start-ups* (10 April 2018).
- xlix. European Commission, *Start-ups and Scale-Ups: The Wide EU Ecosystem* (2018). Available at: <http://europa.eu/rapid/attachment/IP-18-2763/en/Factsheet%20VentureEU-EU%20ecosystem.pdf>.
1. European Commission, *VentureEU: €2.1 billion to boost venture capital investment in Europe's innovative start-ups* (10 April 2018).
- li. The European Investment Fund, *European Investment Fund (EIB Group) and Axis launch new investment fund for financing innovative firms in Spain* (21 March 2019). Available at: https://www.eif.org/what_we_do/equity/news/2019/axis-investment-fund-spain.htm.
- lii. European Investment Fund, *European Angels Fund (EAF)*. Available at: https://www.eif.org/what_we_do/equity/eaf/index.htm.

- liii. European Investment Fund, *European Investment Fund and Fraunhofer join forces to establish joint technology transfer fund in Germany* (26 February 2019). Available at: https://www.eif.org/what_we_do/equity/news/2019/fraunhofer-efsi-innovfin.htm. See also European Investment Fund, *InnovFin – EU Finance for innovators*. Available at: <https://www.eib.org/en/products/blending/innovfin/index.htm>.
- liv. European Investment Fund (26 February 2019).
- lv. German Private Equity and Venture Capital Association (BVK) *et al.* (June 2018). Available at: https://www.bvkap.de/sites/default/files/publication/rb_pub_18_019_cop_ief_bvk_online_en_with_publication_date.pdf.
- lvi. *Id.*
- lvii. Preqin, *Growth Equity: Return Expectations and Prospects in Growth PE Investing* (15 November 2017).
- lviii. PitchBook, *4Q 2018 Pitchbook–NVCA Venture Monitor* (2019). Available at: <https://pitchbook.com/news/reports/4q-2018-pitchbook-nvca-venture-monitor>.
- lix. PitchBook, *3Q 2018 US PE Breakdown* (2018). Available at: <https://pitchbook.com/news/reports/3q-2018-us-pe-breakdown>. Insight Venture Partners, *Software Investor Insight Venture Partners Closes \$6.3 Billion Fund X* (19 July 2018). Available at: <https://www.insightpartners.com/about-us/news-press/software-investor-insight-venture-partners-closes-6-3-billion-fund-x/>.
- lx. PitchBook, *3Q 2018 US PE Breakdown* (2018).
- lxi. National Venture Capital Association Growth Equity Group, *Defining Growth Equity Investments*. Available at: <https://nvca.org/growth-equity-group/>.
- lxii. European Bank for Reconstruction and Development, *EBRD Transition Report 2015-16* (2015). Available at: <https://www.ebrd.com/news/publications/transition-report/ebrd-transition-report-201516.html>.
- lxiii. PitchBook, *2018 Annual Global League Tables* (31 January 2019). Available at: <https://pitchbook.com/news/reports/2018-annual-global-league-tables>.
- lxiv. *Id.*
- lxv. PitchBook, *1Q 2018 Pitchbook–NVCA Venture Monitor* (9 April 2018). Available at: <https://pitchbook.com/news/reports/1q-2018-pitchbook-nvca-venture-monitor>.
- lxvi. American Banker, *Money Keeps Flowing to Fintechs* (14 March 2019). Available at: <https://www.americanbanker.com/list/money-keeps-flowing-to-fintechs>.
- lxvii. PitchBook, *4Q 2018 Pitchbook–NVCA Venture Monitor* (2019).
- lxviii. Innovate Finance, *2018 Fintech VC Investment Landscape* (2019). Available at: <https://cdn2.hubspot.net/hubfs/5169784/Innovate-Finance-2018-FinTech-VC-Investment-Landscape.pdf>.
- lxix. General Atlantic, *General Atlantic Announces Strategic Investment in Greensill* (16 July 2018). Available at: <https://www.generalatlantic.com/media-article/general-atlantic-announces-strategic-investment-in-greensill/>. See also *The Wall Street Journal*, *General Atlantic Invests \$250 Million in Lending Startup Greensill* (16 July 2018). Available at: <https://www.wsj.com/articles/general-atlantic-invests-250-million-in-lending-startup-greensill-1531713660>.
- lxx. BBVA, *BBVA backs UK banking disruptor Atom with further investment* (7 March 2018). Available at: <https://www.bbva.com/en/bbva-backs-uk-banking-disruptor-atom-further-investment/>. See also BBVA, *BBVA completes £85.4m investment into UK Digital bank Atom, increasing stake to 39%* (1 June 2018). Available at: <https://www.bbva.com/en/bbva-completes-85-4m-investment-uk-digital-bank-atom-increasing-stake-39/>.
- lxxi. Invest Europe, *2017 European Private Equity Activity*, 2 May 2018. Available at: <https://www.investeurope.eu/media/711867/invest-europe-2017-european-private-equity-activity.pdf>. See also Preqin, *The Rise Of Venture And Growth Capital In Europe* (9 August 2018). Available at: <https://www.valuewalk.com/2018/08/rise-venture-growth-capital-europe/>.
- lxxii. European Investment Fund, *Signed Equity deals as of 30/06/2018* (2018). Available at: https://www.eif.org/what_we_do/equity/eif-equity-portfolio.pdf.
- lxxiii. Bridgepoint, *Bridgepoint to acquire Kyriba* (28 March 2019). Available at: <http://www.bridgepoint.eu/en/news/press-releases/2019/bridgepoint-to-acquire-kyriba/>. See also *San Diego Business Journal*, *Kyriba to Become San Diego's Next Unicorn with \$160M Investment* (27 March 2019). Available at: <https://www.sdbj.com/news/2019/mar/27/kyriba-become-san-diegos-next-unicorn-160m-investm/>.
- lxxiv. Business Insider, *A German fintech startup backed by Peter Thiel has raised \$100 million* (16 August 2018). Available at: <http://www.businessinsider.com/german-fintech-deposit-solutions-raises-100-million-2018-8>. See also *Financial Partners*, *FT Partners Advises Vitruvian on its Investment in Deposit Solutions* (15 August 2018). Available at: <https://www.fpartners.com/transactions/vitruvian>.
- lxxv. smava, *smava receives \$65 million investment led by Vitruvian Partners* (9 January 2018). Available at: <https://www.smava.de/presse/pressemitteilungen/smava-receives-65-million-investment/>. See also *Reuters*, *Vitruvian puts German fintech Smava up for sale: sources* (13 February 2019). Available at: <https://www.reuters.com/article/us-vitruvian-smava-divestiture-idUSKCN1Q2194>.
- lxxvi. Bloomberg, *Online Bank Chime Is Close to New Funding at a \$1.5 Billion Value* (5 February 2019). Available at: <https://www.bloomberg.com/news/articles/2019-02-05/online-bank-chime-is-said-to-near-funding-at-1-5-billion-value>. See also *Forbes*, *Chime Raises \$200 Million At \$1.5 Billion Valuation* (5 March 2019). Available at: <https://www.forbes.com/sites/donnafuscaldolo/2019/03/05/chime-raises-200-million-at-1-5-billion-valuation/>.
- lxxvii. Edison Partners, *Edison Partners Leads \$62 Million Investment in YieldStreet* (26 February 2019). Available at: <https://www.edisonpartners.com/blog/yieldstreet-investment>. See also *Forbes*, *YieldStreet Raises \$62M To Bring Alternative Investing To The Masses* (26 February 2019). Available at: <https://www.forbes.com/sites/donnafuscaldolo/2019/02/26/yieldstreet-raises-62m-to-bring-alternative-investing-to-the-masses/>.
- lxxviii. Great Hill Partners, *MineralTree Closes \$50 Million Growth Financing* (28 March 2019). Available at: <https://www.greathillpartners.com/mineraltree-closes-50-million-growth-financing/>. See also *Boston Business Journal*, *Cambridge fintech firm MineralTree closes \$50M round led by Great Hill Partners* (27 March 2019). Available at: <https://www.bizjournals.com/boston/news/2019/03/27/cambridge-fintech-firm-mineraltree-closes-50m.html>.
- lxxix. *Reuters*, *Goldman Sachs, Point72 and others invest \$44 million in business credit startup Nav* (11 February 2019). Available at: <https://www.reuters.com/article/us-nav-investment-goldman-sachs-idUSKCN1Q01BJ>.
- lxxx. CNBC, *SoftBank leads \$440 million investment in UK fintech OakNorth, valuing it at \$2.8 billion* (8 February 2019). Available at: <https://uk.finance.yahoo.com/news/softbank-apos-vision-fund-pumps-100413059.html>. See also *Finextra*, *OakNorth raises \$440 million for US expansion* (8 February 2019). Available at: <https://www.finextra.com/newsarticle/33346/oaknorth-raises-440-million-for-us-expansion>.

Acknowledgment

The author would like to thank the Transatlantic Technology Law Forum at Stanford Law School for its encouragement in the undertaking of comparative and international academic research on venture capital financing of Fintech.

Disclaimer

The views and opinions expressed in this chapter are those of the author alone, and do not necessarily reflect the views of Stanford University, the University of Vienna, the American Bar Association or Crowell & Moring LLP. The material in this chapter has been prepared for informational purposes only and is not intended to serve as legal or investment advice.



Jonathan Cardenas

Stanford Law School
559 Nathan Abbott Way
Stanford, CA 94305
USA

Tel: +1 650 723 2465
URL: www.law.stanford.edu

Jonathan Cardenas is a Fellow with the Transatlantic Technology Law Forum at Stanford Law School. He is a former Visiting Fellow at Yale Law School's Information Society Project, and a former visiting researcher at the Swiss Federal Institute of Technology ("ETH Zürich") Center for Law & Economics. He serves as Founding Chair of the Financial Services Technology Joint Subcommittee within the Commercial Finance Committee and Private Equity & Venture Capital Committee of the American Bar Association's Business Law Section.

Jonathan received his J.D. from New York University School of Law, where he was a Jacobson Leadership Program in Law & Business Scholar, and where he served as a Managing Editor of the NYU Journal of Law & Business. He received an M.Phil. in International Relations from the University of Cambridge, and a B.A. in Political Science, *summa cum laude*, from the University of Pennsylvania.

Jonathan is admitted as an attorney in the District of Columbia, the State of Florida, and the State of New York. He practises law as a corporate associate with Crowell & Moring LLP in Washington, D.C.



Funded by a generous grant from the Microsoft Corporation, the Transatlantic Technology Law Forum ("TTLF") aims to promote a balanced approach to today's and future transatlantic tech law issues and to focus scholarly attention on these issues by involving academics, businesspeople, government officials, legal professionals, legislators, policy makers, representatives of international organisations, scholars, students and the public at large from both sides of the Atlantic. The TTLF's institutional framework is co-sponsored and operated by the Stanford Law School Program in Law, Science & Technology and the University of Vienna School of Law, which established TTLF jointly in a transatlantic academic partnership in 2004. The TTLF serves as a coordinating and working platform for a series of institutionally open transatlantic tech law projects. A number of American and European universities and other academic institutions as well as international organisations are actively involved in TTLF projects.

Australia

Gilbert + Tobin

Peter Reeves



1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Australia has seen a continued proliferation of active fintech businesses over the past year.

Investments in insurance technology have grown, with companies and fintechs increasing their focus on forging cross-sector alliances in order to embed their offerings into other value propositions. The increase in partnerships and alliances between insurance fintechs and incumbents with established customer bases will be particularly effective for insurance start-ups to fuel expansion.

The growing cost of compliance has pushed many companies to invest in regulatory technology, or regtech, particularly in areas including artificial intelligence (AI), customer due diligence (e.g., ‘know-your-customer’) and data breach monitoring (e.g., ‘know-your-data’).

In May 2018, the Australian Prudential Regulation Authority (APRA) granted its first restricted authorised deposit-taking institution (ADI) licence, which is designed to facilitate new businesses entering the banking industry.

There has also been a steady increase in Australian consumers’ preference of electronic payment methods over cash payments and, subsequently, a rise in the establishment of non-cash payment platforms and solutions aimed at maximising cost and time efficiencies and improving consumer experience. The New Payments Platform (NPP) was launched in Australia in February 2018 as the result of industry-wide collaboration between Australia’s largest banks and financial institutions as well as Australia’s central bank, the Reserve Bank of Australia (RBA). The NPP is a payments infrastructure that enables Australian consumers, businesses and government agencies to make real-time, data-rich payments between accounts with participating financial institutions. Over time, the NPP is expected to replace a significant portion of direct payments made between consumers’ bank accounts, particularly those which are time-critical or benefit from additional data capabilities.

Further, there has been sustained attention on blockchain technology, and a growth in interest in the technology by established businesses. Fintech businesses have begun moving beyond the proof-of-concept stage to formalising actual use cases for distributed ledger technology

such as managing supply chains, making cross-border payments, trading derivatives, managing assets and digital currency exchanges. Notably, the Australian Securities Exchange (ASX) is progressing with its plans to adopt a blockchain-based technology for its clearing and settlement process to replace its current system. The ASX is currently conducting internal analysis and testing of the technology which is set to conclude at the end of August 2020, with the implementation of the new system scheduled for March 2021.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

At the time of writing, there have not been any prohibitions or restrictions on specific fintech business types. Cryptocurrency-based businesses are permitted in Australia, provided such businesses comply with applicable laws (including financial services and consumer laws).

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

Equity Funding

Businesses can raise equity using traditional private and public fundraising methods (e.g., private placement; initial public offering; seed and venture capital strategies), through grants and initiatives offered by Government and State/Territory agencies, and through crowdfunding.

In late 2017, a regulatory framework was introduced for crowd-sourced equity funding (CSEF) by public companies from retail investors. While reducing the regulatory barriers to investing in small and start-up businesses, the framework also created certain licensing and disclosure obligations for CSEF intermediaries (i.e., persons listing CSEF offers for public companies).

Under the CSEF framework, there are exemptions for persons operating markets and clearing and settlement facilities from the licensing regimes that would otherwise be applicable to those facilities. These additional exemptions provide a means by which a person operating a platform for secondary trading can seek an exemption with tailored conditions from more onerous licensing requirements.

On 19 October 2018, the *Corporations Amendment (Crowd-sourced Funding for Proprietary Companies) Act 2018* (Cth) came into effect, which further extended the CSEF regime to also apply to proprietary companies. While there are a range of reporting requirements imposed on proprietary companies engaging in crowdfunding, there are also a number of concessions made with respect to restrictions that would otherwise apply to their fundraising activities.

The Australian Securities and Investments Commission (ASIC), Australia's corporate regulator, has released Regulatory Guides 261 and 262 to assist companies seeking to raise funds through CSEF and intermediaries seeking to provide CSEF services, respectively.

Debt Funding

There have been calls to extend the existing crowdfunding framework to debt funding, and the Australian Government (Government) has previously indicated it intends to consult on this. Debt financing is less common than equity financing in the Australian fintech sector; however, businesses can approach financial institutions, suppliers and finance companies in relation to debt finance.

Initial Coin Offerings (ICOs) and Security Token Offerings (STOs)

Over the past two years, ICOs have become a popular method of funding for blockchain or cryptocurrency-related projects, where token issuers offer tokens in return for funds. In May 2018, ASIC updated its *INFO 225 Initial coin offerings* guidance on the potential application of the *Corporations Act 2001* (Cth) (Corporations Act) to ICOs. Entities should note that the Corporations Act may apply regardless of whether the ICO was created and offered from Australia or overseas.

Generally, ASIC has indicated that the legal status of an ICO depends on the ICO's structure, operation, and the rights attached to the tokens offered in the ICO. Tokens offered during the ICO may trigger licensing, registration and disclosure requirements if the tokens represent financial products (e.g., interests in managed investment schemes, securities, derivatives or non-cash payment facilities). A company participating in a cryptocurrency exchange as a market maker may also be required to hold an Australian financial services licence (AFSL), and an operator of a cryptocurrency exchange may require an Australian market licence (AML), in each case where the relevant tokens constitute financial products.

Given the likelihood that many cryptocurrency-related funding rounds will be considered an offering of a financial product, there is a growing trend for offerors to pre-emptively step into the regulatory framework by means of an STO. This is where companies will knowingly offer financial products (usually represented in a digital form) and therefore comply with all applicable licensing, registration and disclosure requirements applicable to an offer of regulated products.

Regardless of whether a token constitutes a financial product, ICOs and STOs will be subject to the *Australian Consumer Law*, which includes a general prohibition on misleading or deceptive conduct in relation to the offer of services or products. In May 2018, ASIC received a delegation of power from the Australian Competition and Consumer Commission (ACCC), enabling it to take action where there is potential misleading and deceptive conduct associated with such offerings.

Asia Region Funds Passport and Corporate Collective Investment Vehicles

In 2018, the Government passed the *Corporations Amendment (Asia Region Funds Passport) Bill 2018*, which brought into effect the Asia Region Funds Passport (Passport). The Passport is a region-wide initiative designed to facilitate the offer of interests in certain collective investment schemes (CIS), established in Passport member economies, to investors in other Passport member economies. It aims

to provide Australian fund managers and operators with greater access to economies in the Asia-Pacific region by reducing regulatory hurdles.

At the time of writing, the final stages of consultation and implementation are being entered into in relation to the Corporate Collective Investment Vehicle (CCIV) scheme. The CCIV scheme creates a new type of investment vehicle, which will allow Australian fund managers to pursue overseas investment opportunities through a company structure. It is intended to complement the Passport by making Australian funds more accessible to foreign investors.

The Australian funds market is dominated by unit trusts, a structure that is unfamiliar to many offshore economies where corporate and limited partnership investment vehicles are the norm throughout the Asia-Pacific region. The CCIV will provide an internationally recognised investment vehicle which will be able to be more readily marketed to foreign investors (including through the Passport).

There are concerns that the reforms will add extra complexity, given the far-reaching potential changes to corporate, partnership and tax laws. However, the enactment of the Passport and the CCIV may lead to new financing opportunities for fintech businesses.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

Incentives for investors

(1) Early stage innovation company incentives

Incentives are available for eligible investments made in start-ups known as Early Stage Innovation Companies (ESICs), which are generally newly incorporated entities with low income and expenses.

Investments of less than 30% of the equity in an ESIC would generally qualify for a 20% non-refundable tax offset (capped at AUD 200,000 per investor, including any offsets carried forward from the prior year's investment) and a 10-year tax exemption on any capital gains arising on disposal of the investment.

(2) Eligible venture capital limited partnerships

Fintech investment vehicles may be structured as venture capital limited partnerships (VCLPs) or early stage venture capital limited partnerships (ESVCLPs), and receive favourable tax treatment for eligible venture capital investments.

For VCLPs, benefits include tax exemptions for foreign investors (limited partners) on their share of any revenue or capital gains made on disposal of the investment by the VCLP, and concessional treatment of the fund manager's carried interest in the VCLP. For ESVCLPs, the income tax exemption for VCLPs is extended to both resident and non-resident investors, plus investors obtain a 10% non-refundable tax offset for new capital invested in the ESVCLP.

Incentives for fintechs

The Research & Development (R&D) Tax Incentive programme is available for entities incurring eligible expenditure on R&D activities, which includes certain software R&D activities commonly conducted by fintechs. Claimants under the R&D Tax Incentive may be eligible for:

- (a) *Small businesses (less than AUD 20 million aggregated turnover):* a 43.5% refundable tax offset.
- (b) *Other businesses:* a 38.5% non-refundable tax offset for eligible expenditure below AUD 100 million and 30% for eligible expenditure over AUD 100 million.

It should be noted that significant changes to the R&D Tax Incentive programme were announced as part of the Federal Budget on 8 May 2018. The major change is expected to include the introduction of an “incremental intensity threshold” that will increase the tax offset available to large businesses, based on the proportion of their eligible R&D expenditure as a percentage of total business expenditure. At the time of writing, the laws establishing these changes are yet to be enacted.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

The ASX sets out 20 conditions to be satisfied in its Listing Rules. Briefly, these include the entity having at least 300 non-affiliated security holders each holding the value of at least AUD 2,000, and the entity satisfying either the profit test or the assets test (which requires particular financial thresholds to be met).

At the time of writing, the ASX is undertaking a consultation process which may result in the streamlining of the listing requirements.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

In 2018, Avoka Technologies (**Avoka**) was acquired by Swiss banking software company, Temenos, for AUD 339 million. Avoka is a leading Australian-based provider of customer acquisition services to financial institutions, offering a software-as-a-service platform which enables institutions to launch new digital products and monitors customer interaction. The transaction represented one of the biggest exits by a fintech start-up in Australia.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

Broadly, the regulatory framework that applies to fintech businesses includes financial services and consumer credit licensing, registration and disclosure obligations, consumer law requirements and anti-money laundering and counter-terrorism financing requirements.

Licensing obligations apply to entities that carry on a financial services business in Australia or engage in consumer credit activities. The definitions of *financial service* and *financial product* are broad, and will generally capture any investment or wealth management business, payment service (e.g., non-cash payment facility), advisory business (including robo-advice), trading platform, and crowdfunding platform, triggering the requirement to hold an AFSL or be entitled to rely on an exemption. Similarly, engaging in peer-to-peer lending activities will generally constitute consumer credit activities and trigger the requirement to hold an Australian credit licence (**ACL**) or be entitled to rely on an exemption.

Fintech businesses may also need to hold an AML where they operate a facility through which offers to buy and sell financial products are regularly made and accepted (e.g., an exchange). If an entity operates a clearing and settlement mechanism which enables parties transacting in financial products to meet obligations to each other, the entity must hold a clearing and settlement (**CS**) facility licence or otherwise be exempt.

The *Australian Consumer Law* applies to all Australian businesses that engage or contract with consumers. Obligations include a

general prohibition on misleading and deceptive conduct, false or misleading representations, unconscionable conduct and unfair contract terms in relation to the offer of services or products.

The *Anti-money Laundering and Counter-terrorism Financing Act 2006* (Cth) (**AML/CTF Act**) applies to entities that provide “designated services” with an Australian connection. Generally, the AML/CTF Act applies to any entity that engages in financial services or credit (consumer or business) activities in Australia. Obligations include enrolment with the Australian Transaction Reports and Analysis Centre (**AUSTRAC**), reporting and customer due diligence.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

At the time of writing, there are no laws in Australia that have been implemented to specifically regulate cryptocurrencies or cryptoassets. Generally, the predominant focus on the regulation of cryptocurrencies has revolved around its application to the established financial services regulatory framework.

Currently, the only formal monitoring of cryptocurrency activity in Australia is in relation to anti-money laundering and counter-terrorism financing (**AML/CTF**), discussed in further detail in question 4.5.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

Regulators in Australia have been receptive to the entrance of fintechs and technology-focussed businesses. The financial services regulatory regime adopts a technology-neutral approach, whereby services will be regulated equally, irrespective of the method of delivery. However, further concessions have been made by regulators in order to support technologically-focussed start-ups entering the market.

In December 2016, ASIC made certain class orders establishing a fintech licensing exemption and released *Regulatory Guide 257*, which details ASIC’s framework for fintech businesses to test certain financial services, financial products and credit activities without holding an AFSL or ACL by relying on the class orders (referred to as the regulatory sandbox). There are strict eligibility requirements for both the type of businesses who can enter the regulatory sandbox and the products and services that qualify for the licensing exemption. Once a fintech business accesses the regulatory sandbox, there are restrictions on how many persons can be provided with a financial product or service and caps on the value of the financial products or services which can be provided.

Regulators have also committed to helping fintech businesses more broadly by streamlining access and offering informal guidance to enhance regulatory understanding. Both ASIC and AUSTRAC have established Innovation Hubs to assist start-ups in navigating the Australian regulatory regime. AUSTRAC’s Fintel Alliance has an Innovation Hub targeted at combatting money-laundering and terrorism-financing and improving the fintech sector’s relationship with Government and regulators.

ASIC has also entered into a number of cooperation agreements with overseas regulators under which there is a cross-sharing of information on fintech market trends, encouraging referrals of fintech companies and sharing insights from proofs of concepts and

innovation competitions. It is also the intention of a number of these agreements to further understand the approach to regulation of fintech businesses in other jurisdictions, in an attempt to better align the treatment of these businesses across jurisdictions.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

Regulatory hurdles to overcome in order to access Australian customers include registering with ASIC in order to carry on a business in Australia (generally satisfied by incorporating a local subsidiary or registering a branch office), satisfying applicable licensing, registration and disclosure requirements if providing financial services or engaging in consumer credit activities in Australia (or qualifying to rely on an exemption to such requirements), and complying with the AML/CTF regime. Broadly, these regulatory hurdles are determined by the extent to which the provider wishes to establish an Australian presence, the types of financial products and services provided, and the type of Australian investors targeted.

It has been common for foreign financial services providers (FFSPs) to provide financial services to wholesale clients in Australia by relying on ASIC's "passport" or "limited connection" relief from the requirement to hold an AFSL. However, ASIC recently announced that it will be repealing the passport relief and limited connection relief, and instead will implement a new regime requiring FFSPs to apply for a foreign AFSL. It is expected that the new regime will apply from 30 September 2019.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

The Privacy Act

In Australia, the *Privacy Act 1988* (Cth) (**Privacy Act**) regulates the handling of personal information by Government agencies and private sector organisations with an aggregate group revenue of at least AUD 3 million. In some instances, the Privacy Act will apply to businesses (e.g., credit providers and credit reporting bodies) regardless of turnover.

The Privacy Act includes 13 Australian Privacy Principles (APPs), which impose obligations on the collection, use, disclosure, retention and destruction of personal information.

The Notifiable Data Breaches (NDB) scheme was introduced in 2018. The NDB scheme mandates that entities regulated under the Privacy Act are required to notify any affected individuals and the Office of the Australian Information Commissioner (OAIC) in the event of a data breach (i.e., unauthorised access to or disclosure of information) which is likely to result in serious harm to those individuals. The NDB scheme applies to agencies and organisations that the Privacy Act requires to take steps to secure certain categories of personal information.

Consumer data right and access

In response to the Productivity Commission's report on Data Availability and Use, the Government will be implementing the

national consumer data right (CDR) framework which will give customers a right to share their data with accredited service providers (including banks, comparison services, fintechs or third parties), encouraging the flow of information in the economy and competition within the market. The CDR framework will first be applied to the banking sector under the "Open Banking" regime, whereby consumers will be able to exercise greater access and control over their banking data. These sharing arrangements are intended to facilitate easier swapping of service providers, enhancement of customer experience based on personal and aggregated data, and more personalised offerings. The Open Banking regime is slated to commence in February 2020.

Additionally, it is worth noting that the European Union (EU) General Data Protection Regulation has extremely broad extra-territorial reach and may significantly impact the data handling practices of Australian businesses offering goods and services in the EU.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

The Privacy Act has extraterritorial operation and extends to acts undertaken outside Australia and its external territories where there is an "Australian link" (i.e., where the organisation is an Australian citizen or organisation) or carries on a business in Australia and collects personal information in Australia.

Under the framework for cross-border disclosure of personal information, APP entities must take reasonable steps to ensure that overseas recipients handle personal information in accordance with the APPs, and the APP entity is accountable if the overseas recipient mishandles the information. The APP entity must also only disclose information for the primary purpose for which it was collected.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

The Privacy Act confers on the OAIC a variety of investigative and enforcement powers to use in cases where a privacy breach has occurred, including:

- the power to investigate a matter following a complaint or on the OAIC's own initiative;
- the power to make a determination requiring the payment of compensation or other remedies, such as the provision of access or the issuance of an apology;
- enforceable undertakings;
- seeking an injunction; and
- seeking civil penalties of up to AUD 420,000 for individuals and up to AUD 2.1 million for bodies corporate.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

Cyber security regulation has been a key focus of regulators given the rapid innovation in the fintech space and the interplay between financial services, financial products and new technologies. ASIC provides a number of resources to help firms improve their cyber resilience, including reports, articles and practice guides.

ASIC provides guidance regarding cyber security in *Report 429 Cyber Resilience – Health Check and Report 555: Cyber resilience of firms in Australia's financial market*. In these reports, ASIC has examined and provided examples of good practices identified across

the financial services industry and questions board members and senior management of financial organisations should ask when considering their cyber resilience. ASIC's *Regulatory Guide 255* also set out the standards and frameworks which providers of digital advice should test their information security arrangements against, and nominated frameworks set out relevant compliance measures which should be put in place where cloud computing is relied upon.

As part of the Government's Cyber Security Strategy, CERT Australia – the national computer emergency response team – has drafted national cyber security exercise programme guidelines and an evaluation framework for Commonwealth, State and Territory governments and businesses in the private sector. Beyond this, Australia has ratified the Council of Europe Convention on Cybercrime (the Budapest Convention), which codifies what constitutes a criminal offence in cyberspace and streamlines international cybercrime cooperation between signatory states. Australia's accession was reflected in the passing of the *Cybercrime Legislation Amendment Act 2011* (Cth).

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

The AML/CTF Act applies to entities that provide “designated services” with an Australian connection. Fintech business will often have obligations under the AML/CTF Act as financial services, and lending businesses typically involve the provision of designated services. Obligations include to:

- enrol with AUSTRAC;
- conduct due diligence on customers prior to providing any designated services;
- adopt and maintain an AML/CTF programme; and
- report annually to AUSTRAC and as required on the occurrence of a suspicious matter, a transfer of currency with a value of AUD 10,000 or more, and all international funds instructions.

Digital currency exchange providers also have obligations under the AML/CTF Act, and must register with AUSTRAC or face a penalty of up to two years' imprisonment or a fine of up to AUD 105,000 (or both) for failing to register. Exchange operators are required to keep certain records relating to customer identification and transactions for up to seven years.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

An entity that conducts any “banking business”, such as taking deposits (other than as part-payment for identified goods or services) or making advances of money, must be licenced as an ADI. Recently, APRA released the Restricted ADI framework, which allows new businesses entering the banking industry to conduct a limited range of banking activities for two years while they build their capabilities and resources. After two years, they must either transition to a full ADI licence or exit the industry. As stated in question 1.1, APRA granted the first Restricted ADI licence in 2018 and as of January 2019, the first Restricted ADI licensee has now been granted a full ADI licence which allows it to operate as an ADI without restrictions under the *Banking Act 1959* (Cth).

Fintech businesses are also subject to the prohibitions laid out in the *Australian Consumer Law*, which is administered by the Australian Competition and Consumer Commission (ACCC). Broadly, this includes prohibitions on misleading and deceptive conduct, false or misleading representations, unconscionable conduct and unfair

contract terms. While the *Australian Consumer Law* does not apply to financial products or services, many of these protections are enforced by ASIC either through mirrored provisions in the *Australian Securities and Investments Commission Act 2001* (Cth) or through delegated powers.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

The hiring and dismissal of staff in Australia is governed under the *Fair Work Act 2009* (Cth) (**Fair Work Act**). In relation to hiring, minimum terms and conditions of employment for most employees (including professionals) are governed by modern awards, which sit on top of the National Employment Standards. However, modern awards do not apply to employees earning over a threshold of AUD 145,400 (from 1 July 2018, threshold indexed annually), provided their earnings are guaranteed by written agreement with their employer.

To terminate an employee's employment, an employer has to give an employee written notice of the last day of employment. There are minimum notice periods dependent on the employee's period of continuous service, although the employee's award, employment contract, enterprise agreement or other registered agreement could set out longer minimum notice periods. Notice can be paid out rather than worked; however, the amount paid to the employee must equal the full amount the employee would have been paid if they worked until the end of the notice period.

For serious misconduct, employers do not need to provide a notice of termination; however, the employee must be paid all outstanding entitlements such as payment for time worked or annual leave.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Under the Fair Work Act, minimum entitlements for employees are set out under modern awards and include terms and conditions such as minimum rates of pay and overtime.

Australia also has 10 National Employment Standards. These include maximum weekly hours, requests for flexible working arrangements, parental leave and related entitlements, annual leave, long service leave, sick leave, compassionate leave, public holidays, notice of termination and redundancy pay, and a fair work information statement.

The Fair Work Act also has some general protection provisions governing a person's workplace rights, freedom of association and work place discrimination, with remedies available to employees if these provisions are contravened.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

Migrants require working visas from the Department of Home Affairs (**DOHA**) in order to work in Australia, and each type has its own eligibility requirements. Businesses can nominate or sponsor such visas.

As part of the National Innovation and Science Agenda, the DOHA launched an entrepreneur visa stream as part of the Business Innovation and Investment visa programme. Interested applicants must submit an expression of interest and be nominated by an Australian State or Territory Government.

In March 2018, the Government replaced the Temporary Work (Skilled) (subclass 457) visa with the Temporary Skill Shortage (subclass 482) visa (**TSS visa**), the most common form of employer-sponsored visa for immigration to Australia. The new TSS visa will implement a number of changes, including the move to two confined occupation lists:

- the Short-Term Skilled Occupations Lists (**STSOL**) with a maximum visa period of two years and the option to re-apply for another two years, with no pathway to permanent residency; and
- the Medium-Term Skilled Occupations Lists (**MLTSSL**) with a maximum period of four years which can be renewed as long as the occupation is listed, with an option of permanent residency after three years.

The STSOL and MLTSSL will be reviewed by the DOHA every six months.

As at the time of writing, there is no special route for obtaining permission for individuals who wish to work for fintech businesses.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Patent protection is available for certain types of innovations and inventions in Australia. A standard patent provides long-term protection and control over an invention, lasting for up to 20 years from the filing date. The requirements for a standard patent include the invention being new, involving an inventive step and being able to be made or used in an industry. The patent specification must also be clear and the claims must be fully supported by the information disclosed in the specification. An innovation patent is targeted at inventions with short market lives, lasting up to eight years. These quick and relatively inexpensive patents are aimed at protecting inventions that do not meet the inventive threshold, instead requiring that an invention involve an innovative step.

In Australia, provisional applications can also be filed as an inexpensive method of signalling intention to file a full patent application in the future, providing applicants with a priority date. However, filing this application alone does not provide the applicant with patent protection, but does give the person filing 12 months to decide whether to proceed with a patent application.

Design protection is available, for a period up to 10 years, of any design that is both new and distinctive. Protection is based on visual appearance.

A number of patent law reviews are currently under way, including whether to abolish the innovation patent system.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Broadly, the person or business that has developed intellectual property generally owns that intellectual property, subject to any existing or competing rights. In an employment context, the

employer generally owns new intellectual property rights developed in the course of employment, unless the terms of employment contain an effective assignment of such rights to the employee. Contractors, advisors and consultants generally own new intellectual property rights developed in the course of engagement, unless the terms of engagement contain an effective assignment of such rights to the company by whom they are engaged.

Under the *Copyright Act 1968* (Cth), creators of copyright works such as literary works (including software) also retain moral rights in the work (for example, the right to be named as author). Moral rights cannot be assigned but creators can consent to actions that would otherwise amount to an infringement.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

Options available to protect or enforce intellectual property rights depend on the type of intellectual property. As an example, software (including source code) is automatically protected under the *Copyright Act 1968* (Cth). An owner may also apply to IP Australia, the government body administering IP rights and legislation, for software to be registered under the *Designs Act 2003* (Cth) or patented under the *Patents Act 1967* (Cth). Software can also be protected contractually through confidentiality agreements between parties.

A standard, innovation or provisional patent can also be held to protect or enforce IP rights in Australia. Australia is also a party to the Patent Cooperation Treaty (**PCT**), administered by the World Intellectual Property Organisation. A PCT application is automatically registered as a standard patent application within Australia, but the power to successfully grant patent rights remains with IP Australia.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

In Australia, there are generally four commonly used approaches to monetising IP. These are:

- *Assignment*: An outright sale of IP, transferring ownership to another person without imposing any performance obligations.
- *Licensing*: Permission is granted for IP to be used on agreed terms and conditions. There are three types of licence (exclusive licence, non-exclusive licence and sole licence) and each comes with conditions.
- *Franchising*: A method of distributing goods and services, where the franchisor owns the IP rights over the marketing system, service method or special product and the franchisee pays for the right to trade under a brand name.
- *Spin-off*: Where a separate company is established to bring a technology developed by a parent company to the market. IP activities to be carried out for spin-offs include due diligence, confidentiality, employment contracts, assignment agreements and licence agreements.

Broadly, a business can only exploit or monetise IP that the business in fact owns or is entitled to use. Restrictions apply to the use of IP that infringes existing brands, and remedies (typically injunctions and damages) are available where the use of IP infringes the rights of another business.



Peter Reeves

Gilbert + Tobin
Level 35, Tower Two
International Towers Sydney
200 Barangaroo Avenue, Barangaroo
Sydney NSW 2000
Australia

Tel: +61 2 9263 4000
Email: preeves@gtlaw.com.au
URL: www.gtlaw.com.au

Peter Reeves is a partner in Gilbert + Tobin's Corporate Advisory group and is an expert and market-leading practitioner in financial services regulation and funds management. He leads the Financial Services and Fintech practices at G + T. Peter advises domestic and off-shore corporates, financial institutions, funds, managers and other market participants in relation to establishing, structuring and operating financial services sector businesses in Australia. He also advises across a range of issues relevant to the fintech and digital sectors, including platform structuring and establishment, payment solutions, blockchain solutions and global crypto-asset strategies. *Chambers 2019* ranks Peter in Band 1 for Fintech.



Established in 1988, Gilbert + Tobin is a leading independent corporate law firm and a key player in the Australian legal market. From our Sydney, Melbourne and Perth offices, we provide innovative, relevant and commercial legal solutions to major corporate and Government clients across Australia and internationally, particularly in the Asia-Pacific region.

With a focus on dynamic and evolving market sectors, we work on transactions and cases that define and direct the market. Gilbert + Tobin has become the legal adviser of choice for industry leaders who value our entrepreneurial culture and determination to succeed.

Gilbert + Tobin's reputation for expert advice extends across a broad range of practice areas and is built around an ability to execute with innovation, excellence, agility and deep industry knowledge. We don't just deliver on the *status quo* – we work closely with our clients to identify how their contracting and business processes need to transform and work differently. We advise at the innovative end of the spectrum and our fintech team is comprised of market-leading practitioners who provide clients with the full suite of financial services regulatory and commercial advice.

Austria

PFR Attorneys-at-law

Bernd Fletzberger



1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

During the last few years, a lively fintech scene has evolved in Austria with notable accelerators, start-ups and innovation hubs. Generally, Austrian-based companies benefit from an investor-friendly tax system and close links to both Central and Eastern Europe.

In Austria, we are seeing a rising number of young fintech companies. These companies are active in various fintech sub-sectors, such as alternative lending platforms, automated banking advice tools, insurtechs, digital including mobile payment operators, crowdinvesting platforms, online prepaid payment providers, robo-advice and alternative platforms for investment strategies, traders for cryptoassets, and technical service providers for fintech companies. Also, some established banks have developed some innovative products, mostly in cooperation with fintech companies.

Furthermore, more and more fintech events are held in Austria, with the “Pioneers Festival” the most important annual start-up event in Austria. Also, the “Fintechmatters” conference, where European fintech experts meet in Vienna for the “European FinTech Ecosystem Summit”, is an important gathering for the steadily growing fintech community. With its chairman Patrick Poeschl, the association “Fintech Austria” has established a very active Austrian fintech scene gathering on regular meetups, with the Vienna FinTechWeek as the annual event highlight. Hackathons and Backathons have also been held in Vienna recently.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

No, there are no types of fintech business prohibited or restricted in Austria.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

Both equity and debt financing are available in Austria. Generally,

equity financing is the common way of funding new and growing businesses in early stages, whereas debt financing becomes more important in later stages. Austria Wirtschaftsservice Gesellschaft (aws), the Austrian federal development bank, plays an important role in the Austrian Fintech ecosystem. By providing low-interest European Recovery Programme (ERP) loans, grants, guarantees, equity, know-how, consulting and other services, it supports companies in implementing their innovation projects, especially when sufficient financing cannot be obtained through other means.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

In Austria, various public sector organisations support the business community and promote the interests of companies. For example, the Austrian Business Agency is a good contact point for foreign investors interested in setting up business operations in Austria. The Christian Doppler Research Association promotes cooperation between science and business. The Austrian Research Promotion Agency (FFG) promotes and funds corporate R&D in Austria, assisting firms in optimally developing their innovative potential and exploiting new market opportunities by increasing their know-how. The aws, as already mentioned above, helps companies to establish and develop their business and to fund their investments by offering low-interest ERP loans, grants, guarantees, equity, know-how, consulting and other services.

Austria also offers different tax benefits which are linked to specific prerequisites. For example, companies may benefit from a 14% tax credit in connection with innovative research projects. Applications for the research tax credit can be submitted by every company investing in research, innovation and development, regardless of the company’s size, sector or corporate structure. A company is also entitled to claim the research tax credit if it generates no profits or only a small profit. Furthermore, equity stakes and forming tax groups can be worthwhile.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

Generally, an IPO exit requires the articles of association and by-laws to be adjusted, a due diligence to be performed and a prospectus to be prepared. Furthermore, the company will have to enter into an underwriting agreement and participate in road shows.

The concrete conditions mainly depend on the market segment chosen by the business. The Vienna Stock Exchange (VSE) offers the following market segments: standard and prime market (official market) for large and medium-sized companies; and direct market and direct market plus (third market operated as a multilateral trading facility (MTF)) for SMEs and young companies. A very good overview of requirements and rules for exchange-listed companies on the VSE may be found at: <https://www.wienerborse.at/uploads/u/cms/files/issuers/ipo/market-segments-of-the-vienna-stock-exchange.pdf>.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

There were not any notable fintech exits last year.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

There are no fintech-specific laws in Austria. However, depending on the specific business model, fintech companies may be subject to various regulatory licensing requirements:

- the Banking Act – e.g., if a business involves banking activities such as accepting third-party funds for management or granting loans;
- the Payment Services Act 2018 – e.g., when money is transferred to third parties, an account information or payment initiation service is involved;
- the Electronic Money Act – if the company issues electronic money;
- the Securities Supervision Act 2018 – if the company provides investment advice or portfolio management (e.g., certain robo advisor services), receives or transmits orders or operates a MTF;
- the Act on Alternative Investment Fund Managers – if the start-up collects investors' capital to invest in certain assets, including virtual currencies, based on a pre-defined investment strategy;
- the Insurance Supervision Act – if the company offers contract insurance; and
- the Financial Markets Anti-Money Laundering Act (FM-GwG).

Further, public offers of securities or investments might trigger a prospectus requirement pursuant to the Capital Market Act. Whether an initial coin or initial token offering triggers a prospectus requirement depends on the features of the coin or token and requires careful examination of the case at hand.

In Austria, the Financial Market Authority (FMA) is the competent supervisory authority for banking, insurance, securities and pension company supervision. The FMA also supervises payment service providers, e-money institutes and alternative investment fund managers. Thus, a fintech business may be supervised by the FMA if it conducts activities subject to any of the above financial market regulations.

Other commercial activities might be subject to the Austrian Trade Act; for example, insurance brokerage.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

No laws specifically directed at cryptocurrencies or cryptoassets exist in Austria.

Cryptocurrencies, such as Bitcoin, are regarded as digital assets by the regulator and therefore are not subject to regulation. However, certain business models based on cryptocurrencies may be subject to licensing and/or prospectus requirements. Based on the respective services, necessary licences can include banking licences, licences for providing, payment services licences and insurance licences.

Such regulations include:

- the Banking Act – if they involve banking activities such as accepting third-party funds for management by investing in a virtual currency;
- the Act on Alternative Investment Fund Managers – for example, collecting investors' capital to invest in virtual currencies according to a pre-defined investment strategy; or
- the Payment Services Act 2018 – for example, operating an online platform for purchasing virtual currencies which also processes payments in euros.

Furthermore, a public offer of coins and tokens (ICOs and ITOs) may trigger the requirement to publish a prospectus pursuant to the Capital Market Act.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

Austrian financial regulators and policy makers are receptive to fintech innovation and committed to support new entrants to regulated financial services markets.

Recently, the Minister for Finance announced the development of a fintech action plan to foster development in Austria. The plan focuses on regulating trade with cryptocurrencies, providing a new digital prospectus regime for ICOs and fines for misconduct. A fintech advisory board has been established to assist the government with the preparation of specific actions.

Furthermore, the FMA has established a fintech contact point, which handles all kind of regulatory questions. It may be contacted by fintech companies planning to become active in the Austrian market.

Currently, no regulatory sandbox is available. The Austrian federal government very recently announced its plans to establish a regulatory sandbox which allows businesses to test innovative products/business models in the market, with real consumers, but without being required to fulfil all regulatory requirements. We expect the respective draft bill to be adopted by the Austrian Parliament by summer 2019.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

Foreign fintechs looking to expand their business to Austria are subject to the domestic regulatory regime. This includes the various licensing and prospectus requirements as described above.

In practice, a foreign company has the following options:

- establish a domestic subsidiary or branch and obtain a licence from the FMA if it intends to provide a regulated activity;
- cooperate with a partner that holds the required licences;
- if seated in another EEA Member State, passport its existing EEA licence to Austria and either provide its business directly on a cross-border basis or establish a branch; or
- adapt its operations to avoid licence requirements.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

The collection/use/transmission of personal data is regulated by several European and Austrian laws, the most fundamental ones being the European General Data Protection Regulation (GDPR) and on a subsidiary basis, the Austrian Data Protection Act. These rules fully apply to fintech businesses operating in Austria.

Generally, the GDPR's data protection regime is strict. The key principles that apply to the processing of personal data are transparency, lawful basis for processing, purpose limitation, data minimisation, accuracy, retention, data security and accountability. The GDPR provides an exhaustive list of legal bases on which personal data may be processed. The most relevant legal bases for businesses are consent, contractual necessity, compliance with legal obligations or legitimate interests. Stronger grounds are required to process sensitive personal data.

The appointment of a data protection officer might be relevant to fintechs. However, such designation is only mandatory in some circumstances, such as in the large-scale regular and systematic monitoring of individuals or large-scale processing of sensitive personal data. Austria has not made use of the possibility in the GDPR to require the appointment of a data protection officer in additional circumstances.

If a fintech company appoints a processor to process personal data on its behalf, it must enter into a written agreement with that processor which sets out the subject matter for processing, its duration, the nature and purpose for processing data and the obligations and rights of the controller.

Additional data protection regulations can be applicable depending on the operating mode of fintech businesses. For example, payment service providers have to apply specific data protection rules under the PSD2 (e.g., explicit consent requirement for the provision of payment services). However, as in other EU Member States, the relationship between data processing rules under the GDPR and PSD2 is unclear and guidance from data protection and/or financial market regulators is still missing.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

The GDPR is applicable if data is collected, processed or used inside the EU, irrespective of the established location of the data processor. It is also applicable if the data is processed or used outside of the EU in order to offer services and goods to citizens within the EU or to monitor their behaviour.

The international transfer of data to jurisdictions outside of the EU is, barring few exceptions, only permitted if the receiving jurisdiction applies appropriate data protection regulations itself. The European Commission publishes a list of the jurisdictions that have been approved with regards to international data transfer outside of the EU.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

The GDPR provides for administrative fines of up to EUR 20 million or 4% of the company's worldwide annual turnover. The Austrian Data Protection Act contains further subsidiary fines of up to EUR 50,000.

Furthermore, affected individuals are entitled to claim damages for both material and immaterial damages caused by the violation of data protection regulation. Liability for damages can only be avoided if the organisation committing the violation can provide proof that it bears no responsibility whatsoever for the damage claimed.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

In December 2018, Austria implemented the NIS Directive in its own cybersecurity law, i.e. the Network and Information System Security Act (NISG). Certain financial infrastructures (e.g., payment or securities settlement systems, CCPs, trading venues) may be affected. However, only essential services fall within the scope of the NISG.

Furthermore, the Criminal Code penalises certain cybercrimes, including unlawful access to a computer system (hacking), breach of the privacy of telecommunications, abusive interception of data, data corruption, disturbance of the functionality of a computer system, abuse of computer programs or access data and data falsification.

In addition, the data security provisions of the GDPR and Data Protection Act establish several data security measures to ensure IT security.

More specifically for fintechs and based on various supervisory laws, the FMA has issued various guidelines regarding the IT security of financial institutions. These guidelines set out the minimum requirements regarding IT security of financial service providers, such as the FMA guidelines on IT security for credit institutions (dated May 2018), insurance companies (dated July 2018), investment firms (dated August 2018) and pension funds (dated December 2018). The circular regarding banks is also relevant for payment providers and e-money institutions. These guidelines specify the FMA's expectations towards the respective institutions regarding the secure design of IT systems and corresponding processes.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

Fintechs have to comply with AML requirements if they provide activities that require a licence and are therefore subject to the FMA's supervision. This applies to credit and insurance institutions, securities companies, alternative investment funds, payment service provider and e-money institutes. The relevant provisions for the prevention of money laundering and terrorist financing are contained in the FM-GwG.

If a fintech provides services that do not require a licence from the FMA, AML requirements may apply in certain circumstances on the

basis of the Commercial Code (GewO). For example, this is the case for retail tradespersons, real estate agents, consultants and insurance brokers.

If a fintech falls under neither a financial supervisory nor commercial law, it is generally not obliged to apply the AML rules. However, regulated entities are often required to contractually extend the due diligence obligations for the combatting of money laundering and terrorist financing to its outsourcing and cooperation partners; e.g., when a (non-regulated) fintech cooperates with a bank in connection with the sale of the regulated product.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

As mentioned above, there is no legislation in Austria which is aimed specifically at fintechs. Any additional relevant regulatory regimes would likely be specific to the sector in which a particular fintech firm operates.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

Generally, the employer and employee may negotiate the content of an employment agreement on a private contractual basis. However, the applicable statutes and collective agreements often prescribe minimum standards (e.g., for minimum wage, overtime supplements, maximum permitted working hours, annual leave). Said standards may not be deviated from when this is to the detriment of the employee.

The normal daily working time is eight hours, and the weekly normal working time may not exceed 40 hours. However, many collective agreements stipulate a reduced weekly normal working time. For example, the collective agreement for retail workers and the IT collective agreement sets a 38.5-hour limit per week. If normal working times are exceeded, employees are entitled to receive an overtime bonus which is generally 50% of the base remuneration. However, Austrian working time law provides different options for allocating normal working time in a manner which differs to that which has been envisaged by law.

“Termination by notice” is the unilateral, ordinary termination of employment which complies with notice periods and dates. Generally, no particular grounds of termination are required. Particular rules apply to certain groups of employees, such as disabled persons afforded special recognition, staff representatives, pregnant women and employees who have taken part-time parental leave. Notwithstanding the above, there exists a general protection against unfair termination. Basically, if an employer wishes to terminate an employee’s employment contract, there are essentially two sets of justifications that may be used: the first set relates to the behaviour of the respective employee; and the second set is based on organisational reasons (e.g., changes in the economic environment, restructuring, etc). Overall, employment termination rules are significantly more liberal than the ones of other European employment law systems (e.g., Italy, France and Germany).

5.2 What, if any, mandatory employment benefits must be provided to staff?

There is no statutory minimum wage in Austria. However, there are so-called collective agreements (equal to tariff agreements) which provide for a “minimum wage level” in major industry sectors. Employers must not drop below these levels. Salaries are generally paid out in 14 instalments (12 monthly instalments and a special bonus each for annual leave and Christmas).

Employees are entitled to at least 30 paid days of annual leave. The period increases to 36 business days after 25 years of service. Entitlement to annual leave lapses two years after the end of the annual leave year in which said leave days were accrued.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

Immigration rules apply to all companies and are not specific to the fintech sector.

Employment of (non-EU) persons in Austria is subject to various restrictions and controls under the Austrian Employment of Aliens Act. As a general rule, persons are deemed aliens if they do not possess Austrian citizenship. An alien may only be employed if an employment authorisation or secondment authorisation has been issued for that employee or if a confirmation of notice or an EU secondment confirmation has been issued, or the employee holds a valid work permit or exemption certificate.

Highly qualified persons, specialists in occupations in short supply, key workers, graduates of Austrian universities and self-employed key workers may apply for the so-called “red white red card”. This was created back in 2011 in order to introduce a new, flexible system of immigration in Austria. The red white red card is issued for a 24-month period and grants authorisation for temporary residence and employment with a specified employer. The most important criteria governing the granting of a red white red card are qualifications, professional experience, age, language skills, a firm job offer and a particular minimum level of reimbursement, depending on the employee’s qualifications.

Where the work being performed by a foreign employee from a third country does not last longer than six months, aliens may apply for a “secondment authorisation”, which may not be issued for longer than a four-month period.

For short-term work (e.g., business meetings, visiting trade fair events and conferences), no employment or secondment authorisation is required.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Inventions and innovations can be protected by Intellectual Property Rights (IPR), including patents, utility models, trademarks and registered designs:

- Patents are basically territorial rights, and are therefore limited to the state for which the protection is granted and limited to a maximum period of 20 years. An invention is patentable if it is novel, contains an inventive step and if it is capable of industrial application. For example, certain hardware may benefit from patent protection.

- A utility model (commercial right for technical inventions) involves no testing for novelty, the inventive process or commercial applicability. Protection through utility models is limited to a maximum period of 10 years. Normally, these are granted more quickly than a patent, but they confer weaker protection and are only applicable in certain countries.
- A company label can be protected by a trade mark. They can be protected for 10 years with the possibility for extension. The branding applied to a fintech product may be protected by trade marks.
- The appearance of commercial products, e.g. portable or wearable devices, may be protected by registration of an industrial design (e.g., the shape of a mineral water bottle).

However, fintech products will often be based on computer programs. Such software is primarily protected by copyright as a type of literary work. Copyrights arise automatically in the computer code and may also subsist in other elements of the software, such as screen displays, or graphics, such as on-screen icons and designs.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Copyrights do not need any special registration: they are generated by the creation. Under Austrian copyright law, the creator of a work is the owner of a copyrighted work. An author can only be a natural person, not a legal entity. Other than exploitation rights, the ownership may not be assigned to third parties. Generally, copyright protection lasts 70 years after the death of the author, or, in the case of joint copyright, 70 years following the death of the longest living co-creator. In cases of creation of work by employees, copyright resides with the employee or the contractor. Rights of exploitation to the created work will pass to the employer if the work was created by the employee in the course of their employment duties. Austria is a member of all international copyright conventions (e.g., the Berne Convention and the Universal Copyright Convention).

In order to protect a patent in Austria, a patent application must be filed with the Austrian Patent Office. The patent applicant must formulate one or more patent claims. The Patent Office first conducts a preliminary review of the application in its formal and substantive respects. After publication of the patent application by the Patent Office, and provided no notice of opposition is filed within four months, the patent is registered and officially published.

Contrary to trademarks, patents may not be registered for the entire EU. The current European patent, based on the European Patent Convention (EPC), only offers a bundle of national individual patents, but does not provide the option of registering a single patent covering the entire EU. A European patent may be applied for at the European Patent Office (EPO) in Munich and at the Austrian Patent Office.

Shortly, the “unitary patent” will offer standard protection across a number of EU Member States. Once it does become operative, a European Patent Court will decide on the validity of a unitary patent, operating via regional chambers in various Member States (including Austria), the highest instance of the court being the ECJ.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

Please see the answers above under question 6.2.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

IP is usually exploited/monetised by means of licensing, assignment (transfer), and the granting of security interests.

With regards to patents, trademarks and designs, none of these options require any contractual formalities or registration with their respective registers. For patents, a (declaratory) registration of an exclusive licence is possible. As copyrights cannot be transferred themselves, licences are used as the prevalent method of exploitation.

When exploiting IP rights, the general rules of competition and antitrust law, largely determined by EU regulation, should be kept in mind.



Bernd Fletzberger

PFR Attorneys-at-law
Nibelungengasse 11
1010 Vienna
Austria

Tel: +43 1 877 04 54
Email: fletzberger@pfr.at
URL: www.pfr.at

Bernd is a partner of the law firm PFR Attorneys-at-law seated in Vienna. He advises credit institutions, payment and e-money institutions, technical service providers in the mobile payment world, fintech start-ups, investment firms, alternative investment fund managers and insurers in all kind of regulatory matters. Through more than 10 years of experience, he has gained a comprehensive understanding of the challenges the financial industry and young businesses are confronted with. He delivers high-quality legal advice.

PFR RECHTSANWÄLTE

PFR Attorneys-at-law is a boutique law firm specialised on all kind of legal matters relevant for the financial industry, in particular financial market laws. We are seated in the heart of Vienna. We provide outstanding legal advice to credit institutions, payment and e-money institutions, technical service providers in the mobile payment world, fintechs, IT companies, investment firms, alternative investment fund managers, insurers and retailers in all kinds of regulatory matters.

Bermuda



Natalie Neto



Rachel Nightingale

Walkers Bermuda

1 The Fintech Landscape

- 1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).**

The Bermuda Government announced its Fintech Strategy in November 2017 and stated its intention for Bermuda to become a leading jurisdiction for fintech, to embrace the development of new forms of financial technology, including blockchain and cryptocurrencies, and to establish Bermuda as an innovation hub for the development and employment of such technology. The Bermuda Government and the sole financial services regulator, the Bermuda Monetary Authority (the “BMA”), have worked together with industry and technology advisers to create a fit-for-purpose legal and regulatory framework which offers a welcoming environment to foster innovation, but also provide adequate protection for investors and consumers via regulation. Bermuda operates one of the largest (re)insurance industries in the world, which is regulated and supervised by the BMA, and has leveraged its experience and expertise in the regulation of this sector (known for its innovation in terms of the creation of new risk vehicle and products) to develop a robust, risk-based framework and a supervisory environment that is both conservative and effective, but is not unduly burdensome on those who seek to operate their fintech businesses from within Bermuda.

- 1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?**

There are no such restrictions. Bermuda’s legislation captures all forms of fintech businesses provided they are conducting digital assets business activities, which also includes cryptocurrency-based businesses or offering digital assets to the public. Fintech businesses may operate in or from Bermuda, subject to complying with the legislative and regulatory framework. For further explanation as to the type of fintech activities that are regulated, please see our responses below.

2 Funding For Fintech

- 2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?**

The Bermuda Government has passed a bill to create the Fintech Development Fund for the purpose of investing and training Bermudians to build and develop an ecosystem in Bermuda for fintech to develop and thrive. The purpose of the fund is to support the financial technology education for Bermudians, including supporting community-based initiatives.

In addition, the Bermuda Government also passed amendments to the Banks and Deposit Companies Act 2000 to create a new class of licensed bank (with no requirement for a retail presence in Bermuda) for banking services to be made available to fintech businesses in Bermuda.

In February 2019, it was announced that Signature Bank, a New York-based full-service commercial bank, had agreed to provide a full range of banking services to Bermuda-licensed fintech companies that meet both Bermuda and Signature Bank standards.

- 2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?**

Bermuda companies are not currently subject to corporate income tax and Bermuda does not levy personal income tax. Bermuda-exempted companies may apply for an assurance from the Minister of Finance that, in the event of there being enacted in Bermuda any legislation imposing tax computed on profits or income or computed on any capital asset, gain or appreciation, or any tax in the nature of estate duty or inheritance tax, the imposition of any tax will not apply to the company or to any of its operations or to the shares, debentures or other obligations of the company.

- 2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?**

A company which is offering shares to the public is required to comply with the provisions of the Companies Act, 1981, as amended (the “Companies Act”) and, unless exempted, must prepare and file a prospectus with the Bermuda Registrar of Companies.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

None that we are aware of.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

The Digital Assets Business Act 2018 (“DABA”) became operative with effect from 10 September 2018 in Bermuda. DABA regulates the following ‘digital asset business activities’ if carried on in or from within Bermuda, and requires that such activities be licensed by the BMA:

- issuing, selling or redeeming virtual coins, tokens or any other form of digital asset;
- payment service provider business utilising digital assets;
- operating an electronic exchange whereby digital assets of any type are exchanged for cash or other types of digital assets;
- provision of digital assets custodial wallet services; and
- digital asset services vendors.

The term ‘digital asset’ covers anything which exists in binary form and comes with the right to use it and includes a digital representation of value. It captures digital coins, security, equity or utility tokens and anything intended to provide access to an application, product or service by means of distributed ledger technology. Transactions in which a person grants value as part of an affinity or rewards programme (provided value cannot be taken from or exchanged for fiat currency, bank credit or any digital asset), or a digital representation of value used by a publisher within an online gaming platform, are excluded from the definition of ‘digital assets’.

Amendments were also made to the Companies Act pursuant to the Companies and Limited Liability Company (Initial Coin Offering) Amendment Act 2018 on 9 July 2018, to create a statutory framework for the regulation of ‘initial coin offerings’ in Bermuda. The legislation captures the offering by a person of any form of ‘digital asset’ (as defined above) to the public and is not limited to ICOs. Any person who is conducting such an offering must first obtain the consent of the Minister of Finance pursuant to the Companies Act and must publish an offer document in accordance with that Act and the Initial Coin Offering Regulations 2018 (the “ICO Regulations”).

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

Yes, DABA and the Companies Act specifically regulate cryptocurrencies and cryptoassets, as described above.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

There is a two tier-licensing regime under DABA, including a Class M licence, which is a regulatory sandbox option for fintech businesses in Bermuda. For further details, please see our response to question 3.4 below.

In addition, amendments were also made to the Insurance Act 1978 with effect from July 2018 to create an insurtech regulatory sandbox for the purpose of facilitating and promoting experimental and innovative applications of technology in the insurance sector.

The BMA has also established an “Innovation Hub” to promote insurtech innovation.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

Any person who wishes to carry on a digital asset business activity in or from within Bermuda (unless exempted) is required to be licensed and regulated by the BMA.

There are two classes of licence under DABA: Class F, which is a full licence; and Class M, which is a modified ‘regulatory sandbox’ licence. The Class M licence may have restrictions attached and will be issued for a defined period to enable proof of concept to be established, within a controlled environment and under the supervisory oversight of the BMA, with the intention that the licensed undertaking will be able to migrate to a Class F licence once the business meets its critical success factors. Class F licences are not restricted to a specific time period, but may be subject to restrictions, if deemed necessary by the BMA.

Applications for licences must be accompanied by (among other things) a business plan, two years’ financial projections, details of the governance and risk management framework and copies of the policies and procedures which will be in place to comply with the requirements of DABA, the Digital Asset Business Code of Practice (“DABA Code of Practice”) and other rules promulgated thereunder, including copies of the anti-money laundering and anti-terrorist financing policies (“AML/ATF”).

The BMA will not issue a licence unless it is satisfied that the ‘minimum criteria’ have been satisfied with respect to the applicant, which are set out in Schedule 1 to DABA. These criteria are similar to those applied in respect of other regulated entities in Bermuda (such as insurance, insurance manager, investment business and fund management entities) and include the following requirements:

- the ‘controllers’ (managing directors, CEOs, shareholder controllers (owning or controlling more than 10%) and persons in accordance with whose instructions or directions the applicant is accustomed to acting (shadow directors)) must be ‘fit and proper’;
- the business must be conducted in a prudent manner (taking into account any failure to comply with the provisions of DABA, the DAB Code of Practice, AML/ATF requirements and international sanctions measures), and a business will be deemed not to be conducting business in a prudent manner if it maintains less than BD\$100,000 of minimum net assets (or such other amount as the BMA may direct, taking into account the nature, size and complexity of the licensed undertaking);
- the business must have in place appropriate insurance to cover inherent risks or such other risk mitigation measures as the BMA may approve;
- maintenance of adequate accounting records, control systems, policies and procedures, and implementation of appropriate corporate governance policies;
- the business must be effectively directed by at least two directors and under the oversight of such number of non-executive directors as the BMA considers appropriate given the nature, size, complexity and risk profile of the licensed undertaking; and

- the position of the licensed undertaking within the structure of any group to which it may belong should be such that it will not obstruct the conduct of effective consolidated supervision.

A DABA licensed undertaking is required to maintain a head office in Bermuda from which the business will be directed and managed, and the BMA will take a number of factors into account when determining if the head office requirement has been satisfied, including the presence of senior executives in Bermuda and whether the strategic decision-making concerning risk and policy decisions takes place in Bermuda.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

Yes, the Personal Information Protection Act 2016 (“PIPA”) is the principal Bermuda statute regarding the regulation of personal data.

The initial operative provisions of PIPA came into force in December 2016 to enable the appointment of the Privacy Commissioner; the law was expected to become fully effective by December 2018, but is not yet in force as at February 2019.

PIPA generally applies to every organisation that uses personal information in Bermuda either wholly or partly by manual or electronic means. Since fintech businesses typically use a significant degree of personal information, fintech businesses will be required to comply with PIPA.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

PIPA may apply to organisations established outside of Bermuda in the event that they use personal information in Bermuda either wholly or partly by manual or electronic means. PIPA restricts international transfers of data by requiring an organisation to assess the level of protection provided in relation to the personal information by the overseas third party before making any transfer of personal information to an overseas third party.

The Standard for Electronic Transactions (“Standard”) only applies to intermediaries and e-commerce service providers who are carrying on a trade or business or conducting commercial transactions or services in or from within Bermuda, or which are identified with Bermuda for the purposes of the Electronic Transactions Act 1999, whose transactions or services either themselves take place electronically or which assist others to do so, or which relate to business carried out electronically.

Once PIPA substantively takes effect, subject to limited exceptions under PIPA, where an organisation transfers personal information to an overseas third party either on behalf of the organisation or for its own business purposes, the organisation shall remain responsible for compliance with PIPA in relation to that personal information. This will include an assessment of the level of protection provided by the overseas third party for that personal information.

If the organisation is not satisfied that the level of protection provided by the overseas third party is comparable to the level of

protection required by PIPA, the organisation shall employ contractual mechanisms, corporate codes of conduct including binding corporate rules, or other means to ensure that the overseas third party provides a comparable level of protection.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

PIPA incorporates the following sanctions for non-compliance with its provisions:

- For summary convictions of individuals, a fine not exceeding BDS\$25,000, imprisonment not exceeding two years, or both.
- For convictions on indictment of persons other than individuals, a fine not exceeding BDS\$250,000.

A data controller or data processor must comply with the Standard in respect of any personal data that is collected by the data controller. Failure to comply with the Standard may result in summary conviction and imprisonment for six months or a fine of BDS\$50,000, or both.

An intermediary or e-commerce service provider who fails to comply with the Standard must in the first instance be given a written warning by the Minister responsible for economic commerce. The Minister may direct that person to cease and desist or otherwise to correct its practices, and, if that person fails to do so within a period as may be specified in the direction, the person is guilty of an offence and may be liable on summary conviction to a fine of BDS\$5,000 for each day on which the contravention continues.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

Yes, any entity that is licensed under DABA must also demonstrate a comprehensive cybersecurity programme that is commensurate to the nature, scale and complexity of its business and will be expected to have a written cyber security policy which is reviewed at least annually. An external audit of its cybersecurity programme must also be conducted on an annual basis. Such cybersecurity policy is a requirement as part of the Digital Asset Business (Cybersecurity) Rules 2018.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

An undertaking which is licensed under DABA is a ‘regulated financial institution’ for the purpose of Bermuda’s anti-money laundering and anti-terrorist financing laws and regulations (“AML/ATF Laws”) and must comply in all respects with them. The BMA has also issued sector-specific guidance for digital asset businesses with respect to the AML/ATF Laws. Licensed undertakings should apply a risk-based approach and obtain adequate due diligence and verify the identity of its clients, as well as conduct ongoing monitoring and report any suspicious activity.

The Companies Act and the Initial Coin Offering Regulations require any person that is conducting an ‘initial coin offering’ in or from within Bermuda to have in place appropriate measures to verify the identity of participants in the offering, and other anti-money laundering and anti-terrorist financing requirements set out in the ICO Regulations.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

To the extent that a fintech business is operating as an insurance company, it would be required to comply with the Insurance Act 1978 (see further above). If a fintech business is conducting investment business activities from premises in Bermuda, at which it employs staff, it may require a licence under the Investment Business Act 2003.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

The legal framework for hiring and dismissing employees in Bermuda is set out in the Employment Act 2000 (the “**Employment Act**”).

Employers must also observe the requirements set out under the Bermuda Immigration and Protection Act 1956 (as amended), which was created to ensure that suitably qualified Bermudians would have precedence over non-Bermudians with respect to employment opportunities in Bermuda. Subject to limited exceptions, any employment position must be advertised first in the Royal Gazette in Bermuda and also on local job advertisement boards, and guest workers may only be employed on a work permit for a limited period of time in the event that no suitably qualified Bermudians apply for the position.

Any employee hired has the right to bring a complaint to the government’s Department of Workforce Development within a three-month period of the employer’s breach under the Employment Act and/or any unfair dismissal claim. Under Bermuda law, any employee may not be dismissed without a valid reason – such reason being connected to the performance, ability, conduct and/or the operational requirements of the employer’s business.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Every employer in Bermuda must provide a health insurance plan for their employee and each employee’s uninsured dependant. In addition, employers must also provide a pension plan for its Bermudian employees and employed spouses of Bermudians.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

Please refer to the response to question 5.1 above.

In recognition of the fact that many fintech businesses may need to bring specialist staff from overseas in order to establish a business in Bermuda, the Bermuda Government has created a new class work permit called the ‘Fintech Business Work Permit’. A Fintech Business Work Permit allows any newly incorporated fintech company to receive automatic approval for up to five work permits for a six-month period following incorporation. The permits can be used for any job category provided that the position is not an entry

level, graduate or trainee position and the position will not need to be advertised as set out above. Fintech Business Work Permits can be granted for between one to five years.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Innovations, inventions and intellectual property are protected in Bermuda under the Trade Mark Act 1974 (the “**Trade Mark Act**”), the Copyright and Designs Act 2004 (the “**Copyright Act**”) and the Patent and Designs Act 1930 (the “**Patent Act**”). The Registry General in Bermuda is the responsible government department for registration of intellectual property.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Trademarks are registerable under the Trade Mark Act, which is based on the UK Trade Marks Act 1938. The initial registration lasts for seven years and is renewable for successive 14-year periods thereafter. A registered trademark will provide the proprietor with exclusive rights to use and license the trademark. In certain situations, an unregistered trademark may also be protected under the common law tortious remedy of passing off.

The Copyright Act is based on the UK Copyright, Designs and Patents Act 1988 and applies to the copyrights which subsist in original literary, dramatic, musical and artistic works, sound recordings, films, broadcasts, typographical arrangements and databases. In order to be afforded protection under the Copyright Act, each potential copyright must meet the requirements set out under the Copyright Act. The copyright protection is deemed effective from the time the work is created and registration is not a requirement.

The Patent Act provides patent protection in Bermuda. In order to register a patent an application must be submitted to the Registry General in Bermuda, and the application will then be sent to the UK for search, examination and confirmation. A patent is effective for 16 years and may be extended for periods of up to seven years at the relevant Minister’s discretion. The Patent Act provides for a confirmatory patent process, which is a convenient means of securing patent protection in Bermuda, as a UK or European patent designating the UK can be reregistered in Bermuda within three years of the original grant.

Designs may also be registered under the Patents Act and any registration of a UK design may be subject to the confirmatory patent process set out above to extend the registration to Bermuda. Designs can also be protected under the Copyright Act, where a copyright subsisting in a design copyright protection can last for a maximum of 15 years.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

Bermuda is not a signatory to the following treaties: the Paris Convention for the Protection of Industrial Property; the Patent Cooperation Treaty; Berne Convention for the Protection of Literary and Artistic Works; Universal Copyright Convention; or the Agreement on Trade-Related Aspects of Intellectual Property Rights. Accordingly, in order to protect and enforce intellectual

rights in Bermuda, the proprietor will need to have local and/or national rights over the intellectual property and register these in accordance with the processes set out above.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

Intellectual property in Bermuda may be monetised in a number of ways, including utilising a Bermuda exempted entity to hold, sell and license intellectual property rights from Bermuda.

Bermuda, along with other Overseas Territories and Crown Dependencies, is committed to putting in place legislation which would address the EU's concerns over harmful tax practices with respect to Bermuda entities carrying on 'relevant activities', including intellectual property related activities. With effect from 1 January 2019, any company, limited liability company, exempted partnership or exempted limited partnership will be required to observe economic substance requirements and, in the case of intellectual property-related activities, may be required to file additional information with the Registrar of Companies depending on the manner in which such intellectual property activities are being conducted.



Natalie Neto

Walkers Bermuda
Park Place, 55 Par-la-Ville
Hamilton HM 11
Bermuda

Tel: +1 441 242 1533
Email: natalie.neto@walkersglobal.com
URL: www.walkersglobal.com

Natalie Neto is a partner in the corporate and finance practice at Walkers Bermuda*.

Natalie advises on a wide range of Bermuda-based and international corporate and regulatory matters with significant transactional experience advising on M&A transactions for public and private companies, including takeovers, tender offers and squeeze outs, amalgamations, mergers, and schemes of arrangement.

Natalie also advises on private equity investments, debt and equity capital markets transactions, banking and finance matters and has a wide depth of knowledge with respect to complex restructuring projects involving Bermuda companies, LLCs and partnerships, including redomiciliations.

Natalie also advises companies and directors in respect of corporate governance and regulatory matters, including directors' fiduciary duties and responsibilities.

Natalie advises Fintech clients and investors with respect to Bermuda's evolving ICO legislation and blockchain and digital asset framework, including the establishment, licensing and ongoing compliance obligations of digital asset businesses.



Rachel Nightingale

Walkers Bermuda
Park Place, 55 Par-la-Ville
Hamilton HM 11
Bermuda

Tel: +1 441 242 1520
Email: rachel.nightingale@walkersglobal.com
URL: www.walkersglobal.com

Rachel Nightingale is based in the Walkers Bermuda* office and is an associate and member of the corporate, finance and funds practice at Walkers Bermuda. Rachel specialises in advising on corporate, regulatory, compliance and finance matters.

Rachel has particular expertise advising on international M&A transactions, public listings, Bermuda law regulatory and compliance matters and Fintech businesses in connection with the digital asset framework in Bermuda.

Rachel regularly advises licensed insurance and reinsurance entities, financial institutions, investment managers, advisors and brokers as well as start-up Fintech venture companies.



With staff drawn from top international law firms, Walkers Bermuda* provides first-class, commercially-focused advice that is attuned to our clients' requirements and facilitates their business.

Clients include global corporations, financial institutions, capital markets participants, investment fund managers and high-net-worth individuals located throughout the world, but with a primary focus in the Americas.

Walkers Bermuda is a full-service commercial law office. Core practice areas are:

- Corporate & Private Equity.
- Finance.
- Investment Funds.
- Insolvency & Dispute Resolution.
- Insurance.
- Compliance & Regulatory.

*Walkers works in exclusive association with Kevin Taylor, trading as 'Walkers Bermuda', a full-service commercial law firm providing advice on all aspects of Bermuda law. The title of 'partner' is used to refer to a consultant or employee of Walkers Bermuda with equivalent standing and qualifications to a partner of Walkers.

Brazil

Mattos Filho, Veiga Filho, Marrey Jr
e Quiroga Advogados

Larissa Lancha Alves de Oliveira Arruy



Fabio Ferreira Kujawski



1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Brazil leads the way in Latin America with 453 established fintechs (as per Radar FintechLab issued on August 2018) – most of them in the payments sub-sector (26% of Brazilian fintechs). Last year, there was an increase in the number of fintechs operating with cryptocurrency (86%), foreign exchange (55%) and insurance (37%) segments. Initiatives involving online lending also continue to be relevant, particularly considering recent developments in the regulation.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

Many services in the Brazilian financial and capital markets can only be provided by regulated and authorised entities. For example, the provision of loans or financing in Brazil are heavily limited for non-financial institutions, which leads fintechs operating in these fields to evaluate the costs of incorporating a new financial institution *vis-à-vis* the possibility of establishing partnerships with typical financial institutions to perform their activities. In view of that, in April 2018 the Brazilian Monetary Council enacted a rule to regulate online lending fintechs through the creation of two new models of financial institutions, which are able to extend loans with their own capital or intermediate loans among customers through an electronic platform. Although such business is not expressly prohibited, the Brazilian Central Bank and the Brazilian Securities Commission (CVM) issued warnings regarding the risks arising from investing in cryptocurrencies and stated that technically, the issuance of currency is an exclusive attribution of the Brazilian government. The CVM has also declared that if cryptocurrencies or any investment scheme subject to initial coin offerings (ICOs) are considered as securities under Brazilian law, such ICO will be subject to the regulation for public offering of securities.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

New businesses may obtain funding from regular credit lines extended by financial institutions (which will typically require collateral) or less frequently from capital markets, with the issuance of debt or equity instruments. There is a specific form of investment in startups, referred to as “angel investment”, which consists of capital contributions with a limitation in returns applicable to the initial period of investment. An angel investor may only invest in microenterprises and small businesses, and is not deemed as an equity holder of the investee, so is not liable for development of the investee’s activities – including in case of judicial recovery or disregard of legal entity, so it may avoid tax and labour liabilities. The tax treatment to the earnings obtained with this investment mechanism was recently regulated, so, for that reason, this mechanism may become more attractive to investors. Investment-based crowdfunding, characterised as situations in which an idea, project or business is offered as an investment opportunity that leads to ownership interests, partnerships or remuneration, is also becoming more common. This funding alternative is implemented by means of an offer of securities issued by small-sized companies to the public, through electronic participative investment platforms.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

In general, Brazilian tax incentives are designed to promote domestic development policies, such as the economic growth of certain geographic regions (i.e. North/Northeast regions) and specific fields of activity (i.e. technology innovation) among others, and usually take the form of tax exemptions or reductions.

Regarding technology innovation, there are tax benefits constituted with the purpose of fostering technological advances by encouraging research and development (R&D), which include, among others: (i) accelerated depreciation of newly acquired equipment destined to R&D for income taxation purposes; (ii) accelerated amortisation of acquired intangible assets destined to R&D applications for income taxation purposes; (iii) the deduction of expenses incurred during R&D for income taxation purposes; (iv)

exemption of withholding income tax levied on expenses with patent and trademarks registry abroad; and (v) federal VAT (*imposto sobre produtos industrializados*) reduction on manufactured products applied to R&D. Moreover, there is a special tax regime for the export of information technology services (Special Taxation for Export of Information Technology Services – REPES).

In addition to the above, businesses with a yearly gross revenue up to R\$ 4.8 million may opt for a simplified and less bureaucratic tax regime introduced by Complementary Law No. 123/2006 – *Simples Nacional*. Under this regime, taxpayers collect most of their taxes through one unified document, these taxes being: income taxation (*imposto sobre a renda and contribuição social sobre o lucro líquido*); revenue tax (*contribuição para o programa de integração social and contribuição para o financiamento da seguridade social*); federal and state VAT (*imposto sobre produtos industrializados and imposto sobre operações relativas à circulação de mercadorias*, respectively); social security contributions (*contribuição patronal previdenciária*); and service tax (*imposto sobre serviços de qualquer natureza*). The applicable tax rate depends on the company's activity and is applied over gross revenues earned monthly. *Simples Nacional* usually results in lower effective taxation, and reduced tax compliance cost.

At state and municipal level, it is possible to negotiate special regimes in order to obtain a simplification for the fulfilment of ancillary obligations, such as issuance of invoices and record of tax returns.

Considering the above, a fintech that decides to do business in Brazil should seek the best package of federal, state and local incentives available when deciding where to locate its business.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

In order to obtain an IPO in Brazil, a company needs to: (i) obtain its registration as a public company with the CVM; (ii) obtain the registration of the public offering of shares with the CVM; and (iii) obtain its registration as a listed company with the São Paulo Stock Exchange (B3 S.A. – *Brasil Bolsa Balcão* – B3), which are normally carried out simultaneously. The company shall meet certain standards of corporate governance, depending, especially, on the B3's listing segments it will be subject to; for example, the requirement to have independent members on the board and to meet certain requirements for minimum flotation of its stock on the public market (25%). There is also an entry-level access market segment named BovespaMais, which was designed for smaller enterprises and allows the minimum flotation requirements to be met within seven years. This segment has listed a few technology companies, although its success is still to be seen. A public company will also be subject to a significant number of ongoing obligations under Brazilian Corporations Law and regulations issued by the CVM, such as mandatory financial reporting, timely disclosure of material information to the market, and insider trading restrictions, among others. There is also the possibility of performing an IPO through a public offering with restricted efforts, in which case the offering will be directed to a determined number of sophisticated investors and will not be registered before the CVM.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

In the last year, there have been two notable IPOs of Brazilian fintech business, executed in Brazil and offshore: (i) Stone Pagamentos, which

raised US\$ 1 billion at NASDAQ; and (ii) Banco Inter, which raised R\$ 722 million at B3. These transactions involved a secondary offer, in which the founders and/or other investors sold a portion of the equity stake in the company.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

The highest regulatory authority in the Brazilian Financial System is the Brazilian National Monetary Council (*Conselho Monetário Nacional* – CMN). Financial services are regulated by the Brazilian Central Bank and the CMN and include all banking activities, extension of loans, financing, taking of deposits, payment services and card network schemes, among others. Activities in the Brazilian capital markets, such as securities intermediation, public offerings of securities, securities research and consulting and portfolio management, are regulated by the CVM. Private insurance services are regulated by the Superintendence of Private Insurance (SUSEP). Fintechs providing services regulated by the abovementioned entities should request authorisation to operate in Brazil or enter into partnerships or joint ventures with regulated entities, while fintechs that provide pure technology services may fall outside the scope of regulation. Regulated entities may outsource part of their activities and remain liable before third parties and regulators, so fintechs may provide such services as outsourcers. There are regulations governing the delegation of certain financial and capital markets services, which allow fintechs to take on such services in the capacity of banking correspondents or agents on behalf of the regulated entities. Banking regulations also permit non-regulated entities acting as sponsors to deposit collateral with financial entities, which may be used to extend loans and financing to third parties, of which collection will be allocated to settle the deposits and which cannot be claimed in case of defaults. All such types of arrangements are widely used by fintechs in the credit and securities businesses.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

Currently, there is no regulation in Brazil specifically directed at cryptocurrencies or cryptoassets. However, in October 2018, the Brazilian Federal Revenue (RFB) launched a public hearing regarding the provision of information on transactions performed with cryptoassets, pursuant to which Brazilian exchanges, individuals and legal entities that operate with cryptoassets, offshore or in Brazil, will be obliged to report such transactions to the RFB.

The Brazilian Central Bank released a statement about the risks related to cryptocurrencies, warning that cryptocurrencies are not issued nor guaranteed by a monetary authority, and are not backed by real assets. CVM also released a statement informing investment fund managers that cryptocurrencies cannot be classified as financial assets for the purposes of regulation. Therefore, the acquisition of cryptocurrencies by investment funds in Brazil is not allowed. In addition, public offerings involving cryptocurrencies may be subject to CVM regulation, as detailed in question 1.2 above.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

The Brazilian Central Bank, the CVM and the SUSEP have been demonstrating interest to discuss innovative business and regulatory models in the financial and capital markets. Both the CVM and the Brazilian Central Bank have been regularly promoting events and discussion forums, also inviting fintechs and advisors in the fintech field for discussions on innovation and regulation. The CVM's "FintechHub" programme and the Brazilian Central Bank internal work-group were implemented by such regulators to study digital and technological innovations related to the financial and capital markets, and to analyse the development of fintechs and its impact on Brazilian markets. Despite this receptivity, Brazilian regulators also demonstrate concerns regarding the impact of these new models on the stability and soundness of Brazilian markets, especially in regard to cryptocurrencies. They also recognise that traditional regulatory models may not be efficient to deal with the complex challenges offered by disruptive players. For this reason, in December 2018, the CVM's president announced that a sandbox programme may be an alternative to deal with situations of such nature. Also, the Brazilian Central Bank amended the regulation applicable to payment institutions to determine that they are only subject to licence requirements once they reach certain financial thresholds, which allows new players to initiate their operations with less regulatory burden. Therefore, even though there are no current sandbox options for fintechs in Brazil, this alternative is constantly being considered by the CVM or the Brazilian Central Bank and may be developed in the future.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

In situations where services are regulated in Brazil, authorisation and licensing requirements should apply in the same manner to both local service providers and providers established outside Brazil, whenever customers are targeted within the Brazilian territory. Whenever services include offers of investments, these may be treated as public offers of securities regardless of jurisdictions from which they originate. In these circumstances, fintechs may enter into partnerships with regulated entities in Brazil or seek their own licensing or authorisation. When seeking authorisation to operate in Brazil or to provide regulated services to Brazilian domiciled entities or individuals, regulations will typically require those service providers to be established in Brazil.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

In August 2018, the Brazilian Data Protection Law (*Lei Geral de Proteção de Dados – LGPD*) was enacted, regulating the use of

personal data in Brazil. LGPD establishes detailed rules for the collection, use, processing and storage of personal data by private and public entities in all economic sectors, both in the digital and physical environment. Inspired by the European General Data Protection Regulation (GDPR), LGPD is intended to radically change the Brazilian data protection system. Originally, LGPD was intended to become effective within 18 months from its official publication (which would be in February 2020). However, in December 2018, the Brazilian President enacted the Provisional Measure No. 869/2018, which amended certain provisions of LGPD and extended the deadline for organisations to become compliant with LGPD's obligations to August 2020. In case this Provisional Measure is not converted into law in accordance with the Brazilian legislative process, the original deadline will be reinstated and LGPD will become effective in February 2020. Because LGPD did not revoke any pre-existent sector-specific laws, specific obligations may continue to apply to organisations based on such laws, in addition to the requirements imposed by LGPD. In this sense, depending on the nature of the services and the entity, fintechs may be subject to the Banking Secrecy Law which imposes strict confidentiality for customer data and financial transactions, applying to both individuals and legal entities.

Also, there are general principles and provisions on data protection and privacy established in the Brazilian Constitution, in the Brazilian Civil Code, in the Brazilian Consumer Code and in Law No. 12,965/2014 (Internet Act). In addition, Resolution No. 4,658/2018, issued by the CMN, regulates cybersecurity and the engagement of third parties to provide cloud computing and data services to financial institutions or entities authorised to operate by the Brazilian Central Bank.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

LGPD is applicable to any processing operation performed by an individual or legal entity, whether public or private, regardless of the means, the country where it is headquartered or the country where the data is located, provided that: (i) the processing operation occurs on Brazilian territory; (ii) the processing operation has the goal of offering or providing goods or services or such operation relates to the personal data of individuals located on Brazilian territory; or (iii) the personal data was collected on Brazilian territory. In this sense, if an organisation established outside Brazil meets the conditions above, the organisation shall be subject to LGPD. In addition, the Brazilian Internet Act also applies to organisations even if they are not established in Brazil, to the extent that they offer services in Brazil or have customers located in the country. If the fintech is a controlling party or affiliate of another Brazilian entity, the latter may be held liable for acts attributed to the fintech, on a joint liability regime.

With respect to international data transfer, LGPD restricts this operation to the legal bases outlined in the law. In this regard, international data transfers may only be carried out: (i) to countries with an adequate level of protection, as defined by the Brazilian data protection authority; (ii) through the use of standard contractual clauses, binding corporate rules, seals, certificates and codes of conduct approved by the Brazilian data protection authority; (iii) when authorised by the Brazilian data protection authority; (iv) with the specific consent of the data subject; (v) to comply with a legal or regulatory obligation; (vi) when necessary for the performance of a contract; (vii) for the regular exercise of rights in judicial, administrative or arbitral proceedings; (viii) for the protection of the life and physical safety of the data subject or third party; (ix) when necessary for international legal cooperation between intelligence,

investigation and prosecution public bodies, in accordance with the instruments of international law; (x) based on a commitment made in an international cooperation agreement; or (xi) when necessary for the execution of public policy or compliance with the legal attribution of the public service.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

Generally, violation of privacy rights gives rise to compensation for moral and direct damage. Non-compliance with the provisions of LGPD may result in (i) a warning, (ii) the mandatory disclosure of the data incident, (iii) the deletion or blocking of personal data, and/or (iv) fines up to 2% of the company's economic group gross revenues in Brazil in the preceding fiscal year, excluding taxes, but limited to a total of R\$ 50 million per violation. The Brazilian Consumer Code imposes criminal liability (imprisonment from six months to one year) for certain types of conduct that may qualify as a crime against consumers, although imposing criminal liability for violation of cybersecurity and data protection is extremely rare. In addition to civil, criminal or administrative sanctions that may apply depending on the circumstances, failure to comply with privacy rights under certain provisions of the Internet Act may subject fintechs to four different penalties that may be jointly applied: (i) a warning, with a deadline for any corrective measures; (ii) a fine of up to 10% of the economic group's revenue in Brazil in the previous fiscal year; (iii) temporary suspension of activities of collection, storage, retention or processing of records, personal data or communications in Brazil; and (iv) prohibition of activities of collection, storage, retention or processing of records, personal data or communications in Brazil. The Banking Secrecy Law's penalties may also affect the infringing entity.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

In accordance with LGPD, personal data controllers and processors are required to adopt security measures, both technical and organisational, suitable to protect personal data from unauthorised access and accidental or illegal destruction, loss, change, communication, or any other form of inappropriate or illegal processing. Such measures shall be adopted from the creation of any new technology or product, which will require organisations to implement a privacy by design approach. Other sectorial laws, such as those requirements imposed on financial institutions by Resolution No. 4,658/2018 of the CMN (as mentioned in question 4.1 above), may set forth specific cybersecurity requirements on organisations. Also, Decree No. 8,771/2016, which regulates the Internet Act, imposes certain security measures on internet application providers with respect to the storage of personal data that are applicable to fintechs. The Brazilian Internet Steering Committee (CGI) may recommend additional security measures and standards to be adopted by fintechs.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

All entities acting in the financial and capital markets in Brazil are subject to AML requirements and controls, which are mainly regulated by the CVM and the Brazilian Central Bank. Because

most fintechs will either be subject to direct regulation or act in association with regulated entities as outsourcers or business partners, they will usually be subject to those same controls, including being submitted to "know your client" and customer onboard procedures, as well as being required to report suspicious transactions to authorities, implement anti-corruption policies, perform screenings and maintain internal controls to prevent money-laundering acts. Such controls and requirements are currently under discussion by the CVM and the Brazilian Central Bank and, therefore, may be significantly altered soon.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

In relation to products or services provided by fintechs operating in Brazil to retail customers, the Brazilian consumer protection laws will also apply, bringing additional rights to such customers.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

Employees may be hired by oral or written agreement and registered in the Employment and Social Security Booklet (CTPS). Moreover, even if there is no contract among the parties, any individual working personally, on a regular basis, under subordination shall be considered an employee under Brazilian law, being entitled to all rights and benefits granted and assured by the labour system. In addition, employees may be dismissed with or without cause. In the latter case, the employer must pay a fine of 50% over all deposits made in the Severance Fund (FGTS) in the course of the employment agreement, among other severance entitlements. A Labour Reform implemented in 2017 has also brought the possibility of: (i) termination by agreement between the employer and employee; (ii) contractual agreement of certain work conditions for employees who have graduated from university or college and compensation higher than twice the maximum benefit paid by Social Security; and (iii) contracting an individual as an autonomous worker, with or without exclusivity and on a continuous basis or not, without considering him/her as an employee, to the extent that the individual is not working under subordination. The grounds that entitle dismissal for cause are provided by the Consolidation of Labour Laws (CLT) and statutory severance varies accordingly.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Employees are entitled, in general terms, to base salary, 13th salary, 30 days of paid leave with a 1/3 bonus, social security contributions and deposits in the FGTS, payments and benefits arising from collective bargaining agreements with the representative trade union, and transportation vouchers, among other benefits according to their personal situations (e.g., maternity leave for 120 days). Moreover, all employees must be registered at a trade union that represents regulated professions or the employer's economic sector, which may negotiate further benefits with the employer union or with the employer itself.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

Brazilian law applies to any employees rendering services in national territory, regardless of their origin or place of hire. All foreigners must have their employment agreements registered before the Ministry of Labour. The Brazilian Immigration Law contemplates the following types of visa: (i) visit; (ii) temporary; (iii) diplomatic; (iv) official; and (v) courtesy. The visitor visa holder cannot perform paid activities in Brazil, with some exceptions such as travel allowance and reimbursements. Brazilian companies that intend to bring a foreign professional to Brazil, to render specialised services in the name of the foreign company, may request a working visa in their favour, unless covered by one of the exceptions provided by law. Company officers may apply for a residence permit conditioned to an investment of R\$ 150,000 with the creation of 10 new job positions or R\$ 600,000.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

In Brazil, inventions can be protected by patents granted under Brazilian Industrial Property Law (BIPL), which was conceived under the TRIPS Agreement. In order to be entitled to protection under BIPL, an invention must satisfy the requirements of novelty, inventive step and industrial application. Software is not patentable under BIPL, nor any financial plans, principles or methods, which may, however, be subject to copyright protection.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Brazil follows the first-to-file principle for intellectual property ownership. A patent, trademark or industrial design will be owned by whoever applies for and obtains its respective registration/grant from BIPL, which provides a few exceptions to this rule under the prior-user doctrine. Copyrights are protected regardless of any prior registration. However, registration may be useful to prove prior possession of a certain software source code.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

Brazil is a signatory party of the TRIPS Agreement, the Patent Cooperation Treaty, the Paris Convention and the Berne Convention. Nonetheless, in order to be enforceable within Brazil, intellectual property rights (excluding copyrights) must be filed and registered/granted by the INPI, in accordance with BIPL. Another exception is the protection granted to well-known marks by BIPL (in accordance with the Paris Convention) that states that well-known marks in their branch of activity will be granted special protection regardless of filing or registration in Brazil.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

There are no specific restrictions for the licensing of copyrights, including software. Restrictions apply to the monetisation of patents, industrial designs and trademarks, as well as unpatented technology. Foreign royalty remittances can only take place if the agreement is registered with the INPI and the Brazilian Central Bank. The INPI used to interfere on several conditions in the agreements subject to the INPI registration. Specifically, the INPI established that holders of a non-patentable technology cannot license technology to Brazilian parties, but rather can only assign it (i.e., transfer it permanently). In this regard, the INPI used to prevent foreign licensors from limiting the rights granted to Brazilian licensees under technology transfer agreements during, as well as after, the commercial relationship. The INPI could refuse to register a technology transfer agreement that establishes that modifications/improvements made by a licensee on the licensed technologies would belong to the licensor. Restricting the licensee's rights to continue using the transferred technology upon the expiration of the transfer of technology agreement was also not deemed acceptable by the INPI. Several limitations as to the amount of royalties payable abroad were also imposed. Nonetheless, the INPI issued a new ruling (IN 70/2017), reducing the scope of its analysis in the agreement registration process. Therefore, there is an expectation that more flexibility will be allowed in such sorts of arrangements.


Larissa Lancha Alves de Oliveira Arruy

Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados
Al. Joaquim Eugênio de Lima 447
São Paulo – SP, 01403-001
Brazil

Tel: +55 11 3147 2618
Email: larissa.arruy@mattosfilho.com.br
URL: www.mattosfilho.com.br

Larissa represents financial institutions, financial market infrastructures and other financial services providers and fintechs, as well as public companies and investors in financial transactions, with emphasis on banking and capital markets regulations. She advises clients on regulations issued by the Brazilian Securities Commission and the Brazilian Central Bank and is a frequent lecturer in financial regulatory matters. Her expertise includes matters related to payment systems, financial services, clearing and settlement of funds, fintechs, technology, innovation and digital business. Larissa graduated from Universidade de São Paulo (USP) with a Bachelor of Laws and has a specialisation in business administration from Fundação Getúlio Vargas (FGV).


Fabio Ferreira Kujawski

Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados
Al. Joaquim Eugênio de Lima 447
São Paulo – SP, 01403-001
Brazil

Tel: +55 11 3147 2795
Email: kujawski@mattosfilho.com.br
URL: www.mattosfilho.com.br

Fabio practises in the telecoms, intellectual property and technology areas with expertise in transactional and regulatory matters affecting these industries. He advises companies in a wide range of corporate matters, domestic and cross-border. He is the co-author and editor of the book "Legal Trends in Technology and Intellectual Property in Brazil" (2014), an officer of the Brazilian Information Technology and Telecommunications Association (ABDTIC) and a member of the Brazilian Association of Intellectual Property (ABPI). He has a Bachelor of Laws from Pontifícia Universidade Católica de São Paulo, and a Master of Laws in International Economic Relations, also from Pontifícia Universidade Católica de São Paulo.

MATTOS FILHO >

Mattos Filho, Veiga Filho,
Marrey Jr e Quiroga Advogados

Mattos Filho has more than 30 practice areas covering a wide range of legal services (such as Banking, Financing, Intellectual Property, Antitrust, Capital Markets, Corporate and M&A, Infrastructure and Project Development, Tax, Innovation, Technology and Digital Business, etc.). We are recognised for our innovative legal solutions to the most complex cases and for our steadfast commitment to remain the firm of choice for our clients. Such clients include large domestic and foreign corporations, major financial institutions, financial market infrastructures such as exchanges, clearings and trading platforms, fintechs, investors, multilateral agencies, investment funds, pension funds, insurers and reinsurers, public and private companies in various industry sectors, non-profit organisations and government entities. We assist both foreign clients in Brazil and companies doing business abroad. Our lawyers' multicultural background qualifies our firm to act in an extensive range of challenging cases involving clients from around the world. Mattos Filho provides legal advice to all international major players in the financial, technology and payments markets, including names such as Visa, Google, IBM, Amazon, Microsoft, Worldpay, Stone, Goldman Sachs, Cielo, B2W, PagSeguro, Geru, Brazilian Fintechs Association (ABFintechs), Brazilian Digital Credit Association (ABCD) and other fintechs on their regulatory compliance in everyday activities, as well as private equity funds, venture capital and other investors in these markets.

Canada



Pat Forgiore



Anthony Pallotta

McMillan LLP

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Canada is a business-friendly jurisdiction that has a wide array of fintech businesses, at all stages of growth, operating throughout the country. In 2018, Canada continued to follow through with announcements made in its federal budget to promote innovation in Canada. Notably, in February 2018, the Canadian Government named five technology groups that will have access to approximately \$950 million in federal funding, over five years, as part of the government’s “superclusters” initiative. The purpose of this initiative is to develop innovation hubs across Canada within which businesses, academic institutions, and not-for-profits can collaborate, with the goal of promoting innovation.

As the Canadian fintech sector continues to grow, large financial institutions are increasingly investing in, and partnering with, fintech businesses as they look to develop their own solutions. Investment in AI and robo-advisory initiatives has been a particular area of focus for Canadian banks. This past year also saw developments in payment technology, following the December 2017 report published by Payments Canada, which provided details on its payment systems modernisation project. In September 2018, the Government of Canada also announced the establishment of the Advisory Committee on open banking, which is a significant step in its review of the merits of open banking in Canada. The Advisory Committee released a consultation paper on the merits of open banking in January 2019, and a final report is expected to be issued in late 2019 after completion of the consultations.

There was also significant activity over the past year in the cryptocurrency subsector. Specifically, in February 2018, the first blockchain exchange-traded fund (“ETF”) launched and began trading on the Toronto Stock Exchange, and was followed by two additional blockchain-related ETFs later in the year.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

There are no prohibitions or restrictions that are specific to fintech businesses in Canada. However, the growing interest in

cryptocurrencies prompted the Canadian Securities Administrators to release a Staff Notice (46-307 – *Cryptocurrency Offerings*) indicating the continued applicability of Canadian securities laws to cryptocurrency offerings.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

With respect to funding, Canada has both mature debt and equity capital markets which are accessible to any business that meets the threshold limits. To date, only a limited number of Canadian fintech businesses have elected to raise significant capital through traditional financings, such as initial public offerings. Instead, fintech businesses have opted to rely on a number of alternative financing sources, such as venture capital.

Specifically, it appears as though much of the funding for fintech businesses in Canada comes from venture capital investment and other forms of early-stage financing. In an effort to broaden the scope of traditional equity financing, new crowdfunding rules were introduced in 2016 by a number of jurisdictions across Canada which provide retail investors the ability to participate in the raising of capital for small businesses. For instance, Ontario has introduced crowdfunding regulations, which provide companies with the capacity to raise funds from retail investors publicly without the need to file a traditional prospectus. However, investors are only permitted to invest \$2,500 per company up to a maximum of \$10,000 in the same calendar year (the cap is higher for certain qualified investors), and companies must prepare a document which meets a certain prescribed level of disclosure regarding the business and use of proceeds relating to funds raised from crowdfunding. In the first half of 2018 alone, investment in fintech start-ups through venture capital and M&A has totalled \$263 million across more than 50 transactions in the fintech space.

In addition, since 2015, a growing number of peer-to-peer lenders have sprung up in Canada. For example, one provider allows lenders to contribute as little as \$25 to a pool of money destined for a small business. While marketplace lending in Canada is still in its infancy compared to other jurisdictions, the proliferation of online platforms has created another financing source for fintech businesses.

More broadly, the Canadian Government has also demonstrated an increased commitment to providing funding for innovation in its 2018 federal budget.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

There are a number of incentive schemes used throughout Canada to encourage investment in small and medium-sized enterprises (“SMEs”), including those in fintech. The Canadian Government offers the following incentives for SMEs and growing businesses:

- The Scientific Research and Experimental Development Program encourages research and development in Canada by providing tax incentives to qualifying non-Canadian and Canadian companies. Certain non-Canadian companies are eligible to claim tax credits in respect of qualified expenditures (for scientific research and experimental development), while certain Canadian-controlled private corporations may be entitled to claim enhanced refundable credits.
- The small business deduction subjects qualifying Canadian-controlled private corporations to a reduced rate of income tax on qualifying income.
- The Industrial Research Assistance Program (“IRAP”) offered by the National Research Council of Canada assists firms in developing technologies and successfully commercialising them in a global marketplace by providing financial assistance, advisory services, and connecting SMEs with industry experts and potential business partners. The IRAP also provides SMEs with financial assistance to hire young talent.

Businesses can further benefit from a number of provincial grants and tax incentive programmes that reduce the cost of conducting business in the respective provinces. Similarly, both federal and provincial governments offer a large number of funding initiatives for SMEs and start-ups.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

In order to secure a listing on either the Toronto Stock Exchange (“TSX”) or the TSX Venture Exchange (“TSX-V”) – the two main exchanges for equity securities in Canada – an issuer must complete both a listing application and a prospectus (which will be a base disclosure document in connection with an IPO) which demonstrate that the issuer is able to meet the minimum listing requirements of the applicable exchange. The requirements for listing on the TSX, the exchange for senior issuers, will be more onerous than a listing on the more junior TSX-V. In addition, the minimum listing requirements will vary to some extent depending on the nature of the business; both exchanges categorise issuers according to industry segment.

At a high level, a listing on the TSX would require compliance with the following key requirements:

- the issuer must have at least one million freely tradable shares having an aggregate market value of at least \$4 million held by at least 300 public holders;
- the issuer must provide evidence of a successful operation or, where the company is relatively new and its business record is limited, there must be other evidence of management experience and expertise; and
- the issuer must publish an approved long-form prospectus.

In contrast, the minimum listing requirements for the TSX-V recognise that the emerging companies who are applying for listing have different financial needs than more established businesses. The TSX-V classifies issuers as “Tier 1” or “Tier 2” based on

standards, including historical financial performance, stage of development and financial resources.

The basic distribution requirement for Tier 1 issuers is at least one million freely tradable securities held by at least 250 public shareholders. The basic distribution requirement for Tier 2 issuers is at least 500,000 freely tradable securities held by at least 200 public shareholders.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

Shopify Inc. remains the leading case study for equity financing of Canadian fintechs. Most notably, the e-commerce giant has raised over \$131 million since its initial public offering on the New York Stock Exchange and TSX in May 2015, and has raised a total of \$253 million since 2007.

On November 15, 2017, Katapult, a fintech company focused on cloud-based investment software, received approval to go public. Currently listed on the TSX Venture Exchange, the company was able to raise \$1.6 million in its IPO.

In terms of acquisitions or sales, there were a number of notable acquisitions in Canada or involving Canadian fintech companies in 2018. On June 19, 2018, PayPal Holdings, Inc. announced the acquisition of Hyperwallet, a global leading payout platform based in Vancouver, for approximately \$400 million in cash. On March 9, 2018, Purpose Financial LP acquired the Montreal-based leading fintech lender to small business, Thinking Capital Financial Corporation, with the deal estimated to be valued at over \$200 million. Consistent with the AI trend discussed above, in January 2018, Toronto-Dominion Bank announced the acquisition of artificial intelligence start-up, Layer 6 AI, in a deal estimated to be in excess of \$100 million. Other notable transactions include the acquisition of Lendful Financial Inc. by Peoples Trust Company in June 2018, and the acquisition of Zensurance by US-based The Travelers Companies, Inc.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

There is no single Canadian regulatory body, either at the federal or provincial level, which has jurisdiction over fintech businesses. Rather, depending on the type of services provided by the fintech business, a number of regulatory bodies will have jurisdiction.

In particular, fintech businesses that provide banking, consumer credit and insurance services, or capital-raising services, will find themselves subject to the same regulations as incumbent businesses in these areas. In addition, fintech businesses generally will find themselves subject to more general business regulations such as privacy laws (either under the *Personal Information Protection and Electronic Documents Act* or *Canada’s Anti-Spam Legislation*), anti-money laundering laws, or consumer protection laws.

Any company that wishes to engage in a regulated service should discuss with the applicable regulators to see if there are any regulatory exemptions available to them. In particular, securities regulators have been open to providing exemptions to certain securities legislation requirements for fintech businesses.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

In August 2017, the Canadian Securities Administrators (“CSA”) published Staff Notice 46-307 *Cryptocurrency Offerings* (“SN 46-307”), which provides guidance on the application of Canadian securities laws to cryptocurrency exchanges, initial coin offerings, initial token offerings, and cryptocurrency investment funds. The notice clarifies that fintech businesses engaged in the cryptocurrency space may fall under the jurisdiction of Canadian securities regulators. In classifying a coin or token as a “security”, regulators will consider the substance of the instrument. This approach is consistent with securities regulation in other countries.

In June 2018, the CSA published Staff Notice 46-308 *Securities Law Implications for Offerings of Tokens* (“SN 46-308”), which expands on SN 46-307. The notice provides guidance on when a token offering might involve the offering of securities, as well as guidance on offerings of tokens in a multi-step structure. The notice also provides 14 example situations involving tokens and their resulting securities regulation implications.

In 2014, the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (“PCMLTFA”) was amended to apply to those “dealing in virtual currencies” subject to the development of updated regulations. In June 2018, the Canadian Department of Finance published draft amendments to the regulations under the PCMLTFA which introduce a definition of virtual currency, and treats those dealing in virtual currencies as money service businesses for the purposes of the PCMLTFA. These regulations will come into force on the first anniversary of the day on which they are registered (which has not yet occurred). See question 4.5 for more details on the PCMLTFA.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

Financial regulators and policymakers in Canada are cautiously receptive to fintech innovation. The current federal government has made its innovation agenda a priority.

A number of key regulators, including the Department of Finance, the Competition Bureau, and most provincial securities regulatory agencies have taken steps towards developing a fintech regulatory framework. For example, in 2017, the Competition Bureau released a market study entitled “*Technology-Led Innovation in the Canadian Financial Services Sector*”, which acknowledges that Canada “lags behind its international peers when it comes to Fintech adoption”. The study provides recommendations to Canada’s regulators and policy makers, focused both on technical improvements and on broader policy objectives, that would modernise fintech regulation and foster a more innovative and competitive environment.

In 2017, the CSA launched its own regulatory sandbox, which has assisted with capital raising fintech businesses, particularly in the cryptocurrency space (for example, TokenFunder, as mentioned above). This initiative is in addition to the existing crowdfunding regimes and provincial securities regulator programmes, such as Ontario’s Launchpad programme, which helps fintech businesses navigate securities regulations in Ontario. Ontario’s Minister of Finance also announced a commitment to create a “regulatory super sandbox”. The super sandbox will provide certain regulatory exemptions to businesses in the fintech space in order to facilitate

experimentation with business models, products and services. The commitment to the “regulatory super sandbox” was made by the Ontario government in its March 2018 budget.

In 2018, the federal government announced plans to modernise the fintech regulatory environment as it concerns federally regulated financial institutions (“FRFIs”). This includes amendments to key financial system legislation such as the *Bank Act*, the *Insurance Companies Act*, and the *Trust and Loan Companies Act*. The amendments will allow FRFIs to better participate in the fintech sector by permitting FRFIs with the ability to, among other things, engage in fintech activities in-house or through a third party, collect and transmit certain information, and invest in fintech entities. These amendments are not yet in force and regulations relating to these amendments have not yet been issued.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

The same regulatory framework that applies to local businesses operating in regulated environments such as banking or insurance also applies to foreign businesses. Further, as long as a fintech business interacts with Canadian consumers it will fall under the jurisdiction of the existing Canadian regulatory framework.

There are also additional regulations that apply to overseas fintech businesses in certain regulated spaces, including banking and insurance. For example, foreign banks operating in Canada generally cannot accept deposits of less than \$150,000. However, some inroads have been made in reducing regulatory burdens on incoming foreign businesses. Several provincial securities regulators have entered into cooperation agreements with other jurisdictions, which include Australia, France, Abu Dhabi and the United Kingdom, to refer and support fintech businesses.

In addition, in August 2017, the United Kingdom’s Financial Conduct Authority announced the formation of the Global Financial Innovation Network (GFIN) which is comprised of 12 securities regulators from around the globe (including Ontario and Quebec). The main functions of the GFIN will be to enable collaboration and shared innovations between markets, to provide a forum for joint policy work and discussion, and to provide companies with an environment to test cross-border solutions.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

Canada has both public and private sector legislation that regulates the collection, use and disclosure of personal information. Most notably, the federal *Personal Information Protection and Electronic Documents Act* (“PIPEDA”) applies to all private sector organisations in Canada, except in provinces that have enacted “substantially similar” legislation. Currently, only Alberta, British Columbia and Quebec have enacted substantially similar legislation that is applicable in place of PIPEDA. There is also sector-specific legislation (particularly with regard to personal health information)

pertaining to the maintenance of data that may be applicable to certain fintech businesses.

Most privacy legislation throughout Canada, and some sector-specific legislation, contains some or all of the following obligations that are applicable to fintech businesses:

1. informed/knowledgeable consent to the collection, use and disclosure of personal information;
2. openness about information-handling practices (some legislation has specific notice and/or policy requirements);
3. continued responsibility for personal information that is transferred to a service provider; and
4. security measures appropriate to the sensitivity of the information (some legislation contains more specific security requirements).

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

Canadian privacy laws apply to foreign organisations that conduct business in Canada. Also, PIPEDA applies to organisations that disclose personal information across a provincial border in the course of commercial activity and, generally, where an organisation in Canada receives or transmits personal information from or to a destination outside of Canada.

Some Canadian privacy legislation presents barriers to international transfers of data. For instance, public sector privacy legislation in British Columbia and Nova Scotia provide that public bodies must ensure that personal information under their custody or control is only stored and accessed in Canada. The only potential exception to this requirement is obtaining consent from appropriate individuals to the cross-border transfers of personal information. Quebec privacy legislation also contains restrictions on transferring personal information outside of Quebec, unless the organisation can ensure an equivalent level of protection is afforded. Most private sector privacy legislation, such as PIPEDA, also hold organisations responsible for safeguarding personal information even where such information is transferred to third-party service providers. The practical effect of this obligation is that organisations must enter into contracts with service providers to ensure an adequate level of protection.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

Liability for breaches of Canadian privacy legislation can arise in a number of ways, including complaints filed by groups or individuals, as well as audits or investigations initiated by the relevant privacy commissioner or other regulatory body. Penalties under the various statutes vary, but can include substantial fines in some cases, as well as prosecution of individual offenders.

Of note, PIPEDA was amended as of November 2018 to introduce breach notification, reporting and recording requirements in certain circumstances. Failing to report or record a breach in certain circumstances is an offence punishable by fines of up to \$100,000.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

Generally, cybersecurity laws and regulations arise in the context of protection of personal information. As indicated above, most privacy legislation requires that organisations protect personal

information from theft, loss or unauthorised access. The nature of the safeguards will depend on the sensitivity of the information. In the healthcare space, several provinces have enacted personal health information protection statutes which have more onerous data protection obligations given the sensitive nature of healthcare information.

Additionally, Canada's anti-spam legislation contains provisions governing software installation in the course of commercial activities and prohibits the sending of commercial electronic messages without the recipient's consent. While non-binding, a number of regulatory agencies such as the CSA and OSFI have also issued guidelines on cybersecurity to create a set of industry standards.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

Canada's primary anti-money laundering legislation is the PCMLTFA, which has the main objective of helping detect and deter money laundering and the financing of terrorist activities. The PCMLTFA also provides the framework to facilitate the investigation and prosecution of money-laundering and terrorist activity-financing offences.

The PCMLTFA applies to all "reporting entities" which include, among others, financial entities (such as regulated banks, credit unions, trust companies and loan companies regulated under provincial legislation), life insurance companies, securities dealers and money services businesses. There is no anti-money laundering or other financial crime legislation that specifically applies to the fintech sector. Fintech entities need to determine individually whether their activities would make them a "reporting entity" for the purposes of the PCMLTFA.

The specific requirements for each of the different types of reporting entities may differ under the PCMLTFA. However, all reporting entities will be required to: (i) establish a compliance regime and conduct a risk assessment relating to money laundering; (ii) comply with specified record keeping and client identification requirements; (iii) report suspicious financial transactions and attempted transactions as well as terrorist property to the Financial Transactions and Reports Analysis Centre of Canada ("FINTRAC"); and (iv) report certain cross-border movements of currency and monetary instruments to the Canada Border Services Agency. FINTRAC was established pursuant to the PCMLTFA as the agency responsible for the collection, analysis and disclosure of information to assist in the detection, prevention and deterrence of money laundering and terrorist financing in Canada. In addition to complying with the foregoing, money services businesses are required to register with FINTRAC and must supply information about themselves and their activities.

In 2018, the Department of Finance published draft amendments to the PCMLTFA, which among other things, seek to modernise the legal framework and align regulations with international standards. The proposed amendments address areas including prepaid cards, virtual currencies, and foreign money service businesses. The proposed amendments will effect changes to certain identification and authentication requirements, as well as certain recordkeeping requirements, which may benefit some fintech businesses. Examples include the ability to rely on third parties to perform identify verification, and the permitted use of scans and photocopies of identification. The regulations will come into force on the first anniversary of the day on which they are registered (which has not yet occurred).

Apart from this, compliance may be required with separate legislative measures against terrorists, terrorist groups and other

listed and sanctioned individuals and entities (“**Designated Persons**”) pursuant to various Canadian federal statutes (such as the *Criminal Code*) and their regulations, which require, among other things, that a financial institution or other person will not deal directly or indirectly in any property (including money) that is owned or controlled by or on behalf of a Designated Person, will not facilitate any transaction in respect of such property, and will not provide any financial or other related services in respect of such property. Also, other Canadian federal legislation such as the *Special Economic Measures Act* (“**SEMA**”) and its regulations may apply financial sanctions, and such legislation may include lists of designated individuals and entities with whom certain financial transactions are prohibited.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

In addition to the regimes discussed above concerning anti-money laundering, privacy and cybersecurity, the other regulatory regimes that may apply to fintech businesses include consumer protection legislation and competition legislation. Each province has their own applicable consumer protection legislation, which provides certain rights such as protection against misrepresentation and delivery of goods, as well as cost of credit disclosure requirements. Similarly, competition legislation includes regulations to prevent the use of deceptive marketing practices.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

In Canada, legislative authority over labour and employment is divided between the federal and provincial governments. The federal government has jurisdiction over employment laws for specific works and undertakings within exclusive federal jurisdiction, such as shipping, railways, broadcasting, airlines and banks. With respect to hiring, employers in the fintech industry should ensure that: (i) they understand which jurisdiction applies; (ii) the terms and conditions of employment offered to a candidate meet the minimum requirements prescribed by applicable employment standards legislation (further described in question 5.2); (iii) their recruitment and hiring processes are consistent with applicable human rights and privacy legislation; and (iv) pre-employment testing is conducted in accordance with applicable consumer reporting legislation.

There is no “at will” employment in Canada. With respect to the termination of the employment relationship, the analysis begins with an examination of whether there is “cause” for the dismissal, followed by an assessment of the employer’s obligations in connection with the dismissal. An employer is generally only entitled to dismiss an employee from employment without notice where it has “cause” in law to do so. Termination of employment for cause is considered “exceptional” and a substantial burden is placed on an employer to establish that it has cause to end the employment relationship without notice.

In the absence of a cause for dismissal, employers must generally provide employees with a working notice of termination of employment or pay *in lieu* of notice. An employee’s entitlements on termination without cause arise from three potential sources: (i) minimum standards established by applicable employment standards

legislation; (ii) the right to reasonable notice of termination at common law; and (iii) termination provisions in an enforceable, written employment contract.

5.2 What, if any, mandatory employment benefits must be provided to staff?

As noted above, each jurisdiction in Canada has employment standards legislation that sets out the minimum standards that govern the basic terms and conditions of employment for workers, including minimum wage levels, vacation and holiday pay, hours of work, pregnancy and parental leave, notice periods for termination, and severance payments. Employers and employees are not permitted to contract out of these minimum standards.

All employers, whether federally or provincially regulated, must also contribute to both the Canada Pension Plan and Employment Insurance on behalf of their employees. Contributions may then be deducted as a business expense for income tax purposes. Furthermore, employers must deduct and remit income tax, Employment Insurance premiums and Canada Pension Plan contributions to the appropriate authorities on behalf of their workers.

There is no obligation to provide group insured benefits, wage replacement schemes, or supplemental pension plans.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

In general, only Canadian citizens or permanent residents can work in Canada without a valid work permit. Unless an exemption applies, Canadian companies in the fintech industry seeking to hire a foreign worker must obtain a Labour Market Impact Assessment (“**LMIA**”). In order to obtain an LMIA, among other things, the company will have to satisfy the Government of Canada that there is a need for a foreign worker to fill the job and that no Canadian worker is available to do the job.

However, some foreign workers will be able to obtain a work permit in Canada without applying for an LMIA if they are entering the country as intra-company transferees and will be working as senior executives, managers or specialised knowledge workers, or if their work and experience qualifies them as a professional under international trade agreements. Other exemptions may also be available depending on the circumstances.

Depending on the foreign worker’s country of origin, the foreign worker may also need a visa to enter Canada. As part of the visa application process, the foreign worker may require a medical examination and/or biometric fingerprint scans. If a visa is required, it is routinely sought at the time of application for a work permit. Depending on the foreign worker’s country of origin, the foreign worker may also require an electronic travel authorisation to fly to or transit through Canada.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

As fintech products are commonly based on computer software or applications, the protection afforded in Canada is typically through

copyright as a literary work (but it may also be protected as a trade secret or patent, depending on the circumstances).

Copyright may exist in the underlying code and other elements of the software, including the interface, graphics and icons used as part of the software. Copyright in Canada arises automatically when a work is created; however, registering a copyright with the Canadian Copyright Office entails significant benefits. Copyright can protect the software code and also databases, so long as the work meets the standards of skill and judgment and originality.

Typically, the Canadian Patent Office will not consider software as a patentable matter in itself; however, certain software-based patents may be available where the computer implemented invention includes steps that have a physical existence (this is because a patent cannot be granted in an abstract idea, but rather must have some physical manifestation). In Canada, there is no express prohibition against patenting “business methods” and they may be patentable in appropriate circumstances; i.e., where it is claimed in a manner which requires some form of physical manifestation.

Given the uncertainty that can surround the patentability of software-related subject matter, non-disclosure and confidentiality obligations by agreement are of paramount importance in protecting the disclosure of technical information.

Trademarks (registered and unregistered) can also protect the brand of the fintech product or service. There are benefits to registering a trademark in Canada, as registration confers rights across the country, acts as a presumption of those rights in court and expands the scope of remedies available to a trademark owner asserting infringement.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

In Canada, the general rule is that the first owner of copyright will be the author. One statutory exception to this rule is for works created by an individual in the course of his or her employment – as such works are automatically owned by the employer. However, if an entity contracts with a third party, such as a software developer for the creation of the software, then that third party owns the copyright unless there is a written agreement otherwise (assignment of copyright in Canada must be in writing in order to be effective).

One peculiar feature of Canadian copyright law is that the individual author holds “moral rights” in the works he or she creates. Moral rights are the rights to attribution (or the right to remain anonymous), and the right to the integrity of the work. Moral rights cannot be assigned but they can be waived. As a result, employers or other entities seeking to use copyright works should ensure they obtain moral rights from employees or individuals who created the works (or representations from the assignor that moral rights have been waived).

In Canada, a patent for an invention is owned by the inventor. The courts have held that as a general rule, an employee retains ownership of the patent rights in his or her inventions, subject to an agreement otherwise (or if the employee was “hired to invent”). As a result, employers and owners are encouraged to obtain written agreements confirming their ownership in patentable subject matter to avoid the uncertainties that can arise.

Currently in Canada, trademarks can only be owned by a single entity and any use of the trademark (or one confusingly similar thereto) by a third party (including subsidiaries or parents of the owner), must be under licence from the owner, where the owner maintains control over the character and quality of the goods or services offered with the trademark. Use of a trademark without such controls in place can render the mark non-distinctive and therefore vulnerable to challenge. Implied licences have been found by the courts, but written licences are recommended wherever possible.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

International copyright conventions, such as the Berne Convention, provide automatic protection in other countries for qualifying works. The WIPO Copyright Treaty also specifically deals with the protection of computer programs and databases under copyright. As copyright arises automatically upon the creation of the work, registration is not necessary to enforce those rights in court in Canada and an owner can claim statutory damages even where it does not have a registration. However, a registration provides presumptions in litigation that the authorship and ownership set out in the registration is accurate.

Patent protection in Canada may be secured through the national route or under the international (“PCT”) patent application systems.

Trademark rights can exist through registration (coupled with use) or by common law use (where no registration exists). However, common law rights only extend to the geographic region where the owner can establish that use of the trademark has resulted in sufficient reputation and goodwill. In contrast, a registration confers rights across Canada. It also expands the scope of remedies and damages available to an owner in the case of an infringement, and it acts as a presumption of trademark rights in court.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

Intellectual property is typically monetised by an assignment/transfer, licensing or the granting of a security interest.

**Pat Forgione**

McMillan LLP
 Brookfield Place, Suite 4400
 181 Bay Street
 Toronto, Ontario, M5J 2T3
 Canada

Tel: +1 416 865 7798
Email: pat.forgione@mcmillan.ca
URL: www.mcmillan.ca

Pat is a partner in the firm's Financial Services Group, where he practises business and financial services law with a focus on corporate and commercial financing, asset-based lending, syndicated lending, mezzanine financing and private equity. He has extensive experience in fintech, documenting numerous financing transactions involving fintech companies at various growth stages. He also acts for major financial institutions on domestic and cross-border transactions. Pat also provides advice to fintech companies establishing a presence in Canada, as well as implications relating to a fintech company's collaboration with regulated financial institutions. Recently, he assisted The Canadian Institute in organising a fintech conference focusing on regulatory issues and challenges surrounding the industry.

Pat recently obtained the Osgoode Certificate in Regulatory Compliance and Legal Risk Management for Financial Institutions.

**Anthony Pallotta**

McMillan LLP
 Brookfield Place, Suite 4400
 181 Bay Street
 Toronto, Ontario, M5J 2T3
 Canada

Tel: +1 416 865 7850
Email: anthony.pallotta@mcmillan.ca
URL: www.mcmillan.ca

Anthony is an associate in the Financial Services & Restructuring group in the firm's Toronto office. He is currently developing a broad practice in Financial Services, which includes commercial debt financing, asset-based lending, secured transactions, and project financing.

Anthony is a graduate of the combined Juris Doctor and Honours Business Administration degree programme from Western University's Faculty of Law and Ivey Business School. Anthony joined McMillan in 2016 as a summer student and completed his articles with the firm in 2018.

McMillan is a modern, ambitious business law firm committed to client service and professional excellence. As a premier legal services provider in the financial services industry, McMillan is uniquely positioned to help clients exploit the opportunities and mitigate the risks that fintech brings. We have deep regulatory and transactional experience in all parts of Canada's financial services industry, in regulatory oversight and in public policy. We have experience at the highest levels of government, with a former Ontario Minister of Finance in our Toronto office, and lawyers at the leading edge of technology and innovation. While fintech is a young industry, we have built a significant track record of service for clients in the sector.

We are proud of our firm and its history of service to clients, community and the legal profession.

Cayman Islands

Peter Colegate



Anna-Lise Wisdom



Appleby

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

As one of the foremost offshore financial centres, home to approximately 70% of the world's offshore investment funds and with an absence of any direct taxation on companies or individuals, the Cayman Islands is well placed to become an attractive destination for technology entrepreneurs.

Tech City, a special economic zone within Cayman Enterprise City, houses some of the world's leading blockchain and fintech companies. The Cayman Islands is also host to a significant number of investment funds investing in cryptocurrencies and distributed ledger technologies and companies conducting token generation events.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

Crypto-to-crypto and crypto-to-fiat exchanges are currently prohibited as the Cayman Islands Stock Exchange is the only exchange permitted to operate in the Cayman Islands.

There are also potential restrictions on crypto-to-fiat conversions through an OTC desk or similar. Although the position is not currently clear, to the extent that cryptocurrencies can be both purchased with, and redeemed for, fiat currencies via a Cayman entity, such transmission is likely to fall within either the currency exchange or money transmission provisions of the Money Services Law and therefore requires a licence.

Cayman entities cannot be engaged in, or operating as, an online or offline gambling company or platform.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

Though there is no publicly available data on financing in this area, given the emerging nature of fintech business in the jurisdiction,

equity-based funding from, e.g., venture capital firms is more prevalent than debt financing at this time. Offshore investment funds investing in fintech and related businesses/technologies represent additional pools of funding. Further, to the extent that Cayman Islands issuers are involved in initial coin offerings (ICOs), this would constitute another important funding source (see question 3.2 below).

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

The Cayman Islands is a tax-neutral jurisdiction. There is no income tax, wealth tax, profits tax, capital gains tax, payroll tax, social security contribution (aside from mandatory pension contributions for employers and their employees) or corporate tax in the Cayman Islands. A registered Cayman Islands entity is not subject to any direct taxes. There may be tax implications for beneficial owners in their own jurisdiction, however.

The Cayman Islands Government has established a Special Economic Zone (the SEZ) which enables technology companies from outside Cayman to easily and cost-effectively set up and operate offshore with a genuine physical presence.

Benefits of being a resident in the SEZ include:

- no corporate, income, sales or capital gains tax;
- fast-track set up in four to six weeks;
- renewable five-year work/residency visas granted in five days for staff from outside Cayman;
- no Government reporting or filing requirements; and
- presence in a tech cluster with cross-marketing opportunities.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

The vast majority of Cayman Islands incorporated issuers will seek a listing on international exchanges such as NASDAQ or the Hong Kong Stock Exchange, in which case, the IPO will be governed by the laws of the jurisdiction of the relevant exchange. Foreign or Cayman Islands incorporated issuers seeking a domestic listing must first obtain approval from the Listing Committee of the Cayman Islands Stock Exchange. In brief, a listing document incorporating all disclosures necessary to enable an investor to make an informed assessment of the issuer's activities, assets and liabilities, financial position and management and prospects, among

other things, must be formally approved by the Listing Committee, and a number of other conditions set out in the Listing Rules of the Cayman Islands Stock Exchange must be satisfied. A company must be listed on the Cayman Islands Stock Exchange before inviting the public in the Cayman Islands to subscribe for its shares.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

There have not been any notable exits by the founders of fintech businesses in Cayman.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

There is no overarching regulatory framework for fintech businesses. In 2018, a number of working groups were established by the Government to agree a legislative approach to promote and regulate emerging technologies including blockchain and crypto assets.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

There is no separate framework for the regulation of ICOs in the Cayman Islands.

The primary piece of legislation regarding securities and investment business in the Cayman Islands is the Securities Investment Business Law (SIBL). SIBL provides for the licensing and control of persons engaged in securities investment business in or from the Cayman Islands. Importantly, SIBL is essentially consumer protection legislation, designed to protect the investing public and to be construed broadly. When determining whether a business activity is caught by SIBL, therefore, the emphasis is on substance rather than form.

SIBL sets out an exhaustive list of financial instruments that constitute “securities”. Cryptographic tokens are not included in that list. However, whether a token could constitute a security under SIBL is a fact-specific enquiry dependent on the unique functionalities exhibited by the token. If a token qualifies as a security, the issuer will be either dealing in, or arranging deals in, securities, although the issuer’s activities may fall within a list of excluded activities under SIBL.

A person who is not carrying on a securities investment business under SIBL may still bring themselves within the scope of the licensing requirements, where words are used in any language which connote a securities investment business in the description or title of the business in question; a representation is made in a document or any other manner that a person is carrying on investment business; or the person otherwise holds itself out as carrying on investment business. Care should be taken that no such language is used or representations made.

The issuer of a token in the Cayman Islands will also be subject to the general criminal laws on fraud and laws governing intentional or negligent misrepresentation.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

Yes. In 2018, a number of working groups were formed by the Government to establish the broad parameters for a legislative approach for Cayman to adopt to promote and regulate emerging technologies including blockchain and crypto assets. That consultation is ongoing.

As part of this consultation, in November 2018 the Government announced that a technology-neutral regulatory sandbox would be introduced to encourage, foster and incubate companies operating in this fast-moving sector. The Government has also confirmed that it is exploring how regulated digital identity solutions could help streamline and replace more traditional paper-based approaches to AML and KYC compliance.

Cayman Finance, a group that represents Cayman’s financial services sector, has established a fintech innovation lab to engage with the financial services industry, regulators, the Government and the media to promote the development of fintech in the Islands.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

A company incorporated in a jurisdiction other than the Cayman Islands may conduct business from within the Islands if it registers under the Companies Law as a foreign company. Carrying on business in the Islands includes “the sale by or on behalf of a foreign company of its shares or debentures and offering, by electronic means, and subsequently supplying, real or personal property, services or information from a place of business in the Islands or through an internet service provider or other electronic service provider”. Place of business includes a share transfer or share registration office.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

Cayman’s Data Protection Law (DPL) was passed in March 2017, and is expected to come into full force in September 2019. During the transition period secondary legislation and draft guidelines will be prepared, and the Office of the Ombudsman, which will be responsible for enforcing the new law, will be staffed.

The law was drafted with a view to achieving EU adequacy status to enable personal data to move freely between EU Member States and the Cayman Islands. Drafted around a set of EU-style data protection principles data controllers must adhere to, data must be collected in a fair and transparent manner and only be used and disclosed for purposes properly consented to by data subjects. Any

personal data collected must be adequate, kept up-to-date and should not be retained for longer than is necessary to fulfil the collection purpose.

The DPL adopts similar definitions to those found in most EU data protection laws.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

If a business is not established in the Cayman Islands, but nevertheless processes personal data in the Islands (otherwise than for transit purposes), it must nominate a local representative and state the local representative in its privacy notice. The local representative:

- must be established in the Cayman Islands;
- is, for all purposes within the Islands, the data controller; and
- bears all obligations of the data controller under the DPL.

The Cayman Islands has not yet achieved adequacy status from the EU. Transfers outside the Cayman Islands will be permitted under the DPL, but personal data shall not be transferred to a country or territory that does not ensure an adequate protection level for processing personal data.

Where the recipient country or territory cannot demonstrate an adequate level of protection, contracts or binding corporate rules can be put in place to control data transfers with third-party processors, or between members of the same group of companies. The DPL also sets out a number of exemptions from transfer restriction; for example, in instances where the data subject's consent to the transfer has been obtained, the transfer is in the public interest, or the Ombudsman has authorised the transfer.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

Refusal or failure to comply with an order issued by the Ombudsman is an offence.

The data controller is liable on conviction to a fine of C\$100,000 and/or imprisonment for up to five years.

The Ombudsman may also issue a monetary penalty order of up to C\$250,000, payable by the data controller.

Importantly, the Ombudsman also has the right to name data controllers found in breach of the DPL.

Where an offence has been committed by a body corporate, a director, company secretary, or similar officer could be held liable.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

No separate cybersecurity legislation has been enacted in the Cayman Islands. However, in 2016 the Cayman Islands Monetary Authority (CIMA) sent each of its licensees a notice making it clear that, going forward, the CIMA would be reviewing each licensee's approach to cybersecurity.

The DPL requires that "appropriate" technical and organisational measures be taken against unauthorised or unlawful processing of, accidental loss or destruction of, or damage to, personal data. The technical safeguards need to be appropriate to the types of personal data being processed.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

International standards of anti-money laundering and counter-terrorist financing are set by the Financial Action Task Force (FATF). As a member of the Caribbean FATF, the Cayman Islands implements recommendations promulgated by the FATF.

All Cayman Islands incorporated entities are subject to the Proceeds of Crime Law (2019 Revision) which sets out the principal money-laundering offences. Certain "relevant" businesses (which would include, for instance, entities caught within Cayman financial services regulations and other entities thought to be at a higher risk of money laundering) are also subject to the Anti-Money Laundering Regulations (2018 Revision), which prescribe certain identification, record keeping and internal control procedures for such businesses.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

The Electronic Transactions Law (2003 Revision) (ETL) generally puts electronic signatures on an equal footing with "wet ink" signatures in the Cayman Islands. Technologically neutral, the ETL was established to promote public confidence in the validity, integrity and reliability of conducting transactions electronically and recognises electronic records as records created, stored, generated, received or communicated by electronic means.

The Cayman Islands is an early adopter of the Common Reporting Standard promulgated by the OECD and is compliant with FATCA.

While the Cayman Islands has a long-established regulatory structure requiring that, subject to certain exceptions, beneficial owner information be requested by a licensed and regulated corporate service provider, verified in accordance with robust compliance mechanisms, and recorded, the Cayman Islands adopted a new beneficial ownership registration regime effective on 1 July 2017. Cayman companies and limited liability companies are required to maintain a register of beneficial ownership at their registered office, the contents of which register are copied regularly by the corporate service provider to a centralised data platform which can be searched electronically by the Cayman Islands' competent authority. The information is not accessible by the wider public and the existing gateways to legal access by the relevant authorities remain in place. A bill was gazetted in March 2019 that proposes to extend the regime to limited liability partnerships registered under the Limited Liability Partnership Law.

Following assessment by the EU Code of Conduct Group, the Cayman Islands was included in a list of jurisdictions which are required to address the Code Group's concerns about "economic substance". As a result, the International Tax Co-operation (Economic Substance) Law 2018 came into force on 1 January 2019, and certain entities incorporated or registered in the Cayman Islands and carrying on specified activities ("relevant activities") are required to have "adequate substance" in the Islands.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

All non-Caymanians employed in the private sector must have a work permit. An application for a full permit usually takes four to

six weeks to process. A streamlined regime exists for certain types of businesses that can be set up within the SEZ.

Permit costs vary depending on the sector (financial services, tourism or construction) and the skill level of employees. The costs range from an annual minimum of C\$300 for unskilled workers to in excess of C\$30,000 for certain senior management and professional roles. Employers are responsible for work permit fees and these must not be passed on to employees.

Permits are ordinarily renewable for a maximum of nine years. An employee can make an application for permanent residency when he has been in the Islands for a continuous period of eight years, and these applications are determined under a points-based system which examines various economic and social criteria.

5.2 What, if any, mandatory employment benefits must be provided to staff?

For most categories of employee, the employer must pay the premium under a health insurance contract issued by an approved insurer. However, the employer can recover up to 50% from the employee. Employers and eligible employees make mandatory contributions towards each employee's pension plan of 5% of the basic salary up to the maximum prescribed level of pensionable earnings.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

See our response at question 5.1 above.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

The Cayman Islands is a common law jurisdiction with a robust intellectual property protection regime.

In 2015 and 2016, the Cayman Islands updated its copyright laws to bring them in line with the most recent developments under the UK Copyright, Designs and Patents Act 1988, which expressly includes computer programs and databases within the definition of "literary works" and therefore protects them as such for a duration of 50 years.

Open-source code is not separately regulated or protected in the Cayman Islands. It is possible for every contributor to the open-source code to own the copyright to its contribution, although in practice most contributors are likely to agree to license their material under the same licence as the original work. It can sometimes be difficult to ascertain who should make a legal complaint if someone decides to use the program in a way that violates its licence. To avoid this issue, contributors can explicitly assign the copyright in their contributions to a centralised body that administers the open-source project, making enforcement of the licence easier. An alternative

approach would be to have contributors license their contributions to the project's administrative body under a licence agreement that permits the body to relicence these individual contributions.

The main IP rights available to protect branding are registered and unregistered trade and service marks. Fintech companies will generally own a combination of an established brand or trade name – and this can include logos or icons – protected as registered or unregistered trademarks.

Trade mark rights give registered owners the right to prevent others from using identical or confusingly similar marks to their registered mark. Brand owners can also rely on unregistered trade mark rights through the law of passing off. This allows the owner to prevent others from damaging its goodwill with customers by using branding or get-up that is identical or confusingly similar to its own.

Patents and industrial designs registered in the UK or at the European level can also be protected in the Cayman Islands by extension on application to the Cayman Islands Registrar of Patents and Trademarks. Also, the patent regime has been amended to provide innovators with additional protections against abusive challenges to their rights by entities that obtain patents for the sole purpose of taking legal action against those who innovate and develop new products. The Cayman Islands patent laws have been amended to prohibit bad faith infringement claims by so-called patent trolls.

Trade secrets are protected in the Cayman Islands through a combination of common law and rules of equity. A range of remedies are available where trade secrets have been improperly acquired, disclosed or used.

Confidential information is protected through a contractual agreement to keep certain information confidential or through the common law obligation to keep information confidential, because of the nature of the relationship between the discloser and disclosee, the nature of the communication or the nature of the information itself.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

See our response at question 6.1 above.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

See our response at question 6.1 above.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

In December 2018, the Cayman Islands introduced an economic substance requirement for certain companies operating in the Islands. Businesses in Cayman that hold, exploit or receive income from intellectual property assets may be impacted if they are not tax resident outside the Islands.

**Peter Colegate**

Appleby
71 Fort Street, George Town
PO Box 190, Grand Cayman, KY1-1104
Cayman Islands

Tel: +1 245 814 2745
Email: pcolegate@applebyglobal.com
URL: www.applebyglobal.com

Peter Colegate is a Senior Associate within the Corporate practice group where his practice is focused on privacy, data protection, intellectual property and strategic corporate-commercial and regulatory work in the technology, innovation and financial technology sectors. Peter is Joint Global Head of Appleby's Technology and Innovation Group and is based in Appleby's Cayman Islands office.

**Anna-Lise Wisdom**

Appleby
71 Fort Street, George Town
PO Box 190, Grand Cayman, KY1-1104
Cayman Islands

Tel: +1 345 814 2718
Email: awisdom@applebyglobal.com
URL: www.applebyglobal.com

Anna-Lise Wisdom joined Appleby in 2007 and is a Partner within the Corporate department in Cayman. She specialises in subscription financing and debt financing for private equity funds and regularly advises leading financial institutions in related credit facilities. She also has substantial experience in asset finance, particularly ship finance, corporate and acquisition finance and in capital markets transactions. Her practice extends to private equity and hedge fund formation, structuring and operation and she has also advised investment managers on related regulatory and licensing issues in relation to such funds.

APPLEBY

With technological innovation transforming businesses and markets in Cayman and with a burgeoning technology community on the Islands, Appleby has led the way amongst the offshore firms by launching a dedicated Technology and Innovation Team that sits within the Corporate group and supports clients across a broad range of emerging technologies.

Appleby's expert Technology and Innovation team operates in 10 highly-regarded, and well-regulated, global locations. These include the key offshore jurisdictions of Bermuda, the British Virgin Islands, the Cayman Islands, Guernsey, the Isle of Man, Jersey, Mauritius, and the Seychelles, as well as the international financial centres of Hong Kong and Shanghai.

Appleby's global presence enables it to provide comprehensive, multi-jurisdictional legal advice at the times most critical to clients.

China

David Pan



Xun Yang



Links Law Offices

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Fintech business in China continued to grow in 2018 whilst the risks of its fast development were gradually revealed. In response, the China government continues to strengthen the regulation over fintech businesses to tackle potential systematic risks brought by the application of fintech technology. This meets the government strategy that is to allow fintech business to grow in a relative flexible regime, and to only regulate it when the fintech business reaches a certain scale.

During 2018, a number of P2P lending companies in China collapsed. According to public statistics, by the end of 2018, around 1,800 platforms remained in normal operation, with only three-fourths of that of 2017; for the first time since 2007, the total amount of loan balance decreased by 4.18% to RMB 11,000 billion. Small and vulnerable lending platforms which developed fast by levelling on high margins were washed out of the market; this, on the one hand, created market crisis, but on the other hand, is a natural selection process helping shape a healthier market.

The Chinese government tightened its regulation on the online payment business. All companies engaged in online payment business were required by the *People's Bank of China* ("PBOC") to "cut-off" (stop) direct settlements with commercial banks at the end of 2017 so as to avoid money laundering. In addition, in June 2018, PBOC required that all reserves which online merchants deposit to online payment business operators be transferred to PBOC's account to ensure fund safety. Consequently, payment business operators were not able to benefit from the reserves. Despite these regulations, the online payment business experienced robust development last year. Public statistics indicated that the quarterly turnover reached RMB 48.3 billion in Q2 2018, nearly double the number of Q2 2017.

With the innovation of technology and creation of business solutions, new types of fintech business appeared in China, such as the provision of risk-controlling services driven by big data and automatic investment advice services powered by artificial intelligence. Although the issuance and trading of bitcoin are still banned in China, the Chinese government began to embrace the development of blockchain technology and services business. Blockchain-related business has attracted investment of RMB 33.5 billion in 451 deals in China during 2018, which almost accounted for half of the total amount of global investment in the blockchain sector.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

Initial coin offerings ("ICOs") are strictly prohibited in China. According to the *Alert on Preventing Token Fundraising Risks* (the "Risk Alert") issued by PBOC, token financing platforms and token trading platforms in China are not allowed: 1) to engage in the exchange between legal currency and e-coins; or 2) to provide information services or price services relating to ICOs. In addition, unless otherwise approved by government sponsors, all non-financial institutions are not allowed to offer or sell financial products (including in particular asset management products or plans) over the Internet. Under the current PRC legal regime, only very limited insurance products and public securities investment fund products, upon approval, are allowed to be publicly offered for sale to Chinese investors or consumers. Nevertheless, the *Cyberspace Administration of China* ("CAC") issued on January 10, 2019 the *Administrative Rule on Block Chain Information Services* ("Block Chain Rule"), which suggested that the development and provision of blockchain-related technology and services are permitted in China.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

A variety of financing sources are available for both new and growing businesses, covering both equity and debt. Generally, it is hard for start-ups to get straight-forward debt financing, and financing for start-ups is limited to equity or quasi-equity financing, such as angel funding, venture capital, crowd-funding, or, to a limited extent, convertible debt. Financing avenues for growing businesses are more diversified: debt financing sources for a growing company may include traditional financial institutions, micro-credit loan companies and even individuals. Equity financing mainly comprises of private equity funds and strategic investors.

In China, equity financing can be made in the form of debt. In this scenario, equity investors usually impose stringent restrictions and requirements on founders and management teams of the financed companies, such as the founders or the companies' obligations to buy back the investor's equity or shares under certain circumstances.

Preferred stock financing is uncommon because Chinese companies in general are not allowed to issue preferred stock.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

China has adopted comprehensive incentive schemes of tax incentives, subsidies, incubation funds and other preferential government policies. A “high-tech company” recognised by the government is entitled to a variety of preferential policies, including: 1) a reduced enterprise income tax rate of 15% (a 40% decline from the normal rate of 25%); 2) exemption of income tax on certain assignments or licensing of technology; 3) allowing accelerated depreciation of certain fixed assets; and 4) government subsidies paid to the company and talents hired by the company. The threshold for the qualification of a “high-tech company” can be relatively high, and not all tech businesses can be eligible. As to small and medium sized businesses, incentive schemes available may include fiscal subsidies, tax rebate, tax rate reduction, reduced debt costs, and government-led training programmes. Incentive schemes proffered by local governments may differ from one place to another.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

IPO markets in China mainly comprise of the main board (both Shanghai Stock Exchange and Shenzhen Stock Exchange), the small and medium enterprise (“SME”) board (exclusive to Shenzhen Stock Exchange) and the growth enterprise market (“GEM”) board (exclusive to Shenzhen Stock Exchange). The listing requirements for the main board and the SME board are the same, while the requirements for the GEM board are more lenient.

The main listing requirements for the main board and SME board are as follows:

- 1) three consecutive years of business operation;
- 2) no material changes in the major business, management team and actual controller in the past three consecutive years;
- 3) net profit being positive for the past three consecutive years and exceeding RMB 30 million in aggregate; and
- 4) net cashflow from operations exceeds RMB 50 million in aggregate over the past three consecutive years, or revenue exceeds RMB 300 million in aggregate over the past three consecutive years.

The main listing requirements for the GEM board are:

- 1) three consecutive years of business operation;
- 2) operating one primary business, which has not changed in the past two consecutive years;
- 3) no material changes in the management team and actual controller in the past two consecutive years; and
- 4) net profit being positive for the past two consecutive years, and aggregated the net profit exceeding RMB 10 million for the past two consecutive years, or net profit being positive for the past year and net profit exceeding RMB 5 million.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

Ever since Yirendai’s IPO on the New York Stock Exchange in 2015, a large number of Chinese fintech companies went for IPO.

Recent notable IPOs include Dian Niu Finance, Hui Fu Tian Xia, Wei Xin Jin Ke and 51 Credit Card. Due to restrictions imposed by securities regulations, however, founders of fintech businesses recently IPOed may not be able to sell their stock in the listed companies within a certain period after IPOs.

Some fintech businesses sold off part of their business, shifting their focus from “finance” to “technology”. Some P2P loan companies, struggling in the sluggish market, changed hands. These exits, however, may not be mere sales of business by the founders, but rather attempts to discharge financial liabilities or to avoid potential penalties resulting from past non-compliant conduct.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

Currently, there is no single comprehensive law which regulates the fintech businesses in China. Various administrative measures and guidance regarding financial products or services apply to fintech business operators.

PBOC jointly with eight other authorities issued *Guiding Opinions on the Promotion of Sound Development of Internet Finance* (“**Guiding Opinions**”), under which different sectors of “Internet Finance” were governed by different government departments. However, a later ministerial structure reform changed the regulation landscape. An overview of the regulatory regime for fintech business is summarised below:

Business	Regulator	Specific Legislation
Online Payment	People’s Bank of China	Administrative Measures for Payment Services Provided by Non-financial Institutions
P2P Lending	China Banking and Insurance Regulatory Commission	Provisional Rules for the Management of Services Activities of Internet Lending Information Intermediaries
Equity Crowd-funding	China Securities Regulatory Commission	Implementing Scheme of Dedicated Regulation on Risk of Equity Crowd-funding
Funding Sales on Internet	China Securities Regulatory Commission	Administrative Measures for Sales of Securities Investment Fund, and Administrative Measures for Supervision of Money Market Funds
Insurance Sales on Internet	China Banking and Insurance Regulatory Commission	Provisional Measures for Supervision of Internet Insurance Services
Online Trust Business and Consumer Financing	China Banking and Insurance Regulatory Commission	N/A
Blockchain Information Service	Cybersecurity Administration of China	Administrative Rule on Block Chain Information Services

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

ICOs are expressly prohibited in China. Nevertheless, PRC law is silent as to whether the transaction of cryptocurrencies or crypto-assets is legally permissible.

According to the Risk Alert, any individual or entities in China must not provide any service which is or has a similar nature as an ICO. However, the legality of other services relating to cryptocurrencies or crypto-assets, for instance, establishing an exchange for cryptocurrencies or trading of cryptocurrencies, is not expressly prohibited. In judicial practice, Chinese courts hold different views in this regard because the legal nature of cryptocurrencies status has not been well established. Some held that cryptocurrencies or crypto-assets can be protected as a “property right” under *PRC Property Law*, while others considered cryptocurrencies or crypto-assets merely a creditor’s right.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

In 2018, the financial regulators in China continued strengthening their control over fintech services. In particular, the *Special Working Group for Mitigating the Internet Financial Risks* issued the *Notice on Strengthening the Governance of the Provision of Assets Management Business through Internet and Proceeding with the Acceptance-related Work* (the “**No.29 Notice**”) in March 2018.

The Block Chain Rule issued by CAC also demonstrated the government’s efforts in strengthening the fintech market. According to the Block Chain Rule, all blockchain information service providers must file their business via an online management system within 10 days of their provision of service. If the blockchain information service provider fails to file with CAC or submits misleading information when filing, CAC and its local offices may issue a rectification order or, in serious cases, issue a warning and impose a penalty of up to RMB 30,000.

Although the mode of “sandbox regulation” has been heatedly discussed and was reportedly experimented with, China has not officially introduced a “sandbox” in regulating fintech businesses. Encouragingly, the Chinese government does commit to adopt “a prudent yet accommodative regulatory approach” for emerging industries.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

Except for very limited scenarios under the *Administrative Measure on the Registration of Enterprises of Foreign Countries (Regions) Engaging in Production and Operational Activities within the Territory of China*, where a foreign company can conduct business operations directly in China upon approval, PRC laws require that all foreign investors obtain a business licence prior to carrying out business in China; i.e., fintech business operators established outside China must have a business presence within the territory of China in order to operate legally in the Chinese market.

Except for online payment business, none of the regulators in China have specially provided for any policies on whether it is allowed for a foreign investor to provide fintech-related businesses, i.e. P2P lending, equity crowd-funding or internet insurance business, in China. PBOC issued *PBOC Announcement No.7* on March 21, 2018, which allowed foreign investors, subject to four conditions, to engage in payment business in China.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

Over the past decade, China has been strengthening its regulation on personal data protection, and has been introducing laws and regulations that regulate the full life cycle of personal data (from generation to destruction and any process in between). Lacking an overarching personal data protection law, China’s current personal data laws and regulations are scattered in criminal, civil and administrative laws and regulations. The *General Part of the PRC Civil Law* provides that a natural person’s personal data is protected by law, and that no one shall unlawfully collect, use, process or transfer personal data. The *PRC Criminal Law* further provides that sales or supply of personal information in violation of law, and theft or unlawful collection of personal data, constitute a criminal offence. The *Cyber Security Law* (the “**CSL**”) provides that network operators must collect or use personal data based on the principles of legality, legitimacy and necessity, and shall obtain the data subject’s consent. Acting as an important supplement to the CSL, the PRC national standard GB/T 35273 provides very detailed suggestive rules for companies to follow. There are also other administrative rules that govern certain industries or scenarios; for example, personal data protection obligations for financial institutions, or when consumers are involved.

Fintech businesses rely heavily on personal data to develop their business, such as precision marketing, online ads and personal profiling. Therefore, all above-mentioned laws and regulations may apply to fintech businesses.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

With the exception of applicable criminal law provisions, China’s data privacy laws generally do not have extraterritorial jurisdiction. They may nonetheless be applicable to organisations established outside of China if such overseas organisations collect or process the personal data of Chinese nationals, especially if such activities take place within China.

Currently, for data other than state secrets or state intelligence, only the outflow of personal data and so-called “important data” (defined as data closely related to national security, economic development, and social and public interests) by a critical information infrastructure operator (“**CIIO**”, defined as operators of infrastructure in certain key industries, whose destruction, loss of function or data breach may significantly harm national security, social welfare and public interests) is subject to restrictions imposed by law. Pursuant to the CSL, personal information or important data collected or generated by a CIIO in China may not be transferred out of China without

conducting a data cross-border transfer security assessment. Depending on the characteristics and nature of the personal data, the security assessment may be conducted by the CIO itself or by a government authority.

It is worth mentioning that a draft regulation on data cross-border transfer expands the security assessment obligations to all network operators. If the draft regulation is enacted “as is”, all companies operating in China need to conduct the aforementioned security assessment and can only export personal data and important data when the assessment results give the green light.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

In addition to civil damages that personal data subjects may claim, failing to comply with Chinese data privacy laws may have criminal and administrative consequences. Under the PRC Criminal Law, unauthorised collection, transfer or sale of personal data may constitute a criminal offence and the offender may be imprisoned for up to seven years. Under the CSL, network operators who violate personal data protection obligations may be charged a fine of up to 10 times of the illegal gains (in case there is no illegal gain, a fine of up to RMB one million), and individuals in charge of the network operator may be separately fined up to RMB 500,000. In addition to the CSL, there are a number of penalties provided in a variety of administrative regulations at different government levels.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

The CSL defines “network operator” very broadly so that basically every company with a network connection is obliged to comply with it, and fintech businesses are not an exception. In addition to the CSL, other cyber security laws and regulations may apply to fintech businesses as well, especially those that govern the financial sectors. For example, the *Guidelines on Data Governance of Banking Financial Institutions* provide that financial institutions’ collection and use of personal information shall comply with data protection laws and applicable national standards. The latest trend in this area is the Block Chain Rule. With regard to cyber security, the Block Chain Rule requires that blockchain information service providers shall comply with the CSL to verify user identity and shall not use blockchain information services to harm national security or social interests.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

In China, financial institutions are statutorily required to establish anti-money laundering (“AML”) mechanisms and procedures to fully identify, evaluate and safeguard against money-laundering risks. AML obligations are imposed by analogy to other quasi-financial institutions or non-financial institutions. Accordingly, PRC AML laws are applicable to fintech businesses that are financial institutions, quasi-financial institutions and certain non-financial institutions. A notable law that directly regulates fintech businesses is the *Internet Financial Institutions Anti-Money-Laundering and Anti-Terrorism Financing Administrative Rules* (tentative) (“**Tentative Rules**”), jointly issued by PBOC, the *China Banking and Insurance Regulatory Commission* and the *China Securities Regulatory Commission*. The Tentative Rules basically

imposed AML obligations applicable to traditional financial institutions, *mutatis mutandis*, to Internet financial institutions, which include but are not limited to online payments, online credit loans, online loan intermediaries, equity fund-raising, online fund sales, online trusts and online consumer finance companies.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

As business entities, PRC laws and regulations that apply generally to all business organisations apply to fintech businesses as well. In addition, there are laws and regulations that specifically regulate fintech businesses, especially Internet financial service providers such as P2P lending companies and Internet financial intermediaries. Other than those, laws and regulations that relate to intellectual property rights, Internet-based services, financial services and foreign investment may be of particular concern to fintech businesses.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

At the core of China’s labour-related legislation are the *PRC Labor Law* and the *PRC Labor Contract Law*, as well as their implementation rules. Government authorities at different levels can also issue laws, regulations and government orders to regulate local labour issues, provided they are not in contradiction with the *Labor Law* and *Labor Contract Law*.

The *PRC Labor Law* is pro-employee; just to name a few provisions:

- 1) except for a very limited number of legal grounds, employers may not terminate an employee’s labour contract unilaterally;
- 2) except when the employee is at fault (e.g., commits a crime or severely violates company policies) or when he resigns, even if the employer terminates an employee’s labour contract on valid legal grounds, the employer must pay the employee a lump sum severance calculated based on the employee’s length of services; and
- 3) in the event that i) an employee has been employed by the same employer for 10 consecutive years, or ii) the employer and the employee have entered into fixed-term labour contracts for a second time and upon the expiration of the second fixed-term labour contract, the employee is entitled to enter into a non-fixed-term (“permanent”) labour contract with the employer.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Chinese labour laws mandate a number of employment benefits to be borne by employers, and below we list some of the most common and important mandatory employment benefits:

- 1) annual leave: statutory paid leave calculated based on the employee’s labour seniority, ranging between five days per year to 15 days per year;
- 2) overtime compensation: except for a few exceptions (e.g. flexible working hours) that are subject to government approval, employees who work i) after working hours, ii) on

- weekends, and iii) on statutory holidays are entitled to overtime compensation ranging from 1.5 times to 3 times of their ordinary wages; and
- 3) social security benefits: employers must provide certain social security benefits to employees, which include maternity insurance, unemployment insurance, work injury insurance, medical insurance, endowment insurance and housing funds.

In addition to employment benefits provided in the *Labor Contract Law*, local government authorities may also issue labour-related regulations which require employers to provide additional employment benefits to employees.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

Any foreigners who intend to work in China must obtain: 1) a foreign work permit, which categorises foreign employees into three classes: Class A (top talents), Class B (professional talents) and Class C (other foreign employees); 2) a work visa: either a Z visa (for ordinary foreign employees) or an R visa (for foreign experts); and 3) a foreign residence permit.

There is no special route for foreign employees in the fintech sector. As mentioned above, however, foreigners who are “top talents” are eligible for a Class A work permit. Class A work permits are only issued to top talents that are urgently needed for China’s economic and social development, such as top scientists, leading scientific talents, international entrepreneurs, special talents and highly skilled talented persons. Accordingly, individuals in fintech businesses who are qualified as “leading scientific talents” or international entrepreneurs, etc. may apply to work in China under the Class A work permit, which provides a fast-lane process.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Similar to most other jurisdictions in the world, innovations and inventions in China may be protected as copyrightable works under the *PRC Copyright Law*, as patentable creations under the *PRC Patent Law*, and as trade secrets under the *PRC Anti-Unfair Competition Law*. Conditions for the protections are statutory. There is no common law or equity protection. However, in limited circumstances, especially with respect to new business models, innovations and creations may be protected according to the general principles of the *PRC Anti-Unfair Competition Law*, should the statutory protection conditions not be met. For example, in the context of fintech businesses, software and application interfaces may be protected as copyrightable works, innovative business models may be protected as process patents, databases may be protected as copyrightable works if they possess a unique and creative structure, and, to a certain degree, are protected under the *PRC Unfair Competition Law*.

In recent years, China has been improving its intellectual property systems and the protection level in China has been brought onto an international level. Despite the fact that there are still rampant infringements, especially in some online e-commerce platforms, IP awareness has been improved, protections have been strengthened, and, more importantly, the government has been making huge efforts to create an IP-friendly environment.

PRC courts have gradually expanded the scope for the granting of preliminary injunctive reliefs, from only trademark and copyright cases to patent and trade secret cases. The rules for seeking preliminary injunctive reliefs are clearer, and preliminary injunctive reliefs have been granted in an increasing number of IP-related cases.

China has formed specialist intellectual property courts in Shanghai, Beijing and Guangzhou, which are cities where most intellectual property cases are tried and also where fintech business is most prosperous. Additionally, the Intellectual Property Tribunal, a new subdivision in the Supreme People’s Courts, was formed at the end of 2018, and it is responsible for all appeal cases concerning invention patents, utility model patents, technical secrets, computer software, etc. As a result, any of these intellectual property cases would be appealed to the Supreme Court (rather than high courts at each province) if either party is not satisfied with the first instance decision, so that local protectionism can be avoided.

Moreover, China has established the first Internet Court in Hangzhou in August 2018, which is in charge of trying Internet-based disputes and online intellectual property infringements. The parties, judges, and clerks do not need to meet face to face; rather, the court proceedings can be run online and evidence can be digitalised and exchanged online. Blockchain technology has been creatively used to preserve and to present evidence.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Generally speaking, by operation of laws, intellectual property rights arising from innovations or creations vest in the parties which create them. In case of joint development, the joint developers co-own the innovations or creations. If a party engages another party to make an innovation or creation, the intellectual property rights vest initially in the party so entrusted; i.e., the party actually makes such innovation or creation and the engaging party receives the right to use it. However, the engagement agreed between the parties can provide otherwise in this regard.

With respect to innovations and creations made as works for hire: (i) the intellectual property rights vest in the employer if the innovations and creations are protected by patents or trade secrets, or if they are otherwise copyrightable engineering designs or computer programs; and (ii) the intellectual property rights vest in the employee if the innovations and creations are protected as copyrightable works, except for engineering designs or computer programs.

Moral rights always vest in those who make the innovations and creations, which cannot be assigned or waived; nor can their ownership be agreed otherwise.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

Under the Berne Convention requirements, the *PRC Copyright Law* recognises the protection of copyrightable works which are created outside of China. In other words, upon completion of any copyrightable works in any Berne member countries, such works are protected in China without any registration, filing or other procedural requirements.

Trade secrets are protected in China as well regardless of where they are developed, again with no registration, filing or other procedural requirements.

Patents and trademarks are subject to geographic restrictions. They are protected only when they meet the Chinese law requirements and are registered in China. The Patent Cooperation Treaty and the Madrid System, respectively, facilitate foreign patent and trademark holders to apply for protections in China.

It is worth noting that there are some statutory requirements for intellectual protections in China. For example, inventions made in China must undergo a security screening process in China before foreign patents can be sought in respect to them. Otherwise, they may lose protections in China.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

Under PRC intellectual property laws, IP may be exploited or monetised by means of licensing, assigning or, in some cases, as in-

kind capital contributions or as collateral for loans. According to a notice issued by the State Council in September 2017, intellectual property can also be securitised. In December 2018, the first intellectual property ABS was successfully issued, which is a milestone in IP monetisation.

The exploitation of intellectual property rights is subject to antitrust regulations. Except for those general rules under the *PRC Antitrust Law*, the *PRC Contract Law*, and the relevant judicial interpretations provide for certain restrictive provisions in technology related contracts, which are considered monopolistic and unenforceable. These provisions are similar to those in the *EU Block Exemption Act*, including the provisions which require technology licensees to surrender improvements made on the licensed technology, the provisions which require procurement of unnecessary products or technology, and the provisions which prevent the licensee from developing or sourcing competing technology.



David Pan

Llinks Law Offices
19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120
China

Tel: +86 21 3135 8701
Email: david.pan@llinkslaw.com
URL: www.llinkslaw.com

David is a partner at Llinks' Corporate Compliance Practice. David holds an LL.M. from Harvard Law School and a Ph.D. from Shanghai Jiao Tong University. He is admitted in both the USA and China, and has been practising law for over 18 years in both countries. David's clients span the full spectrum from global Fortune 500 companies to local high-potential and high-growth start-ups. He regularly advises on all major corporate & compliance issues ranging from data (cyber security, data privacy and other data-related issues), antitrust and anti-corruption. In addition, the combination of his experience in serving small-to-large financial institutions and his knowledge in cyber security law and technology has enabled him to advise clients on a full range of fintech-related issues.

David is recognised in *The Legal 500* as a leading PRC antitrust and competition lawyer, and is recognised by LEGALBAND as a top 10 PRC cyber security and data protection lawyer.



Xun Yang

Llinks Law Offices
19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120
China

Tel: +86 21 3135 8799
Email: xun.yang@llinkslaw.com
URL: www.llinkslaw.com

Xun Yang is a partner at Llinks' Intellectual Property and Technology Practice. He regularly advises multinational companies on intellectual property, unfair competition, information security, privacy, and regulatory matters with a focus on the TMT, life sciences and finance sectors. He has extensive experience in assisting clients in technology transactions, IP licences, R&D collaborations, IT outsourcing, as well as other technology or IP-oriented investment, cooperation, and M&A.

Xun passed the PRC Bar examination in 1999 and was admitted in New York in 2006. Prior to joining Llinks, Xun worked for reputable international law firms such as Freshfields Bruckhaus Deringer and Simmons & Simmons, based in Shanghai, Hong Kong, London and other international cities for a total of 15 years, among which almost eight years were in foreign jurisdictions. Yang Esq. has been nominated by *The Legal 500* as a recommended lawyer in both IP and TMT areas (International Firm group).



Llinks was founded in 1998, and is an acclaimed PRC firm in business and commercial areas. With specialised practice groups and seamless cross-cutting cooperation among the groups, Llinks' high calibre legal team is known for its professionalism and expertise, and has been recognised as a leading firm in providing innovative and constructive solutions to both domestic and international clients for their complex business needs. Llinks has offices in Shanghai, Beijing, Hong Kong and London.

Llinks aims to help clients achieve their business goals. Llinks' solid relationship with clients and regulators allows Llinks to concentrate on the dynamic and evolving marketplace, while keeping pace with changes in the legal industry to offer sound legal representation. Llinks strives to keep its clients informed ahead of time of changing market trends and developments, so that when the relevant opportunities arise, the clients are in a position to pursue them with certainty and clarity.

Colombia

Santiago Gutierrez



Juan Sebastián Peredo



Lloreda Camacho & Co

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Colombia has seen an active development of several types of fintech businesses. In this regard, the most noticeable businesses are the following:

- Crowdfunding.
- Payment systems.
- Peer to Peer (“P2P”) lending.
- Crowdequity.
- Cryptocurrencies.
- Distributed Ledger technologies.
- Robo-advice technology.

The Colombian legislator has focused on the most active fintech sub-sectors, such as payments, equity, debt crowdfunding and robo-advising, issuing certain guidelines or studying determined subjects specifically.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

Colombian regulation is not particularly restrictive; however, the collection of money from the public is a financial activity that requires authorisation from the Financial Superintendence. Because of this, some types of fintech businesses have restricted operations or are prohibited. The following are some of the restricted or prohibited fintech businesses:

- Limitations for P2P platforms, which have to be analysed on a case-by-case basis since the model may be interpreted as a form of unauthorised fundraising.
- Due to the fact that equity and debt crowdfunding is specifically regulated in Colombia, these businesses must comply with determined requirements and applicable restrictions.
- Trading platforms are not regulated, authorised or under the supervision of the Financial Superintendence. However, these activities are exclusively authorised for financial entities.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

Reward-based crowdfunding and donation crowdfunding are not regulated nor prohibited in Colombia and are alternatives to fund different growing businesses or specific causes. However, debt and equity crowdfunding has been recently authorised pursuant to Decree 1357 of 2018, which allows the issuance of debt or equity-based securities for start-up projects to raise funds. Additionally, crowdfactoring platforms currently represent a way in which small businesses can raise funds for their operations.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

Currently there are no specific prerogatives for investing in tech/fintech businesses, or in small/medium-sized businesses. However, recently, a new regulation was issued allowing some financial entities to invest in fintech businesses. Additionally, the grounds for the national development plan (“*Bases del Plan Nacional de Desarrollo*”) were recently issued by the government, setting forth commitments that aim to eventually provide and create governmental incentive schemes for investments in tech/fintech businesses.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

In general terms, companies (with the exception of *Sociedades por Acciones Simplificadas*) may issue securities pursuant to an IPO by complying with the regulatory guidelines set forth in Decree 2555 of 2010. Some of the general requirements, in addition to being a limited liability company, are to be registered before the National Securities and Issuers Registry (*Registro Nacional de Emisores de Valores*).

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

Since fintech businesses are mostly start-ups incorporated as *Sociedades por Acciones Simplificadas*, there have not been any

IPOs. However, this does not mean that there have not been significant investment rounds for the most notable fintech businesses in Colombia.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

Colombia has recently adopted new regulations regarding different fintech sectors. For instance, a new decree (Decree 661 of 2018) was issued regarding advising activities in the financial market, specifically concerning the use of technology and, therefore, referring to robo-advisors. Additionally, the debt and equity crowdfunding activities have been regulated through Decree 1357 of 2018 and the payment segment is being studied by the regulator, so we shall expect new guidelines and a new regulatory framework regarding this matter. So far, the financial regulator has issued the following regulatory framework regarding fintech activities:

- Decree 661 of 2018. This Decree sets forth that the recommendations in the financial market can be provided with robo-advising technology, as long as the obligations that derive from the advising activity are met. To that extent, investors may use this type of technology for advice and to manage their investments and investment portfolios.
- Decree 1357 of 2018. This Decree establishes the legal framework in relation to the activity of collaborative finance, specifically debt and equity crowdfunding.
- Decree 2443 of 2018. This Decree allows credit and other financial entities to acquire participation in companies specialised in developing new technologies in the financial market.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

There are no specific regulations regarding the use or issuance of cryptocurrencies or crypto-assets in Colombia. However, the Financial Superintendence and the Colombian Central Bank have issued formal instructions setting forth their position regarding cryptocurrencies, as briefly explained below:

Colombian Central Bank: The Colombian Central Bank has issued different official statements setting forth that cryptocurrencies are not recognised as a currency given that they do not have the support or involvement of a central bank. Additionally, they have argued that these instruments are not a high liquidity asset.

Financial Superintendence: The Financial Superintendence has provided official statements setting forth their position and clarifications regarding these instruments and the risks associated to them for consumers and investors. Furthermore, on June 22nd of 2017 the Financial Superintendence published the circular letter 052 of 2017 summarising the position of the Central Bank regarding cryptocurrencies, as well as setting forth that supervised financial entities are not authorised to hold, invest, intermediate or operate with this type of instrument, nor allow the use of their platforms to carry out operations with cryptocurrencies. This circular letter has also clarified that this type of instrument is not considered a security under Colombian securities regulation.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

Yes, Colombia has seen an active development of regulation and legislation aimed at including new players, models and infrastructure to the financial system. This active approach from the Colombian financial regulator has led to the analysis of innovative models that have been brought by fintech companies, both locally and internationally. Colombia currently has the third-largest number of fintech developments in Latin America, only behind Brazil and Mexico. Therefore, the Colombian financial regulator's approach towards fintech has not only focused on the feasibility of allowing or implementing certain models in Colombia, but also on fostering the implementation of those that are deemed to be beneficial to the financial system. For details on the recently adopted regulation, please refer to question 3.1.

Additionally, the Colombian financial supervisor (the Financial Superintendence) has recently adopted a sandbox model for the fintech industry. The Financial Superintendence is already receiving projects for the sandbox, which can be brought by fintech companies, financial entities or both. Since the sandbox is an initiative from the Financial Superintendence, it can only affect or intervene with the guidelines given to the financial entities coming from the Financial Superintendence, and it cannot be considered a regulatory sandbox rather than a sandbox from the supervisor.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

The Colombian financial regulatory framework sets forth certain restrictions whenever foreign financial entities intend to offer financial products in the Colombian territory or to Colombian residents. Whenever a financial product is meant to be offered specifically to Colombian residents or in Colombian territory, it must be done through a representation office authorised by the Financial Superintendence. However, not all fintech businesses are a financial regulated activity and may be considered as regular commercial activities, being able to offer their products without requiring specific authorisation.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

Yes, in Colombia all matters related to the collection/use/transmission of personal data are considered constitutional rights, and are regulated pursuant to Law 1266 of 2008, specifically regarding financial, credit and commercial services. Additionally, Law 1581 of 2012 establishes the requirements and general standards which protect

the constitutional rights of Colombian citizens and allow residents to be aware of, update and rectify the information that is stored in personal databases or files.

Law 1266 of 2008 in its article 2 sets forth that data regulation is applicable to all personal information, and also that all databases and fintech business which manage or use any kind of database are governed by such law, and are liable to keep personal information safe.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

The aforementioned regulations will be applicable whenever the organisations established outside of our jurisdiction have any physical presence in Colombia or provide any financial or commercial service to Colombian residents or within the Colombian territory.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

The sanctions applicable for not complying with data privacy laws regarding financial, commercial, credit and services information are the following:

- for financial entities, the suspension of the activities of the financial entity (for a maximum term of six months) when such entity is in serious violation of this law;
- personal or institutional fines from an amount equivalent to 1,000 monthly legal minimum Colombian wages at the time of the sanction. These fines may be successively imposed until the breach is amended;
- suspension of the activities of data banks for a maximum term of six months. Temporary closure of the data bank once the suspension term has finished and no amendments in the process have been made; and
- definitive closure of data banks, whenever the handling of data is performed with unauthorised data.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

Yes. Pursuant to Decree 663 of 1993 and Decree 2555 of 2010, there are specific regulations that must be applied by financial entities and therefore to some fintech businesses that operate and offer financial services. Accordingly, the Financial Superintendence has recently issued External Circular 007 of 2018 with the purpose of informing financial consumers of operational risks, of cyber incidents and security information as well as of the measures adopted to solve the situation. Additionally, External Circular 008 of 2018 sets forth some of the standards of fintech platforms or financial services platforms which seek to prevent any cybernetic incident regarding cyber-security.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

Pursuant to Colombian regulations, not all AML administration system requirements are applicable to fintech businesses even if they are offering financial products. The AML administration system

requirements are set forth in Circular 029 of 2014 from the Financial Superintendence with certain guidelines applicable for financial entities. The Companies Superintendence also sets forth AML administration requirements through Circular 100-00005 of 2014.

Additionally, we must bear in mind that unauthorised collection of money from the public (*captación masiva y habitual de dineros del público*) is considered a felony pursuant to the Colombian criminal code, and, that in order to carry out this activity, it is necessary to be authorised by the Financial Superintendence.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

Depending on the type of fintech business and if the activity being carried out is considered a financial operation, the financial regime may apply and the fintech business may be subject to the control and surveillance of the Financial Superintendence. Otherwise, the regular commercial regime will be applicable.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

The general legal framework for hiring and dismissing staff in Colombia is set forth in the Colombian Labor Code, as well as in the Political Constitution. There are no particular requirements or restrictions for hiring staff in Colombia. However, regarding the dismissal of staff, we highlight that the Constitutional and Labor Courts have ruled a Jurisprudential Line regarding the protection of certain employees. In this sense, employees three years or fewer from retirement cannot be dismissed; although pregnant women, women on maternity leave and disabled and/or sick employees can be dismissed if the employer gets authorisation from the Ministry of Labor.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Aside from salary, employees who earn an ordinary salary are entitled to receive other mandatory benefits, such as the following:

- Severance payment: the payment of one monthly salary for each year of service and proportionally per fraction. The employer must deposit the severance payment in a severance fund as of December 31st of each calendar year. The deposit must be made no later than February 14th of the next calendar year. The severance fund must be elected by the worker.
- Interest on the severance payments: interest is liquidated on accrued severance payments as of December 31st of each calendar year.
- Semester services bonus: the bonus is the payment of one monthly salary. Fifty per cent of the bonus is paid on the last day of June, and 50% during the first 20 days of December. Please note that it must be paid to any employee who works the whole semester, or proportionally if the employee has not worked the whole semester.
- Transport allowance: the government establishes a fixed amount as transport allowance on a yearly basis. This transport allowance is paid only to employees earning less than two minimum monthly legal wages (for 2019, the minimum monthly legal wage is approximately USD 268).

In addition to fringe benefits, employees are entitled to vacations. The employer must allow the employee vacations consisting of 15 working days per year of service, and proportionally for the equivalent fraction thereof. Vacations cannot be accumulated for more than three years. If at the end of the labour agreement the employee has pending vacation time, such time must be paid in cash.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

In order to bring foreign employees into Colombia, it is necessary to comply with visa requirements. This means acquiring either a Migrant Visa – Type M, or a Visitor Visa – Type V. If the foreign employee subscribes to an open-ended labour agreement, a Migrant Visa – Type M will be required; however, if the labour agreement is for a fixed term, or during the duration of a given work the Visitor Visa – Type V should be requested, the Visitor Visa – Type V will be granted specifically to carry out the determined job for which it was granted.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

It is important to note that Colombia is a member of different treaties that protect intellectual property, such as TRIPS and the Paris Convention. According to these treaties, innovations and inventions can be protected either as patents, utility models or industrial designs. Also, under the local provisions, patents must be granted in all files of technology; this has allowed for the protection of computer-based inventions.

Aside from this protection, copyright also grants protection to software.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

As mentioned above, the ownership of IP in Colombia works through a registration process and is protected by means of patents for inventions, utility models and industrial designs, and layout designs for integrated circuits. Patents may grant the titleholder the exclusivity to exploit the invention and to prevent third parties from manufacturing, selling or using it without prior authorisation or licence.

Patents are granted for a 20-year period, whereas industrial designs and utility models are protected for a period of 10 years.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

In order to protect or enforce IP rights, the same must be granted by the corresponding authority; in Colombia, for example for patents, industrial designs and utility models, this is the Superintendence of Industry and Trade.

The principle of territoriality regulates IP rights; that is to say, an IP right is only enforceable in the territory that it is granted.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

IP rights are negotiable; thus right holders are entitled to sell or license their rights, or use them as encumbrances. The only applicable restriction is if the right holder is a public entity.

**Santiago Gutiérrez**

Lloreda Camacho & Co
Calle 72, No. 5-83, Piso 5
Bogotá 110221
Colombia

Tel: +57 1 326 4270
Fax: +57 1 606 9701
Email: sgutierrez@lloedacamacho.com
URL: www.lloedacamacho.com

Santiago is a Partner at Lloreda Camacho & Co. He joined the firm in 1992 and heads the Corporate and Finance practice areas.

He has a law degree from Universidad Javeriana in Bogotá and completed postgraduate studies in Financial Management at the School of Marketing and Management (ESMA) in Barcelona, Spain.

Santiago also won the "Deal Maker of the Year Award – 2015 Edition" in Colombia, awarded by *Finance Monthly* magazine (UK) with our partner Andrés Hidalgo. He is a member of the International Bar Association and of Lawyers Associated Worldwide. Santiago is co-author of the Colombia chapter of *Getting the Deal Through – Mergers and Acquisitions*, edited by Law Business Research, London, 2015.

**Juan Sebastián Peredo**

Lloreda Camacho & Co
Calle 72, No. 5-83, Piso 5
Bogotá 110221
Colombia

Tel: +57 1 326 4270
Fax: +57 1 606 9701
Email: jperedo@lloedacamacho.com
URL: www.lloedacamacho.com

Juan Sebastián is a Senior Associate of the Financial and Capital Markets Law Practice at Lloreda Camacho & Co.

Juan Sebastián has extensive experience structuring financial transactions, including project finance, syndicated loans, derivatives, repos, and securitisations. Juan Sebastián has advised national and international banks, multilateral creditors, investment firms and private equity funds in syndicated loan transactions, private equity transactions, transactions for the financing of infrastructure in Colombia and several of the most relevant capital markets transactions.

Juan Sebastián earned his JD from Universidad del Rosario and obtained specialisation degrees from Universitat Pompeu Fabra in Barcelona, Spain (2011), and a specialisation degree in financial and capital markets law from Universidad Externado de Colombia (2015). In addition, Juan Sebastián obtained in 2016 a Master's degree (LL.M.) in Banking Law and Financial Regulation from the London School of Economics and Political Science.

LLOREDA · CAMACHO & CO

Lloreda Camacho & Co, with more than 75 years of experience, is widely recognised as a Colombian leading law firm that provides integral legal services, especially to foreign companies doing business in Colombia.

Our Financial Services Practice is recognised for its active involvement with the banking and finance industry in Colombia, and also for our Fintech practice within the Banking and Finance law firm team. Partners and associates of the firm have been involved in some of Colombia's most relevant fintech regulatory developments as a legal partner of the Colombian Fintech Association, as well as structuring different fintech businesses within the Colombian legal framework.

Our members are well regarded for their in-depth knowledge of Colombian and cross-border financial and securities regulation that impact fintech products and operations directly.

Cyprus

Democritos Aristidou LLC

Christiana Aristidou



1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Cyprus accommodates a strong and sophisticated financial services sector, where important banking, investment and financial players are involved. Such dynamic services sector is inviting to fintech businesses. Financial services remain the fastest-growing sector of the Cypriot economy. The emergence of fintech is rapidly turning Cyprus into a significant fintech hub. It shall come as no surprise that TransferWire has recently named Cyprus as one of the eight emerging global technology hubs.

Foreign exchange companies and international money transfer businesses constitute the main types of businesses engaging in the fintech area, owing to the country's well-respected and recognised position as a global specialist centre for retail foreign exchange. Foreign exchange is regulated by CySEC as a financial product under MiFID I; Cyprus is only the second EU Member State to do so after the UK. More than 250 regulated foreign exchange companies have been established in Cyprus and CySEC is one of the most well-respected regulators in foreign exchange. CySEC has already regulated many of the world's biggest brands in retail foreign exchange, which have begun using cutting-edge fintech and regulatory technology.

These companies include electronic money institutions, such as:

- prime brokerages;
- major platform providers;
- liquidity management companies;
- specialist professional services firms;
- regulatory technology companies (regtech); and
- reporting companies.

Other fintech companies include:

- authorised credit institutions (either Cyprus-incorporated institutions or subsidiaries or branches of foreign credit institutions);
- investment firms;
- insurers;
- undertakings for collective investment in transferable securities; and
- other payment institutions.

Further, several information and communication technology companies from the United States, Europe, Russia and Australia base their regional headquarters in Cyprus, and, subsequently, service clients globally.

Fintech has significantly impacted, and is expected to continue to impact, the banking sector in Cyprus, which is one of the main pillars of the Cypriot economy. The EU Payment Services Directive (PSD II 2015/2366/EC), as transposed to Cyprus by the relevant domestic legislation, obliges payment service providers to comply with the new provisions and activates open banking platforms to support the sharing of information. Incumbent banks and other payment institutions have developed technology-oriented strategies with a view to complying with the relevant law, but also as part of a strategic plan to preserve their market share. Most of these institutions have established their own application programming interface platforms (some even before PSD II came into force). Some of them are considering biometrics and other technologies to achieve the required customer authentication and protection. Concurrently, the number of third-party providers (e.g., account information service providers and payment initiation service providers), such as tech start-ups, technicians and programmers, is growing. The Central Bank is accepting and evaluating relevant applications to provide the required authorisations as per the law and regulations.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

No fintech products or services are specifically prohibited in Cyprus. While there is no specific regulation targeted to fintech products and services, such products or services may be subject to the existing regulatory framework, depending on the activities carried out or to be carried out by the fintech businesses concerned. In these cases, fintech businesses must comply with certain conditions, or obtain a licence to conduct their activities to the extent that no exemptions apply.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

New and growing businesses, including fintech start-ups, may obtain funding through various financing means. These, primarily, include:

- personal savings or funding from family and friends;

- loans;
- EU funding;
- venture capital;
- angel investors;
- crowdfunding; and
- grants and subsidies.

Convertible loan notes constitute a popular financing method for start-ups. Such loan notes are used at an early stage, when conducting a proper business valuation may seem difficult, unreliable, or inaccurate. Pursuant to these notes, once a prescribed event occurs, or once certain prescribed conditions are met, the loan converts into equity (e.g., shares).

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

Tax incentives are not specifically provided to tech/fintech businesses. Still, such businesses could very well benefit from several business-friendly initiatives undertaken in the tax area, especially regarding start-up businesses.

Natural persons investing in qualifying start-ups enjoy income tax relief of up to 50% on their taxable income, subject to a cap of €150,000, per year. Investors can claim tax relief within five years of their investment.

Further, as per the new IP box regime, qualifying taxpayers are eligible to claim a tax deduction of 80% on qualifying profits resulting from the business use of qualifying assets. Patents and software copyrights are considered qualifying IP assets.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

Different conditions apply to the holding of an IPO, depending on the market in which the shares are to be listed. Cyprus CSE, the official stock exchange in Cyprus, has a regulated market (the main markets there are the “Main Market” and “Alternative Market”) and a non-regulated market, which is not governed by the mandatory requirements for regulated markets (“Emerging Companies Market”).

For an IPO carried out in relation to the regulated market, the following main general requirements apply:

- Observance of formalities in relation to the formation of a public company.
- Sufficient working capital.
- Publishing of a Prospectus that requires approval by CySEC.
- Basic requirements of listing, particular to the Main and Alternative Markets, are the following:
 - Submission of duly audited financial statements of three years preceding the listing application for the Main and two years for the Alternative Market.
 - The public must hold at least 25% of the company’s shares for the Main and at least 10% for the Alternative Market.
 - Exclusively for the Main Market: minimum equity capital of €3 million for each one of the two years preceding the listing.

Admission requirements are less rigid in relation to the Emerging Companies Market. The main requirements are the following:

- Observance of formalities in relation to the formation of a public company.

- Prospectus approved by CySEC for listing through a public offer. For listing through a private placement, an Admission Document (approved by CSE) must be prepared in place of a Prospectus, unless the shares offer is higher than €5 million and addressed to more than 150 investors.
- Observance of listing requirements. These are more lenient than the Main Market requirements. The main requirements include:
 - Appointment of a Nominated Advisor, who must be registered with CSE.
 - The company must prepare audited accounts demonstrating relevant operation and activities for two years preceding the listing. For newly established companies, the relevant authority must be satisfied that the available information to investors allows for a fair valuation of the company’s titles.
 - No minimum amount of shares must be necessarily held by the public.
 - No minimum market capitalisation.
 - No minimum equity capital requirement.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

No notable exits have been made by founders of fintech businesses in Cyprus.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

No fintech-specific regulation is currently in place in Cyprus; fintech products and services are currently regulated in the same way as “traditional” financial products and services. Fintech businesses are bound by the legislation that regulates the provision of “traditional” financial products and services to the extent they conduct certain regulated financial activities.

Existing legislation governing the provision of financial services may apply to fintech businesses. This could happen, provided that fintech businesses:

- provide services that are not covered by an exemption; and
- engage in or carry out certain activities specified or provided for by the relevant law – including:
 - the Business of Credit Institutions Laws 1997 to 2018;
 - various EU regulations (which have direct effect in Cyprus) dealing with banking regulation, including EU Regulation 575/2013 on prudential requirements for credit institutions and investment firms;
 - the Law on Electronic Money;
 - the Provision and Use of Payments Services and Access to Payment Systems Law 2018;
 - the Securities and Exchange Commission Law;
 - the Transparency Requirements Law;
 - the Investment Services and Activities and Regulated Markets Law;
 - the Takeover Bids Law;
 - the Public Offer and Prospectus Law;
 - the Open-ended Undertakings of Collective Investments in Transferable Securities Law;

- the Alternative Investment Fund Managers Law;
- the Alternative Investment Funds Law;
- the Securities and Stock Exchange Law; and
- the Prevention and Suppression of Money Laundering and Terrorist Financing Law.

In relation to the securities sector, it must be noted that CySEC has entered an MoU with the FCA (UK competent authority) with a view to maintaining effective cooperation, exchange of information, supervision and monitoring of both jurisdictions' securities markets after the UK's exit from the EU. The same MoU was entered between all EU/EEA Securities Regulators and the FCA. The above MoU will become effective only in case of a no-deal Brexit.

The relevant regulatory authority for the authorisation, operation and supervision of payment institutions, including all Cyprus-incorporated commercial banks, is the Central Bank.

The financial regulator is CySEC, which is responsible for the supervision of the Cyprus Stock Exchange; licensed investment services companies, collective investment funds, fund management companies and consultants are under CySEC's control. CySEC grants licences to investment firms and brokers and has the authority to impose disciplinary penalties for deviations from stock market legislation.

That Cyprus has not yet developed fintech-specific laws or regulations does not mean that CySEC is disinterested in the development of the regulatory framework in this area. CySEC is currently in the process of assessing draft legislation on the introduction of a crowdfunding mechanism for start-ups, which will cover initial coin offerings (ICOs), tokenisation and asset securitisation.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

Activities relating to virtual currencies are not specifically regulated in Cyprus. Virtual currencies may still be regulated under the existing regulatory framework, as per CySEC's relevant announcement, to the extent that these currencies fit within the existing provisions.

Despite the lack of specific regulation directed at cryptocurrencies, CySEC has expressly embraced the ESMA's approach, which included Contracts-for-Differences (CFD) within the scope of its intervention. CySEC has, accordingly, issued a circular, whereby derivatives on virtual currencies may be considered financial instruments for the purposes of the relevant investments' legislation; as such, specific authorisation must be granted by CySEC. Beyond the typical conditions imposed regarding registration of companies engaging in investment services in relation to financial instruments, companies seeking to invest in derivatives of virtual currencies must abide by further requirements, aiming at protecting investors from the risks associated with virtual currencies.

ICO founders must comply with several single market regulations. However, ICOs are, at present, largely unregulated in Cyprus, as they are in most European countries, but it could be sensibly argued that businesses which choose to launch ICOs in Cyprus may, most probably, benefit from access to:

- its extensive list of Double Tax Treaties; and
- EU Member States, which are fully compliant with EU laws and regulations and enjoy white-list status among tax authorities, globally.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

Authorities are generally receptive to fintech innovation. Cyprus launched its Digital Strategy in 2012, which is in line with the Digital Agenda for Europe and promotes information and communication technology in all sectors of the economy. There is also an e-government strategy and a relevant plan in place. Cyprus also adopted a national cybersecurity strategy in 2012. Importantly, CySEC has adopted an active and positive stance towards innovative technology.

Although not introduced as a "sandbox" option *per se*, CySEC has launched the "Innovation Hub", with a view to advancing the dialogue in the areas of fintech and regtech. CySEC, since October 2018, welcomes applicants eager to see the development of the regulatory framework accommodating emerging financial technologies. The eligibility criteria for applicants, as issued by CySEC, demonstrate CySEC's intention to emphasise the need to support and engage with businesses offering services of genuine innovative character.

CySEC, as per its Chair's contentions, has established this Hub as a means to opening immediate channels of communication with innovative businesses.

CySEC has demonstrated its interest in the regulatory implications of shared distributed ledgers. Particularly, it is currently exploring and testing the way in which technology could afford greater opportunities of over-the-counter markets' supervision. CySEC participates in the Blockchain Technology for Algorithmic Regulation and Compliance (BARAC) project, run by University College London (UCL) Blockchain Technologies. The project examines the impact of distributed ledgers in the services industry, and the appropriate approach of regulating novel business models. Cyprus has also joined the European Blockchain Partnership, which aims at developing blockchain infrastructure for the provision of digital services.

The application and use of Smart Contracts are currently under the government's review. Cyprus Standards (CYS), the national standardisation body and member of the International Standardisation Organisation, participates in the International Standardisation Organisation/Technical Committee TC/307 for Blockchain and Distributed Ledger Technologies, through approved professionals/national delegates. CYS actively contributes to specialised working groups and study groups in the areas of Foundations, Security Privacy and Identity, Smart Contracts and their Applications, Governance, and Use Cases. The work undertaken within these working and study groups is directed, among other things, at issuing international standards, technical specifications and technical reports concerning smart contracts and their uses.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

Regarding foreign fintech businesses seeking to provide regulated financial services in Cyprus, a difference between businesses from EEA countries and third countries must be maintained. Also, the nature of activities determines the kind of licence that fintech businesses must obtain prior to offering their services. Fintech businesses that wish to undertake regulated activities as a:

- banking or credit institution;

- credit acquiring company;
- financial leasing company or payment institution;
- electronic money company;
- foreign exchange company;
- alternative investment fund; or
- insurer,

shall seek specific licences, as distinctively provided by law.

Businesses from EEA countries may offer fintech-related services by: establishing a branch or a subsidiary company in Cyprus; through the provision of cross-border services; through establishing a representative office in Cyprus; or through a representative office located abroad where the business is incorporated and licenced in Cyprus. Different conditions apply to these different modes of offering services in Cyprus.

Providing fintech services requires the approval and licence by the relevant authority, depending on the nature and scope of the said services, as explained above. In case the activities of such businesses are eligible to benefit from EU passporting rights, then Cyprus, as a fully-fledged EU Member State, obviously provides such option.

Briefly, passporting can occur either:

1. through establishing branches in other EEA countries; or
2. through the provision of cross-border services within the EEA.

The following entities can passport their single licence across the European Union:

- alternative investment fund managers;
- credit intermediaries;
- credit institutions;
- electronic money institutions;
- insurers and reinsurers;
- insurance intermediaries;
- investment firms;
- payment institutions; and
- Undertakings for Collective Investment in Transferable Securities managers.

Businesses from third countries could also provide services in Cyprus, by establishing a branch or a subsidiary company, again with the approval of the relevant authority, depending on the nature and scope of the concerned services.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

The processing and transfer of data relating to fintech products and services are governed by the EU General Data Protection Regulation (GDPR) (2016/679), as transposed to the domestic legal framework by the relevant Cypriot legislation. The GDPR has been in force since 25 May 2018. The GDPR applies to *processors* or *controllers* processing data of natural persons. To the extent that fintech businesses process personal data, they are bound by the provisions of the GDPR.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

The GDPR contains specific extra-territorial provisions that apply to *controllers* or *processors* based outside the European Union that offer goods or services to individuals in the European Union or monitor individuals within the European Union. Controllers and processors covered by these provisions will need to appoint an EU representative, subject to certain limited exemptions.

Specific provisions are made in relation to the international transfer of data. For certain third countries (or international organisations) outside the EEA, the EU Commission has issued “Adequacy Decisions”, whereby such third countries (or such organisations) are deemed to offer adequate personal data protection. In these cases, no additional measures need to be taken by processors or controllers when they transfer data to these countries, other than, of course, those anticipated for EU-wide personal data processing. Absent such adequacy decisions, some additional safeguards are imposed on processors or controllers, including:

- the inclusion of standardised contractual terms ensuring adequate data protection;
- binding corporate rules for transfers within a group of undertakings;
- consent of subjects, whose personal data are implicated; and
- for special categories of personal data, as defined in the GDPR, the competent, domestic Commissioner’s approval.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

Non-compliance with data privacy laws engenders a wide range of sanctions:

- The competent Cypriot regulatory authority may impose fines, not exceeding the upper limits as provided by the EU Directive.
- Aggrieved individuals that suffer from personal data infringement have a right to seek redress at court, and a right to compensation; this effectively enables the pursuit of class actions.
- Processors or controllers may be held personally liable in case they commit specific offences as provided in law. Personal liability includes imprisonment (of up to one, three or five years depending on the gravity of the offence), and/or imposition of fines.

In case processors or controllers are legal persons, then certain officers, as specifically provided by the law, may be held liable.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

Cyprus has a comprehensive information and communications technology legislative and regulatory framework. Within this framework, cyber-security provisions have been adopted. These may apply to fintech businesses.

The following legislation and regulations contain provisions relevant to cyber-security:

- the Electronic Commerce Law (156(I)/2004);
- the Law for the Protection of Confidentiality of Private Communications (92(I)/1996);

- the Law Regulating Electronic Communications and Postal Services (112(I)/2004), last amended by Law 76(I)/2017;
- the Law transposing Regulation 910/2014/EC on electronic identification and trust services for electronic transactions in the internal market (Law 55(I)/2018); and
- the Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data (Law 125(I)/2018).

Cyprus is a party to the Council of Europe Convention on Cybercrime, which was incorporated into domestic law through Law 22(III)/2004. The Law mainly deals with:

- illegal access;
- illegal interception;
- data interference;
- system interference;
- the misuse of devices;
- computer-related forgery;
- computer-related fraud;
- offences relating to child pornography;
- offences relating to copyright infringement and related rights; and
- penalties and measures.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

Cyprus has implemented all the necessary mechanisms for the prevention and suppression of money laundering and terrorist financing activities.

The provisions of the EU Fourth Anti-Money Laundering Directive (2015/849/EC), regarding the prevention of the legalisation of proceeds from illegal activities or terrorist financing, have been transposed into national legislation through the relevant amendment to the Prevention and Suppression of Money Laundering Activities Law 2007 to 2016.

All physical and legal persons that conduct financial services activities, potentially fintech businesses, must introduce adequate procedures and mechanisms to protect themselves, their companies and Cyprus's financial system from money laundering. The necessary procedures and mechanisms include:

- measures to identify and report suspicious transactions; and
- the know-your-client principle, which requires the industry to adhere to and apply strict procedures for maintaining accurate and up-to-date records.

Further, it must be noted that the Fifth Anti-money Laundering Directive (2018/843/EC) was adopted in May 2018. Member States have by 1st January 2020 to implement its provisions. The scope of the Directive extends to and now covers providers of virtual currencies exchange and custodian wallet providers that need to be registered and comply with the AML provisions.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

Beyond the cyber-security, anti-money laundering, and data protection regulations, one further regime that seems to be of potential concern to fintech businesses is the consumer protection regime. Depending on the exact scope and nature of the activities and services offered by fintech businesses, other regulatory regimes could potentially apply.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

Employers in Cyprus typically hire staff on the basis of a contract, either written or oral. In case of an oral contract, however, employers are obliged by law to provide, in writing, the basic employment terms and conditions to their staff. Terms may be negotiated between employers and individual employees. In case employers have concluded collective agreements with trade unions, it is possible for the relevant contractual terms to be determined by the content of these collective agreements.

Regarding the dismissal of staff, employers are obliged to give notice to terminate the employment contract of their employees who have completed 26 weeks of continuous employment. In turn, employees may claim their salaries for a number of months as specified by law, depending on the period of their employment.

In case of unlawful termination by their employer, employees are entitled to compensation for unfair dismissal. Further, the law provides for compensation in case employees are dismissed on the grounds of redundancy.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Cyprus does not mandate the provision of any special employment benefits. Yet, certain benefits are provided to employees:

- Minimum wage for a limited list of occupations.
- Employees are entitled to 20 or 24 days paid leave (based on a five-day or six-day employment, respectively).
- Unpaid parental leave of 18 weeks is allowed.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

EU/EEA residents face no restriction in potential employment by businesses in Cyprus, as secured by the free movement of persons within the EEA.

Non-EEA residents may work in Cyprus once they obtain a work permit, which, broadly speaking, is granted once the competent authority is satisfied that after the employer has made efforts to hire EEA employees, who were appropriate to take up the relevant work position, no such employees were available. Cyprus authorities impose a national maximum percentage of foreign workforce that may be employed in Cyprus at a given point in time. Certain limited categories of employees, such as employees of high quality of academic and/or professional skills, are exempt from certain restrictions on their potential employment; for them the obtaining of a work permit is, in practice, a matter of formality. Also, certain highly skilled professionals are not counted towards the national maximum percentage of international employees that may be employed in Cyprus at a given point in time.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

A comprehensive legal framework guarantees that the outcome of innovation – including fintech innovation and creativity – is protected at a national, EU and international level through specific IP rights (i.e., copyright, patents, trademarks and industrial designs), which are granted to the author or inventor.

Copyrights and patents are relevant to the protection of innovative works and inventions.

Copyright

Copyrights are protected under Law 59/76 on the Protection of Intellectual Property, which offers protection at the national level. Copyrights are not registrable in Cyprus.

Cyprus is a signatory to the Bern Convention for the Protection of Literary and Artistic Works, which covers a broad range of rights, including software copyrights and computer programs, which are directly relevant to the fintech industry.

A copyright on computer programs or software will arise automatically and extend to:

- computer code;
- visual interface features;
- audio;
- video guides;
- application programming interface structures;
- screen displays or graphics; and
- computational and usability efficiencies, if they exist.

Patents

Fintech innovations and products, such as hardware, may also be protected through the registration of a patent. However, under Cyprus patent law, computer programs are excluded from patentability.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

The author of a work is considered the first owner of its copyright. As regards computer-generated works, the author will be the person who engaged in the necessary creative activity to produce such

work. However, if the author of the work has an employment contract or any other pertinent relation with a fintech business (legal person) or a fintech individual employer (natural person), ownership of the work and its copyright rests with the employer (i.e., the fintech company or employer). This does not apply to third-party contractors who do not have an employment contract or relationship with a fintech company (i.e., any third party that created a computer program or software will own the copyright). However, fintech companies or individual employers may require that the owner of the copyright assigns on to them the right (a third party will assign his copyright to the employer fintech company or individual).

A patent for an invention is owned by the inventor.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

Patents can be enforced upon their registration and the obtaining of:

- a national patent certificate granted by the Department of the Registrar of Companies and Official Receivers;
- a European patent issued by the European Patent Office; or
- an international patent under the provisions of the Patent Cooperation Treaty, administered by the World Intellectual Property Organisation.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

Cyprus presents important opportunities for IP rights exploitation through a robust and comprehensive IP rights protection regime and a beneficial tax regime. For these reasons, Cyprus holds a significant position as a holding company jurisdiction for IP rights exploitation.

Exploitation of such rights may occur through licensing or assignment of these IP rights, either by the owner of the said rights, or by third parties granted the right to use and exploit such IP rights. No specific rules affect or restrict the exploitation of IP rights; the sole action that needs to be taken is the preparation of a contract providing for the licensing or assignment of these IP rights. No specific restrictions are imposed on the content of these contracts, other than, obviously, any general contract law restrictions.



Christiana Aristidou

Democritos Aristidou LLC
80, Georgiou G. Digheni Avenue 3101
Limassol
Cyprus

Tel: +357 99 453 019
Email: christiana@aristidou.com
URL: www.aristidou.com

Christiana Aristidou is an International Business and Technology lawyer with more than 21 years in practice. She is a Certified International Legal Project Practitioner (LPP) and has been a litigator since 1997. Christiana is a National Delegate to the ISO TC/307 Blockchain Committee and a founding member and vice-president of the Cyprus Blockchain Association.

A recognised expert in the fields of technology, business, commercial, international tax, finance, intellectual property, e-commerce, investment and securities laws, Christiana has been involved, advised and managed complex business and technology legal projects involving major foreign legal jurisdictions and a variety of legal and regulatory frameworks. She possesses exceptional skills in Comparative Law.

She is currently focused on innovation, start-up projects and new technologies, ICOs, STOs and LCOs and she is researching blockchain, DLTs and smart contracts.

Christiana is a legal author and policy influencer with numerous publications and articles in various journals, legal magazines, databases and on social media.



Established in 1971, Democritos Aristidou LLC is an independent, full-service Limassol-based law firm, and among the top local law firms offering legal advice and services to clients in Cyprus and internationally. The law firm enjoys an excellent reputation built through the years and is rich with history, ethos and character. The longstanding experience of the firm in tandem with the firm's commitment to leading the way towards technological evolution, development and innovation result in the provision of high-quality and multi-faceted services. The firm's rapid expansion over the last decade has not made its management lose sight of the necessity to focus the firm's undivided attention and interest to each and every client. Democritos Aristidou LLC is consistently driven towards accommodating future developments while remaining a well-respected firm with deep-rooted foundations in the Cypriot society and business world.

Czech Republic

Ondřej Mikula



FINREG PARTNERS

Jan Šovar



1 The Fintech Landscape

- 1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).**

The innovative area of financial technology has become very popular over the last years in the Czech Republic, and this trend will definitely continue in 2019. This is driven by the high standard of financial literacy, the majority of contactless payments, penetration of smart phones to daily activities and a big focus on privacy versus big data analysis.

Fintech companies in the Czech Republic mainly provide services through finance, crowdfunding and peer-to-peer lending platforms, alternative payment solutions, personal finance management applications and open banking applications using the framework created by the PSD2 and cryptocurrency exchange businesses.

Besides fintechs, traditional financial institutions such as banks and insurance companies are also very active in terms of innovation.

The insurtech sector is also on the rise in the Czech Republic, and new projects (such as DOK by Home Credit) have already been launched.

- 1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?**

There are no specific restrictions or prohibitions on types of fintech businesses in the Czech Republic. Most of the services provided by fintechs are licensable financial services, and it is therefore advisable to carefully review the business concept of any fintech which is to be established or marketed in the Czech Republic before it has been launched, from the perspective of licensing requirements.

2 Funding For Fintech

- 2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?**

Equity and debt funding are both possible ways of funding in the Czech Republic. Generally, the most common way to obtain funds

for business is from banking institutions. However, new businesses are usually financed by private investors, business angels, VCs and seed capital funds. Czech banks and other traditional financial institutions are only a little active in providing investment and other financial support to Czech fintechs in comparison to their Western peers. Mbank, which operates in the Czech Republic as well, introduced mAccelerator, a EUR 50 million venture capital fund focusing on investments in fintech entities.

In certain cases, it is also possible to obtain funding from governmental or regional supporting programmes or to apply for resources from EU grants. Popular reward crowdfunding platforms, such as HitHit, startovac.cz or nakopni.me, may serve as alternative financing options for young businesses, while later stage businesses may consider equity and debt crowdfunding platforms such as the fundlift platform.

- 2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?**

There are no special incentive schemes for investment in fintech businesses in the Czech Republic. However, in certain cases fintech companies may receive financial support from governmental or regional supporting programmes.

In 2018, the Czech government abandoned its plan to launch the National Innovation Fund (NIF), which was supposed to invest up to EUR 25 million into innovative startups. However, certain supporting programmes might still be available for tech businesses and other innovators through the Agency for Business and Innovations (*Agentura pro podnikání a inovace*).

- 2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?**

Prague Stock Exchange operates three main listing boards: the Prime Market; the Standard Market; and the Start Market. The Prime Market and Standard Markets are intended for trading in the largest and most prestigious issues of shares in Czech and foreign companies. The Start Market is a market for small and medium businesses. The key legislation covering the listing and trading of shares on a regulated market is the Capital Markets Act (Act No. 256/2004 Coll.).

The main requirements for Prime Market and Standard Market listings include:

- approved and valid prospectus;

- minimum three-year reporting history;
- minimum free float of 25%; and
- minimum market capitalisation of the share issue at EUR 1 million.

Start Market, which was launched in 2018, is a market for small innovative companies worth more than CZK 25 million (approx. EUR 970,000) and less than CZK 2 billion (approx. EUR 77.9 million). The relevant requirements are therefore less strict in comparison to Prime and Standard Markets. In particular, instead of a prospectus, the companies may present only the information document (simplified prospectus) if such prospectus is not required in accordance with the law.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

So far there have been no notable sales or IPOs of fintech companies.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

There is no specific fintech regulatory framework under Czech law. The applicable regulation depends on the nature of business activity of the relevant fintech company. Fintech businesses may fall, e.g., under the scope of regulation of payment services, banking, insurance, investment services, management companies and investment funds or under the regulation on the provision of consumer credit. Most services provided by fintechs require an authorisation (a licence) from the Czech National Bank (CNB). The CNB is a single national regulatory authority responsible for the financial services sector in the Czech Republic.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

In the Czech Republic, there are no regulations specifically directed at cryptocurrencies or cryptoassets.

However, the Czech AML Act (Act No. 253/2008 Coll.) brings cryptocurrency exchanges and wallet providers (broadly defined as persons providing services in connection with cryptocurrencies) within the scope of the AML/CFT regulation in order to improve the detection of suspicious cryptocurrency transactions.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

The position of the CNB in respect of fintech is based on technological neutrality, and as such the CNB is restrained from having any leniency towards fintechs.

In 2018, a new Payments Regulation and Financial Division was established within the CNB, which shall be focused on fintech regulatory matters. This step is promising as it may signal that the

CNB is open to certain future regulatory adjustments, which may foster digital innovations in the financial sector.

The Czech Republic is one of a small number of EU countries which have not launched a regulatory sandbox or innovation hub for fintechs yet. While this may change in the future, the relevant authorities (including the CNB) have been rejecting the idea of creating such platforms so far. However, existing Czech regulatory framework allows fintechs to carry out certain activities, which would otherwise be regulated, without the relevant licence, provided that such activities do not amount to "undertaking of a business activity" (e.g. testing/development). Local counsels must be consulted should any business wish to rely on such exemption.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

Fintech businesses established outside of the Czech jurisdiction which intend to enter the Czech market should properly assess whether their activities or services as provided in the Czech Republic are licensable. If such services are licensable, the local licence must be obtained from the CNB. EU entities with an appropriate licence may passport such licence into Czech Republic via the standard notification procedure under EU legislation. The local licensing procedure might be relatively complex and of a considerable length, particularly in respect of new licences frequently used by fintech companies, such as licences under the PSD2 (in 2018, only one company – SPENDEE, with the assistance of FINREG PARTNERS law firm – obtained such licence).

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

Protection of personal data is generally governed by European Regulation No. 2016/679 (GDPR), which applies equally to fintech companies as a result of the law. There are not any special legal requirements or regulatory guidance relating to personal data specially aimed at fintech companies.

The collection and transmission of data are only permitted if mandated by law or a contract, or with the prior consent of the affected individual. Individuals may withdraw their consent and require the deletion of all their personal data anytime. They may request detailed information from every data processing organisation about whether and to what extent their personal data is or has been used. When the security of personal data is breached, the processing organisation is obliged to inform the Czech Office for Personal Data Protection within 72 hours.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

Yes, the GDPR applies to the collecting, processing or use of personal data in the EU, irrespective of whether the data processor is

established in EU or not. That means that that fintech company has to comply with the GDPR even when it carries out the processing of personal data outside the EU. The GDPR also restricts transfers of personal data outside the EEA, unless the country has an adequate level of personal data protection.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

The Czech Office for Personal Data Protection may impose sanctions such as enforcement notices, orders to suspend data processing and fines. The maximum fine can be up to EUR 10 million or up to 2% of global turnover for legal entities, and EUR 20 million or 4% of world turnover according to the GDPR. The amount of the fine depends on the nature of the breach. In addition, breaching entities may also be obliged to pay damages to individuals. Criminal sanctions may also be imposed in certain cases of significant breach. In such cases, imprisonment of up to eight years or prohibition of activity may be imposed.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

Cybersecurity is regulated by Act No. 181/2014 Coll. (Cybersecurity Act), which provides a general framework of regulations for the IT security of critical infrastructure. The law defines critical information infrastructure as an element or system of elements of the critical infrastructure in the sector of communication and information systems, within the field of cybersecurity. In other words, only systems, networks, or elements directly related to critical infrastructure may be considered as part of critical information infrastructure. Critical infrastructure consists of nine groups, one of which is the financial market.

The National Cyber and Information Security Agency (NCISA), the main state body for cybersecurity, may decide that a financial entity is a basic service operator and as such, it is subject to the obligations set out in the Cybersecurity Act and its implementing regulations. Financial entities may thus be subject to obligations to, e.g., detect cybersecurity events, notify the governmental computer emergency response team of the implementation of any reactive measure, keep safety records, etc.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

Certain fintech companies, such as payment services providers (including account information services providers), virtual currency wallet providers or exchange operators (or any other entity listed in the AML Act), are subject to AML requirements set out in Act No. 253/2008 Coll. on selected measures against the legitimisation of proceeds of crime and financing of terrorism (the AML Act).

If a fintech company falls under the scope of the AML Act, the relevant requirements will apply to them in the same way as in the case of other financial institutions. However, according to the Financial Analytical Unit (the supervising authority in respect of AML), AML requirements should apply proportionately, especially in case of certain activities which are less risky from the AML perspective (such as activities of account information service providers).

The main requirements include the obligation to identify customers during the onboarding process and/or to carry out customer AML due diligence, should the customer be a politically exposed person or if such customer is domiciled in a FATF high-risk jurisdiction, or

if the relevant transaction exceeds EUR 15,000, as well as in some other cases. Furthermore, fintech companies falling within the scope of the AML Act shall set up their own internal system of AML risk management in order to properly monitor transactions of their customers from the perspective of AML. Suspicious transactions or suspicious activity of the customers must be notified to the Financial Analytical Office.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

There is no specific regulatory regime that applies for fintech companies in the Czech Republic. However, the general laws, such as the Civil Code, in particular the consumer protection regulation, and the competition and antitrust rules are naturally also applicable to fintech companies.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

All companies must decide whether to hire people on a full-time basis as employees (dependent employment) or freelancers (independent contractors). As regards employment, it is possible to have fixed-term employment contracts or indefinite duration employment contracts. In addition, there are two special types of employment agreements. The first is the Agreement to Complete a Job. The scope of work for which such agreement is concluded may not exceed 300 hours in one calendar year. The second type is the Agreement to Perform Work. This agreement may be concluded by an employer with an employee where the average scope of work does not exceed one-half of normal weekly working hours (40 hours). The relationship based on the Agreement to Complete a Job and Agreement to Perform Work is much easier and faster to be terminated than the employment relationship for both the employer and the employee. If the company hires employees coming from outside of the EU, there is a need to apply for a work permit for non-EU workers. There may also be some visa issues which need to be considered.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Mandatory benefits for employees in the Czech Republic include sick days, where employees are entitled to sick pay leave. During the first 14 days of sickness (excluding the first three days), the employee is entitled to 60% of their average salary from the employer. After this period, sick leave is funded by the social security system. There is also a minimum of four weeks paid vacation per calendar year, social security payments, public health insurance, pension insurance, maternity or parental leave and minimum wage.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

There is no such specific route in respect of fintech. Citizens of the EU, EEC and Switzerland do not require work permits/visas in

order to be employed in the Czech Republic. Citizens from third countries require a work permit explicitly allowing employment with a specific employer in the Czech Republic.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Inventions are mainly protected by patent law. Applicants can file a patent application with the Czech Industrial Property Office. Patents are granted for inventions that are new, involve an inventive step and are susceptible to industrial application. A patent granted in the Czech Republic is valid for 20 years from the filing date of the application and its basic effect represents the right for the patentee to prevent anybody from using the invention without the relevant agreement. The right to utilise a patent is granted by a licence agreement. Business models are not protectable under Czech patent law.

Trade secrets and confidential information are protected under Czech civil law and are also kept confidential during court proceedings.

Brands are protectable in the Czech Republic informally under the provisions on unfair competition contained in the Civil Code, or they may be formally registered as trademarks under the Trademark Act (Act No. 441/2003 Coll.). The application for trademark registration may be filled with the Industrial Property Office by any natural person or legal entity.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

IP rights may be sold, assigned or licensed to third parties. Patentable inventions made by employees may be claimed by the employer as its own, which may thus lead to the financial compensation of the

employee. If there is no agreement stating otherwise, all economic rights in IP developed by employees during the employment relationship are exclusively exercised by employers. The same rules are also applicable to contractors or consultants who developed new intellectual property for the company.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

IP rights are generally territorial rights. There are certain multi-jurisdictional rights and several applicable treaties. The Czech Republic is a party to the Patent Cooperation Treaty, which allows innovators to apply for patent protection in over 140 countries through the centralised application process. For copyright, there is the Berne Convention for the Protection of Literary and Artistic Works 1928, which requires contracting parties to give reciprocating rights to copyright owners whose work is created in one member country and used in another member country. The Czech Republic is also a party to the TRIPS agreement, which includes principles of national treatment and automatic protection.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

IP rights may be exploited directly by the owner of the right or by third parties if they are authorised to do so, typically on the basis of the licence agreement. IP rights may be assigned, licensed and granted as security interests. Usage of IP rights by third parties is usually limited by a contractual agreement between the owner of the IP right and the user, under terms and conditions for the price determined by the parties of such agreement. There are no special restrictions with respect to the exploitation or monetisation of IP rights in the Czech Republic. IP rights and licences need to comply with the general legal framework and mandatory public policy rules.

**Ondřej Mikula**

FINREG PARTNERS
Havlíčkova 1682/15, New Town
110 00 Prague 1
Czech Republic

Tel: +420 773 616 166
Email: omikula@finregpartners.cz
URL: www.finregpartners.cz

Ondřej Mikula is an attorney-at-law and a co-founder of FINREG PARTNERS law firm. He is specialised in fintech, AML/CFT, blockchain and STO, banking and finance and capital markets, including issues of notes and other securities.

Before founding FINREG PARTNERS he worked in one of the biggest Czech law firms, Kocián Šolc Balaščík (KSB), where he advised Czech and international clients in respect of domestic or cross-border issues of bonds and other (hybrid) financial instruments, as well as large loan transactions and M&A. He also participated in the implementation of key pieces of financial regulation (particularly MiFID II or MCD) at Czech banks and other financial markets participants, and on several innovative (fintech) pioneering projects in the Czech Republic (such as in the area of crowdfunding).

**Jan Šovar**

FINREG PARTNERS
Havlíčkova 1682/15, New Town
110 00 Prague 1
Czech Republic

Tel: +420 724 043 058
Email: jsovar@finregpartners.cz
URL: www.finregpartners.cz

Jan Šovar is an attorney-at-law and a co-founder of FINREG PARTNERS law firm. In his practice he focuses on the regulation of the financial sector, securities, fintech, blockchain and STO, payment and banking services, and investment services. He also regularly provides regulatory and compliance advisory services to investment fund and asset management clients.

Before founding FINREG PARTNERS he worked for one of the biggest Czech law firms, Kocián Šolc Balaščík (KSB), and also for the predecessor of ESMA in Paris and for Deutsche Bank in London. Jan has in-depth knowledge on Czech and EU financial market regulatory and related matters, which he gained in part from almost a decade as the head of capital markets legislation at the Czech Ministry of Finance, where he supervised the preparation of key legislative proposals in the area of capital markets (particularly the Czech Management Companies and Investment Funds Act and the legislation on bonds issuance) and represented the Czech Republic at the working committees of the EU Council.



FINREG PARTNERS is a law firm specialised in financial services, fintech, investment funds and capital markets.

Financial services: Our legal and regulatory advice covers a wide range of financial services, including payment services, investment services, banking and consumer credit services. We help compliance departments of financial institutions to understand and to implement new pieces of EU regulation, such as MiFID II, PSD2 and PRIIPS.

Fintech: We provide complex advisory services to fintech professionals and entities in each of their stages of existence, including services in relation to licensing, setting up internal processes and contractual relationships with clients and investments and M&A. We help Czech and foreign fintechs to collaborate with banks and other established financial institutions to further develop their business.

Investment funds: We help clients to establish various investment and asset management vehicles, including licensed investment funds. We provide comprehensive legal and regulatory services to real estate and private equity AIFs and UCITS, including in respect to carrying out investments and marketing to investors. We also assist clients in establishing foreign investment vehicles.

Denmark



Morten Nybom Bethe



Tue Goldschmieding

Gorrissen Federspiel

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Denmark is generally perceived as a country with a high technology penetration ratio. With policy-makers promoting fintech businesses and fintech investments and supporting Copenhagen as an international fintech hub, the fintech scene is flourishing, hatching new start-ups; and at the same time, research is carried out at university level.

The Danish fintech scene is diverse and materialises across a wide palette of financial sub-sectors and digital start-up businesses. The largest group of fintech businesses in Denmark operate within the sector of digital payment solutions with mobile payment currently at the forefront. Danske Bank's "MobilePay" has become the most downloaded Danish app with more than four million downloads as per December 2018 by private users. The app was originally designed to handle and streamline private money transfers, but is now being used as a payment method in shops and e-commerce. However, as a payment method, "MobilePay" is facing increasing competition from other digital payment solutions developed by local Danish businesses, as well as by global players such as Apple, Alphabet and Samsung that have found their way to the Danish fintech scene, enhancing the movement towards a cashless society.

In addition, Danish fintech businesses are becoming increasingly active within sub-sectors such as alternative financing methods supported by online platforms, digital administration of receipts, the sharing economy, solutions for more secure online trading and peer-to-peer lending or investment facilitators that enable non-financial players to offer financial services in competition with traditional financial players. In terms of blockchain technology, two of the biggest Danish market players within digital payments and blockchain payments, Nets and Coinify, are collaborating on testing and developing new business opportunities involving blockchain technology.

Fintech innovation has also influenced the asset management solutions provided by major Danish financial advisors. This particular sector has been affected by the introduction of Robo advice solutions offering automated portfolio planning, automatic asset allocation, online risk assessments, account re-balancing and other digital planning tools.

The current trend of fintech businesses is seeking to partner and collaborate with existing, well-established financial sector players rather than trying to compete against such market players. One recent example is the collaboration between the "neobank" Lunar Way A/S and the Danish bank, Nykredit Bank A/S. Such collaborations offer a way for start-ups to overcome typical market barriers while also allowing banks to offer increasingly competitive and user-friendly fintech solutions to their customers.

Other noteworthy Danish fintech innovation trends include online invoice trading, online debt collection, online advisory systems for pension and personal economical overviews, as well as mobile-based lending services. The introduction of e-money is increasingly gaining attention in the fintech landscape, alongside smart contracts supported by blockchain technology.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

There is presently no specific Danish regulation governing fintech businesses or cryptocurrency-based businesses. Consequently, there is no specific regulation prohibiting or restricting such businesses. Conducting fintech business and cryptocurrency-based business will, however, have to be carried out within the framework established by the Danish regulation on the conduct of financial businesses and the provision of financial services.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

On the whole, new and growing businesses may encounter difficulties obtaining debt funding from banks in Denmark without providing security. However, the Danish Growth Fund (in Danish: *Vækstfonden*) provides debt funding as well as bank securities to businesses that meet certain criteria. Alternatively, new businesses may look for crowd-lending opportunities.

Equity funding can be obtained through venture funds, Danish financial institutions and business angels, but publicly funded innovation incubators can also be relied on if funding is required at an early stage. Additionally, different forms of crowdfunding can be used, although equity-based crowdfunding is not widespread in Denmark, due to legislative obstacles with respect to obtaining a

shareholding in consideration for the funding. Consequently, the funding for fintech start-up businesses is obtained from more traditional sources of funding.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

There are no special incentives schemes for investment in neither tech/fintech businesses nor small-/medium-sized businesses in Denmark.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

Compared with a number of other countries, Denmark faces challenges in making start-up companies grow.

The number of potential Danish IPOs depends heavily on the number of start-ups established in Denmark, how easily they will be self-financing and grow in size, and how many entrepreneurs can resist the temptation to realise their gains early through a genuine M&A transaction.

Companies that are successfully publicly quoted in Denmark are almost always market leaders, for which the risk has fallen considerably as compared to earlier stages of growth. It is only to a limited extent customary to list start-up companies and companies in the intermediate segment.

In Denmark, no mitigating regulatory measures or financially innovative measures exist that can facilitate small- and medium-sized companies' access to the capital markets.

Thus, small IPOs as a source of capital for the growth of high-risk profile start-ups are hardly ever seen.

Stock market listing in Denmark takes place on Nasdaq OMX and DK First North, where listings at the former typically are large listings with international aspects, whereas the listings at DK First North typically are small- and medium-sized companies.

The general legal framework for IPOs in Denmark is set out in the Danish Capital Markets Act, which regulates the prospectus requirements (based on the EU Prospectus Regime). Following the IPO, the newly listed company will be subject to the EU Market Abuse Regulation ("MAR") and its implementing acts as well as a number of national acts, which, *inter alia*, sets out the rules governing the issuer's obligation to publish inside information and the prohibition against market abuse (e.g. insider dealing and market manipulation). Ongoing financial reporting obligations and requirements for major shareholder reporting are covered by the Danish Capital Markets Act.

Nasdaq Copenhagen has also issued certain rules for issuers related to the admission for trading and official listing, specific/recurring disclosure obligations and corporate governance reporting. Furthermore, the Danish Companies Act and the Danish Financial Statements Act include regulation which must be complied with by listed companies, such as rules on governance structure, duties and responsibilities of the board of directors and the executive management, special requirements for the articles of association, general meetings and governance rules on financial reporting.

The regulatory process for launching a prospectus is based on the guidelines published by the Danish Financial Supervisory Authority (the "Danish FSA").

The process for listings and IPOs in Denmark is broadly similar to that which applies in other European jurisdictions. The listing process

for a company with no prior listing, which makes a public offering of shares in connection with the listing, normally takes between three and eight months depending on a variety of circumstances, e.g. the complexity of the company's business and its IPO readiness.

The majority of recent IPOs in Denmark have taken place on Nasdaq Copenhagen's Main Market. However, Nasdaq Copenhagen also operates an alternative marketplace, Nasdaq First North, where smaller listed companies are subject to less extensive reporting requirements. First North has a "Premier segment" for companies voluntarily submitting to the same requirements applicable to companies listed on Nasdaq Copenhagen ("Main Market"). First North may be a starting place for smaller companies to gain access to the capital markets, become accustomed to the legal framework for listed companies, and eventually work towards listing on the Main Market. Another alternative for raising capital on Nasdaq Copenhagen may be to issue and list corporate bonds which are subject to similar but reduced requirements, e.g. in respect of the contents of the prospectus and reporting requirements subsequent to the listing.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

There were no such notable exits in 2018.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

As there is no specific regulation in Denmark targeted specifically at fintech activities, the conduct of such activities must take place within the current framework governing the conduct of financial businesses and the provision of financial services. Thus, the key challenge is to translate the fintech solution into the existing legal framework.

The main Danish legislation is contained in the Danish Financial Business Act (general licensing requirements, etc. relating to financial business), the Danish Capital Markets Act (implements a number of EU financial directives and regulates securities trading, etc.), the Danish Act on Payments (implements the PSD2) and the Danish Services Act. The Danish FSA has stated that the already existing legal framework covers most fintech models.

Note that a licence may be required to operate in Denmark, which is in particular the case for:

- Deposit-taking activities.
- Performing payment services (as defined in the Annex to the Payments Act implementing Annex I of the PSD2).
- Issuing e-money.
- Services related to foreign exchange.
- Investment services and/or investment advice.
- Insurance activities.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

There is presently no specific Danish regulation governing cryptocurrencies or cryptoassets. However, the conduct of cryptocurrency-based businesses must take place within the current legal framework for the conduct of financial businesses and the provision of financial services.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

The focus on fintech innovation is relatively new in Denmark and is therefore an area subject to rapid development. However, Danish policy-makers generally recognise fintech as an important driver for innovation. The Danish government has announced its intention to improve the environment for the fintech sector. Further, there is a significant focus on ensuring – to the extent possible – that, as part of the Danish implementation of the PSD2, it should be easier for fintech start-ups to apply for the necessary licences/authorisations.

The Danish government has set up support schemes for research projects and start-ups in general, primarily organised through the Innovation Fund Denmark (innovationsfonden.dk) and the Danish Growth Fund (www.vf.dk). In addition, through the Danish FSA, Denmark has entered into global partnerships and alliances with the purpose of helping fintech companies doing business beyond national borders, but also with the purpose of attracting foreign companies and talent to Denmark. The Danish FSA has created a dedicated fintech team aiming to minimise regulatory uncertainties and to assist and guide fintech entrepreneurs in the process of obtaining the necessary licences/authorisations.

In order to gain greater understanding of fintech businesses in general and especially the regulative/legislative hurdles of such businesses, the Danish FSA launched an experimental “sandbox” scheme named “FT Lab” in 2018. The purpose of FT Lab is to enable fintech businesses to test new technologies and business models on customers in a safe environment in collaboration with the Danish FSA. The participating companies must, subject to guidance by the Danish FSA, comply with all applicable rules within the existing regulatory framework. The sandbox is not an exception to the rules, but a test environment. The scheme is ongoing and it is too early for the Danish FSA to evaluate the scheme. However, FT Lab is expected to continue, providing the opportunity for new companies to participate.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

As fintech solutions must be provided within the existing regulatory framework, fintech businesses will have to overcome the same hurdles and obstacles that apply to any other provider of financial products and services. If the product or service in question involves conducting financial business, the fintech business cannot provide such product or services without either obtaining the relevant licence or obtaining the relevant passporting rights.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

Regulation (EU) 2016/679 of the European Parliament and of the

Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data, which form part of a filing system or are intended to form part of a filing system. The Danish Data Protection Act supplements and implements the General Data Protection Regulation.

The General Data Protection Regulation applies to all processing of personal data within the scope above. Accordingly, said Regulation applies to any electronic processing of personnel data, including electronic processing in connection with financial solutions such as electronic payments and e-money. The Danish financial regulatory framework also has specific provisions on the processing of personal data in connection with bank operations and electronic payment services. The Danish Data Protection Act specifically regulates the processing of personal data for credit agencies. Accordingly, there is no specific regulation in Denmark of the targeted processing of personal data in connection with fintech activities. The General Data Protection Regulation governs such activities.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

Infringement of the provisions of the General Data Protection Regulation shall be subject to administrative fines up to 10 million EUR or up to 20 million EUR, depending on the infringed provision of the Regulation, or in the case of an undertaking, up to 2% or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher, depending on the infringed provisions of the Regulation.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

The General Data Protection Regulation applies to the processing of personal data activities of an establishment of a controller or a processor in the European Union, regardless of whether the processing takes place in the European Union or not.

The General Data Protection Regulation also applies to the processing of personal data of data subjects who are in the European Union by a controller or processor not established in the European Union, where the processing activities are related to (i) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the European Union, or (ii) the monitoring of their behaviour as far as their behaviour takes place within the European Union.

Further, the General Data Protection Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country (non-EEA country) or to an international organisation shall take place only if the provisions of the Regulation are complied with by the controller and processor, including for onward transfers of personal data from the third country, or an international organisation to another third country or to another international organisation. The provisions in the General Data Protection Regulation Chapter V shall be applied in order to ensure that the level of protection of natural persons guaranteed by the Regulation is not undermined.

Accordingly, the provisions of the Regulation restricts transfer of personal data internationally to a third country, and a transfer requires a specific legal basis.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

There are no specific cybersecurity laws as such in Denmark. Rather, the legal framework consists of several laws promoting cybersecurity, including the current framework governing the conduct of financial businesses and the provision of financial services, including the Danish Financial Business Act, the Danish Act on Payment Services, the Danish Order on Management and Control of Banks and the Danish Order on Outsourcing. According to the latter, companies within the financial sector are required to comply with an extensive set of requirements when outsourcing is a key activity. Examples of these requirements include preparing an IT security policy promoting cybersecurity and preparing a contingency plan as a response to incidents.

Denmark has adopted ISO 27001 as the state security standard, which has been compulsory for public authorities and state institutions to follow since January 2014.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

The provision of financial products and services in Denmark is, in general, governed by the requirements of the Danish AML Act, implementing, *inter alia*, the relevant EU Directives, including the fourth AML Directive, which was implemented into Danish law at the end of June 2017. Therefore, any fintech business will, in general, be subject to the same AML requirements as any other provider of financial products and services.

There is no special regulation in Denmark concerning financial crimes, as this regulation is contained in the Danish Criminal Code. The Danish Criminal Code equally applies to fintech businesses operating in Denmark.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

There is no legislation targeted specifically at fintech businesses. Please see our comments above on data protection and anti-money laundering.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

Denmark does not have comprehensive employment laws. The freedom of contract prevails, though numerous important principles are laid down in case law as well as in mandatory employee protection legislation. Labour market customs and collective agreements also play an important role.

Under the Danish employment legislation, the employer's dismissal of an employee is generally not subject to specific requirements or

approvals although specific notice periods apply to white-collar employees. However, some specific requirements apply in the event the termination of the employment is part of a material redundancy programme, in which case certain rules in relation to process must be followed.

White-collar employees who are dismissed without just cause, and who have been employed for at least one year at the time of dismissal, are entitled to compensation for unfair dismissal. The maximum amount payable is the salary payable for 50 per cent of the statutory notice period. However, if the employee has reached the age of 30, the potential compensation is increased to an amount equalling three months' salary. If the employee has been employed for at least 10 years, the compensation may be increased to a maximum of four months' salary. The amount payable is increased further to six months' salary if the employee has been employed for at least 15 years.

A dismissal is without just cause if it is not reasonably justified by the conduct of the employee, e.g. poor performance or misconduct or by the circumstances of the company, e.g. restructuring or cutting of costs. If the dismissal is due to performance-related issues on the part of the employee, a written warning will normally be required in order to render the dismissal just. As a general rule, the fact that a dismissal is considered to be without just cause does not render the dismissal void. Instead, the employee may be entitled to financial compensation as described above.

5.2 What, if any, mandatory employment benefits must be provided to staff?

The material mandatory benefits are provided for in the Danish Salaried Employees Act and the Danish Holiday Act (in Danish: *ferieloven*).

The Danish Holiday Act provides that employees are entitled to five weeks' holiday per year corresponding to 25 working days, irrespective of whether the employee has earned the right to paid holiday.

The employee earns the right to 2.08 days of paid holiday for each month of employment in a calendar year (qualification year). Holiday must be taken during the holiday year from 1 May to 30 April following the qualification year.

The 25 days of holiday are divided into the main part of the holiday (in Danish: *hovedferien*), which amounts to 15 days, and the remaining part of the holiday (in Danish: *restferien*), which is 10 days.

The employer shall, with due consideration to the operation of the business, to the widest possible extent, meet the employee's wishes as regards to the timing of the holiday, including the employee's wish to take the main part of the holiday during the school holidays of the employee's child(ren).

It is normal practice in individual employment agreements and most collective bargaining agreements to provide for five additional special days off.

Female white-collar employees are entitled to half pay during four weeks of pregnancy leave and 14 weeks of maternity leave pursuant to the Salaried Employees Act. Moreover, white-collar employees are entitled to full salary, including a bonus, during sick leave.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

When employing in Denmark, some basic requirements must always be fulfilled, e.g. the drafting of employment contracts. The

individual requirements will, however, depend upon the nationality of the employee, *cf.* also below. As an example, all EU citizens can remain under his/her home countries' social security scheme for a limited period of time while working in Denmark, provided that he/she fills out certain forms.

Citizens of the Nordic Countries:

Citizens of Norway, Sweden, Finland, and Iceland are covered by agreements between the Nordic countries, which, among others, specify the right to enter and reside in Denmark without a visa or residence permit.

EU/EEA Citizens:

EU/EEA citizens as well as citizens of Switzerland are covered by the EU rules on the free movement of people and services, and are therefore exempt from the requirements of residence and work permits.

The Danish Aliens Act:

The Danish Aliens Act (in Danish: *udlændingeloven*) provides regulation on residence and work permits.

Residence and work permits are normally required if a foreign national wishes to seek a paid or unpaid job in Denmark.

The Positive List and the Pay Limit Scheme:

Foreign nationals from outside the Nordic countries, the EU/EEA and Switzerland, who have been offered a job within professional areas where there is a shortage of specially qualified professionals, will have easy access to a residence and work permit, provided the applicant is in possession of a written job offer or employment agreement and the proposed salary and employment conditions correspond to Danish standards. The Danish Immigration Service has drafted a so-called Positive List with examples of professional fields currently lacking specially qualified professionals.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Fintech products have strong connections to intellectual property law and may enjoy protection from a combination of different intellectual property rights.

As a fintech product rarely does not contain a software code, which is protected under copyright legislation, there will almost always be copyright protected elements in a fintech product. It is most likely that any visual interface, other graphics, audio, video and text of a fintech product also will enjoy copyright protection, provided that they fulfil the copyright legislation's relatively gentle requirement of originality.

The underlying core technology of a fintech product may be patentable or, if it is a smaller invention, protectable as a utility model. Obtaining patent protection is strictly formal, technically complicated and often expensive. This is one of the reasons why utility model protection, which is simpler and cheaper, can be an alternative. The downside to utility models is the 10-year maximum term compared to the 20-year patent duration. If the technology is not patented or protected as a utility model, the owner of the fintech product may, in respect of the product's technology, have to rely on the limited protection of trade secrets.

As a fintech product is typically marketed under a brand, there may also be trademark rights associated with a fintech product. The fintech product may have its own trademark protected name or logo, or the trademarks of others, e.g. the trademarks of the company behind the product may be used in it or in connection with it. In

Denmark, trademarks can be protected as either a registered trademark or an unregistered trademark. An unregistered trademark is established by commercial use of the mark in Denmark.

Finally, except for the technology of the fintech product, the product is likely to enjoy some protection against parasitism under the unfair competition legislation in the Danish Marketing Practices Act.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Copyrights always arise with the natural person(s) who develop(s) the work. This also applies if the work has been created by an employee as part of his/her employment. There are no formalities connected with obtaining copyright protection. The symbol © is often used but it has no legal relevance in Denmark. Registration of copyrights is neither required nor possible under Danish law. A piece of work may be protected before it is completed, as copyright protection occurs as soon as the work has the required originality. Unless otherwise agreed, employees will, as a general rule, maintain ownership of the copyrights to works that they create during their employment. The employer will only receive a right to use the work in the employer's ordinary course of business. The rights are similar to a licence. The same is more or less the case with regard to commissioned work. For works made during employment, there is a specific exception to the main rule with regard to software codes. The copyright to software codes will also arise with the employee programming the code, but the right will automatically and immediately transfer to the employer in all respects. This exception does not apply to commissioned work, and neither does it extend to other parts of a software program, e.g. the graphical interface.

Design rights also arise with natural persons. It is generally presumed that design rights to a design that has been created by employees as part of their employment are automatically transferred to their employer. With regard to Community Designs, this is stated directly in the Council Regulation on Community Designs. In respect of national design rights, there is some uncertainty with regard to designs which also enjoy copyright protection. It is possible that the design rights in these cases will only be transferred to the employer to the extent that the copyrights in the design are transferred.

The rights to an invention, which is patentable or protectable as a utility model, will as a general rule also belong to the natural person(s) behind the invention. This is also the case with regard to inventions created by employees. However, subject to certain requirements, an employer has the right to have the rights to such invention transferred (against payment) and to apply for protection of the invention under the patent or utility model legislation.

A trademark right is a priority right, meaning that the right belongs to the person or company that first registers the mark for the Danish market or acquires the right by commercial use of the mark in Denmark.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

As IP rights are territorial rights, it will in general require rights covering Denmark to enforce against infringements in Denmark.

Copyrights are national rights, but the Danish copyright legislation provides works from other countries, which have acceded to the same treaties/conventions as Denmark, with the same protection as Danish works.

A design can obtain design protection for Denmark by national design registration or Community Design registration through the EUIPO. Further, a design may obtain protection in Denmark as an unregistered Community Design.

A mark can obtain trademark protection covering Denmark through use in Denmark, or by national trademark registration or EU Trademark registration through EUIPO. EU Trademarks are protected in all EU Member States and enforced by the national courts.

In order to obtain patent or utility model protection in Denmark, there are three different ways to go. However, they all result in a national Danish patent or utility model, as applicable: 1) a national, Danish application; 2) an international application under the PCT system; or 3) a European application via the EPO. However, Denmark will also be part of the Unified Patent Court and patents with unitary effects will apply in Denmark as well.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

Danish IP rights are exploited by use in Denmark and may be monetised through assignment, licensing (compulsory or voluntary) and/or through securitisation.

As a starting point, IP rights can be assigned in their entirety, but there are some exceptions for certain types of copyrights, e.g. moral rights.

There are in general no formal requirements for the assignment of IP rights under Danish law. Assignment may be made by oral as well as written agreement. For certain registerable IP rights, including EU Trademarks, it is, however, a requirement that the assignment is made through written agreement.

Instead of assigning the entire IP rights, the rights are often licensed either by exclusive, sole or simple licences. Licences to registered IP rights may, on request, be registered in the public registers. This is not a requirement for validity of the licence, but may be advantageous for documentation purposes and for maintaining priority against third-party interests.

Under Danish law, IP rights can be pledged as security. A security interest is perfected by way of registration of the mortgage with a registration authority.



Morten Nybom Bethe

Gorrissen Federspiel
Axel Towers, Axeltorv 2
1609 Copenhagen V
Denmark

Tel: +45 33 41 41 14
Email: mnb@gorrissenfederspiel.com
URL: www.gorrissenfederspiel.com

Morten Nybom Bethe provides advice to domestic and foreign banks and financial institutions on all aspects of financial law, such as ordinary loan and security agreements, acquisition finance and bond issues, as well as more specialised products, such as securitisation, financial instruments and derivatives. Further, he provides advice on netting, clearing and regulatory matters.



Tue Goldschmieding

Gorrissen Federspiel
Axel Towers, Axeltorv 2
1609 Copenhagen V
Denmark

Tel: +45 33 41 42 03
+45 24 28 68 75
Email: tgg@gorrissenfederspiel.com
URL: www.gorrissenfederspiel.com

Tue Goldschmieding provides advice to Danish and international clients on outsourcing, IT contracts and the protection of information privacy. Tue has extensive experience in complex outsourcing and IT transactions as well as the handling of legislative and security-related issues concerning protection of information privacy.



Gorrissen Federspiel

Gorrissen Federspiel is positioned as one of the leading law firms in Denmark with strong and long-standing international relations. More than half of our 460 employees are lawyers. Gorrissen Federspiel is a fully integrated law firm covering all relevant aspects of business law. Our vision is to continue offering the best possible legal advice while meeting all our clients' additional requirements. We aim to be available at all times, to offer prompt advice and to coordinate complex international cases with foreign law firms. Our Banking and Finance Group covers the full spectrum of banking and finance law. Our IP & Technology Group is a full-service practice focused on patent issues, marketing law and trade mark and design matters. We have established a fintech cross-practice group, which is rooted in our knowledge and experience within different legal areas. Our cooperation across practice groups ensures an efficient one-stop-shop for the provision of high-quality advice within fintech across the practice areas.

France

Bena Mara



Vincent Langenbach



Bredin Prat

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Currently, more than 300 fintechs are operating in France, in particular in the following businesses:

- payment services (including payment institutions and electronic money institutions);
- alternative lending and funding (such as crowdfunding);
- personal and business finance management; and
- banking and insurance services to individuals.

There is also a trend towards growth in payment initiation services and account information services following implementation into French law of the Revised Directive on Payment Services (“PSD2”), by Law no. 2017-1252 of 9 August 2017.

France enacted a statute to permit the use of distributed ledger technology (“DLT”), such as blockchain technology, for the transfer and recording of unlisted securities (*Ordonnance* no. 2017-1674 of 8 December 2017 relating to the use of distributed ledger technology for the representation and transfer of securities). The *ordonnance* came into force on 1 July 2018 and has been further specified by a decree of 24 December 2018, which entered into force on 26 December 2018.

Finally, the French financial markets authority (*Autorité des Marchés Financiers* – “AMF”) held a public consultation regarding the appropriate regulatory framework for initial coin offerings (“ICOs”) in December 2017, the findings of which may lead to adoption of a specific legal framework in 2019 with the enactment of a statute dedicated to the regulation of ICOs (and, more generally, services provided in relation to cryptoassets) (see question 3.2 below).

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

So far there are no particular types of fintech business that are prohibited, but regulated sectors require a licence to conduct business (banking and insurance activities especially) and must

comply with existing applicable regulations. The French banking and financial market authorities have initiated several procedures against companies acting in the fintech sector, including a licence withdrawal procedure and disciplinary proceedings. Operating without such licence may lead to criminal and civil sanctions for the fintech companies and their directors, as well as regulatory sanctions. In this respect, the French banking and financial market authorities regularly issue blacklists of suspect websites and service providers.

More specifically, cryptocurrency-based businesses are not regulated *per se* and are governed by all applicable laws generally, which raises the question of their legal qualification. While no general official publication has been issued on this topic to date, the AMF recently issued an opinion on the legal analysis of cryptocurrency futures, to specify that such future contracts qualify as financial contracts under French law. A statute may be adopted in 2019 with respect to certain services related to cryptocurrencies and crypto-assets (see question 3.2 below).

Regarding foreign investment in France, it should be noted that EU investors benefit from fewer restrictions than non-EU investors.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

Investors usually have recourse to both equity and debt instruments when starting up or developing a business. The instruments commonly used in France include:

- straight equity (shares); and
- straight, contractually subordinated loans.

In practice, financing in France generally consists of a mix of these various instruments, mostly with a combination of pure equity and subordinated debt.

Debt structures can be simple, such as single facility loans, or complex (involving different tranches of debt, such as senior, second lien and/or mezzanine debt, or the issuance of high-yield bonds, or the use of revolving credit facilities).

Furthermore, the French public investment bank (“BPI”) can provide loans to fintechs or invest in their share capital.

Finally, fintech companies can develop partnerships with credit institutions and insurance companies.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

French supervisory authorities (the financial market authority, the AMF, and the banking authority, the ACPR – see question 3.1 below) have jointly set up a support service in order to provide advice on crowdfunding rules applicable to fintech businesses with a view to gaining a competitive advantage and attracting foreign investors.

In accordance with SMEs' incentive tax schemes, and under specific conditions, private individuals having their tax residence in France and investing in fintech companies may qualify for tax benefits (exemptions, reductions or deferrals) in personal income tax (*impôt sur le revenu*, or "IR").

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

The main company types authorised to carry out an IPO are French *sociétés anonymes* (a form of limited company) or *sociétés en commandite par actions* (limited partnerships with a share capital), as well as foreign equivalent companies.

The company must meet certain requirements relating to the market on which it is to be listed, including, in principle, the following:

- companies to be listed on Euronext have to provide three years of certified accounts (and additional half-yearly interim accounts in certain cases) under IFRS. The minimum float must represent 25% of the company's share capital or 5% if it represents a value of at least €5 million (on the basis of the offer price). The IPO also requires the preparation of a prospectus to be approved by the AMF;
- companies to be listed on Euronext Growth have to provide two years of audited accounts, under either IFRS or French accounting standards. The minimum float must represent €2.5 million. The IPO requires the preparation of a prospectus to be approved by the AMF except in the case of a private placement with qualified investors, which requires only an offering circular which does not have to be approved by the AMF; or
- for companies listed on Euronext Access, requirements are less stringent than for Euronext and Euronext Growth. Disclosure requirements are lighter and there is no minimum marketing amount, but the IPO requires the preparation of a prospectus approved by the AMF in the case of a public placement.

In order to facilitate access to financial markets for small and mid-cap companies, Euronext has also developed a platform dedicated to the financing and promotion of such companies, Enternext.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

Since most of the French fintech companies have less than five years of activity, there have only been a few notable exits by founders in France, even though there is a trend in the increase of investments in fintech; examples include Boursorama's acquisition of Fiduceo, a fintech company specialising, *inter alia*, in account information services, the acquisition by Natixis of Dalenys, a fintech company specialising in payment services, or the acquisition by La Banque Postale of KissKissBankBank, a crowdfunding intermediary. In parallel, a certain number of venture capital firms or banks have invested in fintech businesses. Notable transactions over the past few years include capital raisings by United Credit

(€31 million), Slimpay (€15 million) or Lendix (€12 million), or the acquisition of a controlling stake in Leetchi, a payment services provider, by Credit Mutuel Arkea for €50 million.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

The two main regulators in charge of supervising fintech companies are the AMF and the French banking and insurance authority (*Autorité de Contrôle Prudentiel et de Résolution*, the "ACPR").

Unlike the Financial Conduct Authority, which has implemented the "sandbox" concept in the United Kingdom, consisting of an experimental phase with lighter regulation for fintech businesses, fintech businesses in France do not benefit from preferential regulations. The French regulators' approach consists of personalised assistance to fintechs by providing comprehensive support concerning regulatory requirements. In line with the "Guide to assessments of fintech credit institution licence applications" issued by the ECB in March 2018, the French regulators hold fintech banks to the same standards as other banks and apply a comparable regime to them.

However, a specific regime has been set up for crowdfunding actors, creating two specific categories:

- crowd-sourced investment advisers (*conseiller en investissements participatifs*, "CIP"), whose purpose is to provide investment advice regarding crowdfunding via a website. A CIP may arrange up to €2.5 million in financing for projects, exclusively through ordinary shares or fixed-rate bonds; and
- crowdfunding intermediaries (*intermédiaire en financement participatif*, "IFP"), which have a platform available on their website allowing private individuals to assess a project's investment potential for the purchase of goods or the provision of services. An IFP may arrange up to €1 million in financing for projects through loans with a maturity of less than seven years. Each private individual may provide loans of up to €2,000 per project with interest and €5,000 per project without interest. No threshold applies in the case of a gift.

As regards other fintech companies, the applicable regulations depend on the nature of their business. Specific categories include, *inter alia*:

- credit institutions, investment services providers, payment institutions or electronic money institutions (requiring a licence);
- a status introduced by PSD2, i.e. account information service providers (*prestataires de services d'information sur les comptes*); and
- financial investment advisers (*conseiller en investissement financier*, "CIF"), banking or payment service intermediaries (*intermédiaire en opérations de banque et en services de paiement*, "IOBSP") or insurance intermediaries (*intermédiaire d'assurance*) (simply requiring registration).

Fintech companies may also qualify as "intermediaries in other assets" (*intermédiaires en biens divers*), which may constitute in the future a single category with token issuers (see question 3.2).

Certain exemptions exist where it is not necessary to obtain a licence to pursue payment services or electronic money services.

The grant of a licence or registration does not necessarily imply an authorisation for "door-to-door" selling, unsolicited commercial contact at home, at work or any other unusual place, which falls within the scope of different regulations.

Engaging in the abovementioned businesses without complying with the licence or registration requirements may lead to criminal sanctions.

More generally, applicable regulations relate to capital and insurance requirements or obligations with respect to client information, internal procedures, anti-money laundering and governance practices.

Finally, the AMF held a public consultation regarding the appropriate regulatory framework for ICOs in December 2017, the findings of which may lead to adoption of a specific legal framework in 2019 with the enactment of a statute dedicated to the regulation of ICOs (see question 3.2 below).

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

The French central bank clarified in a recent publication that cryptoassets are defined by article L. 561-2 of the French Monetary and Financial Code, as “*any instrument containing, in numerical form, non-monetary units of value that can be held or transferred for the purpose of acquiring a good or a service, but not representing a claim on the issuer*”. This article provides for certain AML obligations for entities acting on a usual basis as counterparty or intermediary with a view to acquire or sell such instruments (see below). In the same publication, it is stated that crypto-assets cannot have a legal course in France and are not considered electronic money.

However, entities providing services as intermediaries in the exchange of cryptocurrencies against legal tender in France are already required to be approved as payment services providers.

In addition, as of early 2019, the French Parliament is discussing a draft governmental bill which aims at introducing tokens into French law and setting up the legal framework applicable to ICOs. A draft of this bill has been adopted by the second Chamber of Parliament (*Sénat*) but is yet to be reviewed and discussed before the first Chamber of Parliament (*Assemblée Nationale*) as of the writing of this chapter.

The current state of the draft governmental bill as adopted by the second Chamber of Parliament, and before any further potential amendment which may be discussed and made before the first Chamber of Parliament, would entail the enactment of the following legal framework:

- The “token” (*jeton*) would be defined as “*any immaterial asset representing, under digital form, one or several rights which may be issued, registered, deposited with or transferred via a distributed ledger technology system allowing for the identification, directly or indirectly, or the owner of said asset*”.
- The issuers of tokens would fall within the same category as the “intermediaries in other assets”, leading to the creation of a new legal category consisting of the “intermediaries in other assets and token issuers”.
- Granting of an optional visa from the AMF could be required by the token issuer in the context of the ICO he would carry out. Obtaining such visa would not be mandatory to carry out an ICO; however, the AMF visa on the white paper issued by the token issuer would signal to the market that the token issuer has taken all required steps to ensure safeguarding of the assets collected in the context of the ICO. Granting of such visa from the AMF would entail for the token issuer the obligation to comply with certain obligations relating, *inter alia*, to AML rules, the issuance of a white paper, the provision of sufficient guarantees and certain investor information rights. Also, the draft bill introduces the obligation for credit institutions to set up clearly-defined rules regarding access to a bank account for issuers of ICOs having been granted such visa.

- A framework enabling the setting up of a secondary market for tokens and digital assets would be implemented, with the creation of a new category of service providers defined as “services providers on digital assets” (“*prestataires de services sur actifs numériques*”). Such services providers may opt for an optional licence status from the AMF leading to the application of several requirements such as professional insurance, client information and complaint, internal control, conflict of interests and IT/security obligations, shareholder monitoring procedures as well as specific obligations depending on the nature of the business exercised.
- In any case, such service providers on digital assets would have to register with the AMF should they provide the services (i) to safeguard private cryptographic keys or digital assets on behalf of third parties, to hold, store and transfer digital assets, or (ii) to buy or sell digital assets in legal tender, leading, *inter alia*, to the application of good repute/competence requirements in relation to their directors and beneficial owners.

As part of the 2019 Finance Bill, France has enacted a specific tax regime regarding the sale of crypto-assets by individuals acting in the context of the management of their private wealth. This regime provides for tax neutrality upon exchange of crypto-assets against one another and for a 30% flat tax rate upon cash out. In addition, as from 1 January 2020, French taxpayers will have to declare to the French tax authorities their crypto-assets accounts opened abroad (in a foreign exchange for instance).

The French competent body for accounting rules (*Autorité des normes comptables*) also released guidelines in December 2018 on how to treat, accounting-wise, crypto-assets from the issuer and the holder perspectives.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

French authorities are very receptive to fintech innovation and technology-driven new entrants.

The ACPR and the AMF have set up a joint support unit in order to: (i) direct fintech companies to the relevant authority depending on the nature and the scope of their business activity; and (ii) discuss and identify the requirements resulting from such innovations so as to respond with the proportionate regulatory measures.

They also regularly provide training and presentations to the fintech sector, including in fintech incubators.

The French legislator also appears very attentive to fintech businesses. A decree was released on 28 October 2016 that introduced “*minibons*”, which may be offered to the public by crowd-sourced investment advisers or investment service providers. Such commercial papers may be registered in the books of the issuer individually or registered by shared electronic means (e.g. distributed ledger technology, such as blockchain technology), making France one of the first countries in the EU to legislate on this new technology.

Additionally, as mentioned above, France recently enacted a statute to permit the use of distributed ledger technology for the transfer and recording of unlisted securities (*Ordonnance* no. 2017-1674 of 8 December 2017 relating to the use of distributed ledger technology for the representation and transfer of securities). The *ordonnance* came into force on 1 July 2018 and has been further specified by a decree of 24 December 2018, which entered into force on 26 December 2018, which also addresses the pledging of securities so recorded.

Lastly, and as set out above, there is no particular “sandbox” option available for fintechs in France, where authorities rather apply the proportionality principle and assist fintechs by providing comprehensive support concerning regulatory requirements. As mentioned above, in line with the “Guide to assessments of fintech credit institution licence applications” issued by the ECB in March 2018, the French regulators hold fintech banks to the same standards as other banks and apply a comparable regime to them.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

The licences and registrations required for certain fintech businesses and the prohibition of customer solicitation mentioned above (question 3.1) constitute hurdles to the provision of services in France.

For EU entities, thanks to the EU principles of the freedom to provide services and the freedom to establish a branch, these hurdles can be overcome. In this respect, a simplified and accelerated licensing procedure allows companies to run an insurance, investment, credit institution, payment initiation or electronic money business in France if they are eligible for the European passport procedure. If the existing activities are supervised by the competent authority in their home country, any documents already available in English can be used by the ACPR. However, certain fintech activities may not benefit from the accelerated European passport procedure (including those that do not require a licence, such as CIF or IOBSP).

More specifically, for non-EU entities, the MIF II Directive 2014/65/EU and MIF Regulation 600/2014, applicable as from 3 January 2018, have introduced new ways to access the European investment services market. Non-EU entities may provide investment services and ancillary services to professional clients and eligible counterparties on a transnational basis without setting up a subsidiary or a branch in France, provided that (i) an equivalence decision has been adopted by the European Commission, (ii) a cooperation arrangement has been established between the ESMA and the relevant competent authority of the third country, (iii) such non-EU entity is registered with the ESMA, and (iv) any dispute relating to the services provided under such regime by the non-EU entity shall be submitted to the jurisdiction of a court in a Member State. Non-EU entities may also provide investment services and ancillary services to retail clients by either (i) setting up a branch in France, which must be approved by the ACPR to provide such services in France, or (ii) setting up a subsidiary in France, which must be approved by the ACPR to provide such services in France, the said subsidiary being in this case allowed to passport its authorisation in other EU countries.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

France regulates the collection/use/transmission of personal data. The legal basis for such regulation is the French Data Protection Law no. 78-17 of 6 January 1978 and its implementing decree no. 2005-1309 of 20 October 2005, and from 25 May 2018, the General Data Protection Regulation (“GDPR”). French data protection law

has been amended by the French Data Protection Law no. 2018-493 of 20 June 2018, which brought the provisions of French law into line with the GDPR. There are provisions relevant to the processing of personal data in other French statutes, including the Criminal Code, Consumer Code, Public Health Code and the Property Code.

Data protection laws apply to fintech businesses operating in France to the extent such businesses process personal data.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

Article 5 of the French Data Protection Law provides it applies to any kind of data processing when (i) the data controller is established on French territory, or (ii) the data controller, although not established on French territory or in any other Member State of the EU, uses means of processing located on French territory.

Article 3 of the GDPR expands upon article 5 of the French Data Protection Law and provides that the Regulation applies to any kind of data processing when (i) the data controller or processor is established in the EU, or (ii) the data controller or processor is not established in the EU, but the processing relates to: (a) the offering of goods or services to data subjects in the European Union (even where the goods or services are provided for free); and/or (b) the monitoring of their behaviour (e.g. by online tracking) if that behaviour takes place in the EU. Under both the French Data Protection Law and the GDPR, international transfers of data to jurisdictions that do not provide a sufficient level of protection of individuals’ privacy, liberties and fundamental rights with regard to the actual or possible processing of their personal data (e.g. the United States), are restricted, although the laws also specify the means for achieving such transfers in compliance with legal requirements (e.g. use of agreed contractual clauses or Binding Corporate Rules).

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

Public enforcement of privacy laws in France can be both administrative, carried out by the French data protection agency (the CNIL), and criminal, performed by the public prosecutor. Those two forms of enforcement are independent and can be implemented simultaneously or separately, and both authorities can exchange information regarding their respective investigations. Non-compliance with data privacy laws may also give rise to claims from individuals seeking damages.

Under the GDPR, the CNIL may impose a range of sanctions including the issuance of enforcement notices, orders to suspend data processing and the imposition of fines. The maximum fine which can be issued by the CNIL is in line with the GDPR, namely €10 million or 2% of global turnover for legal entities, or €20 million or 4% of global turnover for legal entities – depending on the nature of the breach. The French Criminal Code also imposes sanctions for the breach of provisions relating to the protection and respect of private life, including imprisonment for up to one year and a fine of €45,000.

An entity’s failure to notify information security breaches, which may involve personal data (see question 4.4 below) may also result in additional fines by the authorities responsible for enforcing relevant security breach notification laws.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

France has a number of laws that address information security.

The French Data Protection Law of 6 January 1978 and the GDPR provide that data controllers and data processors must take all appropriate technical and organisational measures, with regard to the nature of the data and the risks of the processing, to protect personal data and, in particular, to prevent it from being altered, lost or accessed by non-authorised third parties. The CNIL has provided guidance on specific technical measures that satisfy the statutory obligations.

The GDPR introduces a mandatory data breach notification obligation for all data controllers; previously, only certain types of controller were required to notify the CNIL of breaches. Other laws containing mandatory breach notification rules, which may be relevant to fintech companies, include the French Monetary and Financial Code and the draft law implementing the National Information Security Directive (2016/1148) (“NIS Directive”), applicable to Operators of Essential Services (“OES”) and Digital Service Providers (“DSP”). Like the GDPR, the NIS Directive (and the draft French implementing law) also requires OESs and DSPs to identify network security risks and implement appropriate technical and organisational measures to protect against such risks, manage incidents and ensure continuity of service. A list of OESs will be published by the government but will include banks and key financial market participants. DSPs include operators of online marketplaces, cloud service providers and search engines.

The GDPR also introduces an obligation for data controllers to conduct data privacy impact assessments prior to the commencement of significant new data processing operations or technologies. Part of the assessment, which must be documented, must include a review of the security measures being adopted to protect personal data.

In addition, articles 323-1 to 323-8 of the French Criminal Code provide sanctions for different kinds of unauthorised access to automated data processing systems. Also, French law has transposed the security incident notifications of PSD2 and payment services providers must notify the Banque de France or the ACPR without undue delay in relation to major security or operational incidents.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

France has set up an enhanced regime of anti-money laundering requirements, recently extended by the implementation of the EU’s Fourth AML Directive (20 May 2015). As a principle, fintechs subject to supervision by the AMF or the ACPR must identify their customers, and, as the case may be, the effective beneficiaries of transactions using a risk-based approach prior to entering into a business relationship. The scope of such obligations varies depending on the circumstances of the transaction, e.g. they are less cumbersome if the funds come from or are sent to a bank account located in the European Economic Area or are more restrictive where the customer relationship is entered at a distance, i.e. without physical attendance of the other party.

France has adopted a strict position regarding anonymous electronic money and prohibits anonymous digital financial transactions. The risk of money laundering is assessed by the service provider which must set up an internal system to manage such risk and maintain up-to-date information throughout the duration of the business relationship. Any suspicious activities by a customer must be reported to the French anti-money laundering authority (TRACFIN). In addition, both the AMF and the ACPR may conduct audits and on-site inspections of compliance by fintechs of their AML obligations.

Specific rules also apply to the use of electronic money. In December 2016, French law limited (i) payments of debts by electronic money to a maximum of €3,000, (ii) the amount of deposits, withdrawals or repayments using prepaid cards of €1,000 per month, and (iii) the amount of electronic money stocked on a prepaid card to €10,000.

France also enacted in 2016 and 2017 the requirement for all non-listed companies registered in France to declare the individuals who are their ultimate beneficial owner(s), as from 1 April 2018, in accordance with the Fourth AML Directive.

To be noted is that further extension of the AML regime will be made in the course of the transposition of the Fifth AML Directive (30 May 2018). Such transposition into French law will have to be made prior to 10 January 2020. The directive provides, *inter alia*, for:

- the application of the European anti-money laundering obligations to providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers; and
- the public nature of the Member States’ registries of beneficial owners (subject to certain exceptions).

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

Please refer to question 2.1.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

Hiring procedures

The administrative hiring formalities consist of completing a single reporting form, which must be sent to the Labour Authority within eight days prior to the employee’s start date. In addition, the following formalities may notably be required:

- When employers hire their very first employee, they must inform the labour inspector of the hiring.
- Employers must register their company with complementary pension funds.
- When hiring a non-French employee, the necessary immigration formalities must be carried out.
- The full names of all employees must be recorded in the personnel ledger.
- The employer must arrange for the employee to undergo a medical examination.

Dismissal procedures

In France, employees’ employment contracts can be terminated either for “personal” reasons (e.g. because of the employee’s conduct) or for economic reasons. In both cases, dismissals must be based on valid and serious grounds.

The dismissal procedure includes, most importantly, a pre-dismissal meeting with the employee concerned (or an information/consultation of staff representatives) and the delivery of a dismissal letter stating the grounds for the dismissal. It should be noted that the procedure applicable to “protected employees” (essentially staff representatives) provides for additional steps prior to notification of the dismissal, which include an authorisation from the Labour Inspectorate.

An employee who is dismissed is entitled, *inter alia*, to:

- paid leave compensation;
- compensation *in lieu* of notice (except in the case of dismissal for gross or wilful misconduct); and
- severance pay, which is provided for by the law, the collective bargaining agreement or, in some cases, the employment contract.

If a court finds the dismissal to be unfair, employees will also be entitled to damages.

5.2 What, if any, mandatory employment benefits must be provided to staff?

In addition to the mandatory minimum wage stated by law (or by the National Collective Bargaining Agreement if more favourable to the employee), employees must be provided with supplemental health insurance. The employer must also pay half of the public transportation expenses incurred by the employees to commute to work. It should also be noted that employees are legally entitled to five weeks of paid leave per year. The applicable collective bargaining agreement may, however, provide for additional/better benefits.

Companies having 50 employees or more are also required to share part of the company's annual profits with its employees and to grant staff representatives specific budgets.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

With the exception of citizens from Switzerland, Andorra, the Vatican, San Marino, Monaco or European Union countries, foreign workers need, in principle, a work permit in order to be hired as an employee by a French company. In such case, the employer in France is required to file an application with the Labour Authority prior to the hiring of the employee. In this context, the Labour Authority will take into consideration several factors when deciding whether or not to grant a work permit (one of the main factors being the employment situation within the relevant profession or geographical area).

The same applies for the transnational posting of workers (i.e. when an employer, usually based outside of France, gives an employee a specific assignment that has to be carried out in France, with the intention that, once the assignment has been completed, the employee will resume their work within their home company). Regardless of the citizenship of the employee posted, the foreign employer is required in any case to send a pre-posting declaration to the Labour Authority.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Innovations and inventions are protected by intellectual property legislation, mainly through patents, trademarks, designs and patents rules. Nevertheless, software developments and computer programs are only protected by copyright, unless they are deemed to be a part of a patented invention.

- Patents: French patentability requires an invention to be new, inventive and with an industrial application. Applicants can

file a patent application with the French National Intellectual Property Office ("INPI"): patents are granted for a 20-year period as from the date on which the application is filed.

Furthermore, a European patent, called the "unitary patent", provides uniform protection across 25 EU countries in one step, after being filed at the European Patent Office. A Unified Patent Court will also offer specialised and exclusive jurisdiction for litigation involving European patents.

- Copyright: please refer to question 6.2 below.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Software developments and computer programs are covered by copyright, which also protects literary works, music and art, but does not protect ideas or concepts.

Copyright arises automatically from the mere act of creation without any formalities, and confers on the author an imprescriptible and non-transferable moral right. It also grants the author property rights lasting up to 70 years after his death, which may be defended by actions for infringement.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

In order to protect IP rights, the owner must pay annuities or renewal fees and maintain exploitation; failure to do so may allow, for example, third parties to obtain a compulsory licence with respect to a patent or apply for judicial revocation with respect to a trademark.

In the case of a French registered fintech, a filing of its intellectual property rights (in particular patents) should be made first with the INPI before extending it to any international protection. In this respect, France has ratified the main international conventions regarding IP rights (such as WIPO PCT, WIPO Madrid and WIPO Hague), which ensure such rights are recognised in countries which are a party thereto and are enforceable in France.

It is to be noted that, as regards foreign countries that are not party to such conventions, innovations or inventions will only be filed with the French INPI, which will only protect the respective intellectual property rights within the French territory.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

The owner of IP rights has exclusive rights to exploit them for a certain duration and can thus bring any relevant legal action in the event of infringement of such rights.

IP rights can be assigned either in whole or in part by the owner and may also be subject to a licence allowing their exploitation.

Acknowledgments

The authors would like to thank Julia Apostle, counsel at Bredin Prat, and Timur Celik, Adrien Soumagne and Maxime Garcia, associates at Bredin Prat, for their invaluable contribution to the preparation of this chapter.

Tel: +33 1 44 35 35 35 / Emails: juliaapostle@bredinprat.com / timurcelik@bredinprat.com / adriensoumagne@bredinprat.com / maximegarcia@bredinprat.com.

**Bena Mara**

Bredin Prat
53 quai d'Orsay
75007 Paris
France

Tel: +33 1 44 35 35 35
Email: benamara@bredinprat.com
URL: www.bredinprat.fr

Bena Mara is an associate specialising in banking and financial regulation and mergers and acquisitions. She holds law degrees from the Paris II University and Paris I University, and an LL.M. from the University of Cologne. She is admitted to the Paris Bar.

**Vincent Langenbach**

Bredin Prat
53 quai d'Orsay
75007 Paris
France

Tel: +33 1 44 35 35 35
Email: vincentlangenbach@bredinprat.com
URL: www.bredinprat.fr

Vincent Langenbach is an associate specialising in banking and financial regulation and mergers and acquisitions. He holds a law degree from the Paris II University, a finance degree from Sciences Po and an MSc from the University of Oxford. He is admitted to the Paris Bar.

B R E D I N P R A T

Founded in 1966, Bredin Prat is a leading law firm which is highly reputed in its selected practice areas: Corporate and M&A; Securities Law; Litigation and International Arbitration; Tax, Competition and European Law; Banking and Financing; Restructuring and Insolvency; and Employment and Public Law.

With now 180 lawyers in Paris and Brussels, Bredin Prat has successfully grown while at the same time respecting the firm's culture and remaining committed to the highest standards of excellence.

Over the years, advice in banking law has become a key element of Bredin Prat's practice. The firm has indeed worked on the majority of landmark M&A transactions (both public and private) in the banking and financial industry in France over the past 30 years, including high-profile privatisations, recommended and hostile tender offers, and contested takeovers.

Bredin Prat has also developed renowned expertise on the regulatory aspects of such transactions, as well as on the day-to-day banking regulation issues of French and international banking and financial groups.

Germany

Dr. Stefan Weidert



Gleiss Lutz

Dr. Martin Viciano Gofferje



1 The Fintech Landscape

- 1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).**

In Germany, fintechs mainly offer services relating to alternative payment methods, automated portfolio management and investment advice, blockchain technology, crowd-funding (including crowd-investing and crowd-lending), automated order execution and virtual currencies. Examples of successful innovative concepts can be found for almost all of these areas. Berlin has grown into one of the global centres for the development of blockchain applications and infrastructure. Well-known projects including the IOTA Foundation, the smart contract platform Lisk, the prediction platform Gnosis, and the tokenisation platform Neufund are located in Berlin. Even though many blockchain projects have their official headquarters abroad for legal reasons, large parts of the management and development levels are physically located in Berlin.

Naturally, there is an increasing focus on smartphone applications in the fintech sector. Many companies, especially in payment and banking, concentrate on optimising classic financial services for smartphones.

In the blockchain area, there is a trend towards tokenisation of real world assets. Various platforms make it their task to link digital tokens with real goods (e.g. company shares or real estate) and thus increase their marketability. Particularly in this area, there are, however, still legal uncertainties.

- 1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?**

There are no types of fintech businesses that are generally prohibited in Germany. That said, German law does not provide for a general privilege for fintech concepts under financial regulatory laws. For that reason, whether a fintech concept requires a licence under German regulatory laws must be carefully reviewed before it is implemented in Germany. The Federal Financial Supervisory Authority (*Bundesanstalt für Finanzdienstleistungsaufsicht* – BaFin) has recently introduced the idea of regulating cryptocurrencies. In particular, this is relevant for cryptocurrency-based businesses.

Although German law does not provide for a general ban on the issuing, trading or possession of cryptoassets, BaFin emphasises that a token could be regarded as a regulated financial instrument depending on its structure.

2 Funding For Fintech

- 2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?**

Both equity and debt financing are available in Germany. In general, equity financing is the most common way to fund new and growing businesses in early stages, whereas debt financing becomes more important in later stages. In debt financing, venture debts are becoming continually more important. Regarding fintech, funding has been largely driven by financial institutions in recent years. German banks have provided financial support to fintech businesses through investment and collaboration, e.g. allowing them to use their products and to develop and launch new technologies and services.

- 2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?**

In Germany, a large number of incentive schemes for investment in small/medium-sized businesses exist which are also applicable for fintech start-ups. The German government-owned development bank (*Kreditanstalt für Wiederaufbau* – KfW) provides different funding programmes mostly consisting of favourable loans, grants or co-financing for small/medium-sized businesses, as well as for innovative research and development projects. Due to Germany's federal structure, various additional programmes are available on a regional level. In particular, the 16 German federal states have their own programmes and development banks.

For business angels (individual investors and small corporate investors who only have up to six additional individual investors), Germany's INVEST Venture Capital Grant provides a 20% acquisition grant for EUR 10,000+ investments in young small/medium-sized businesses, as well as a tax relief on profits in case of an exit scenario.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

The conditions for an IPO vary depending on whether the company wishes to be listed on the regulated market segment (subject to EU securities legislation) or on the open market segment (subject solely to the rules and regulations of a given stock exchange). The Frankfurt Stock Exchange, Germany's largest stock exchange, offers Prime Standard and General Standard listings on the regulated market. While the Prime Standard provides a higher level of transparency and is aimed at large companies, the General Standard also caters to medium-sized enterprises and provides a more cost-effective option. The key requirements for a General Standard listing include:

- a. a valid and audited securities prospectus;
- b. minimum three-year reporting history;
- c. at least EUR 1.25 million probable total price value;
- d. a minimum free float of 25%; and
- e. a minimum issuing volume admitted to trading at least 10,000 shares.

The Frankfurt Stock Exchange also offers an open-market option for small/medium-sized businesses called Scale. The key requirements for a Scale listing include:

- a. inclusion documents or a public-offer valid and approved prospectus;
- b. a minimum two-year company history;
- c. a minimum market capitalisation estimated at least at EUR 30 million; and
- d. a minimum free float of 20% or at least one million free float shares.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

The Naga Group AG was one of the first German fintech start-ups to go public. The IPO was issued in Frankfurt Stock Exchange's Scale segment for a total volume of EUR 2.51 million and was finalised in July 2017. In December 2017, Naga also carried out an ICO and collected approximately EUR 42 million. The ICO caused controversy because the proceeds did not go to the Naga Group AG, but to an unaffiliated company, the NAGA Development Association Ltd., which was founded in Belize. In July 2018, the Scout24 Group acquired the finance portal finanzcheck.de for EUR 285 million. This was one of the largest exits in German fintech. Finanzcheck.de is one of the three leading online consumer credit portals in Germany. As a result of the takeover, Scout24's turnover increased considerably in 2018.

Also in July 2018, Creditsheff raised a total of EUR 16.5 million in its IPO. Founded in 2014, the company developed a digital platform to broker loans to small and medium-sized companies.

Not an exit, but still remarkable in this context, is the recent financing round from the Berlin-based fintech start-up N26 in January 2019. N26 raised EUR 260 million from the New York-based venture capitalist Venture Partners and the Singapore investment fund GIC. In total, N26 has raised over USD 500 million since its foundation in 2013. It is currently valued at USD 2.3 billion.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

There is no general fintech "privilege" under German regulatory law. If a fintech company's business falls under the German banking act, insurance act or investment act, the company must obtain the relevant licence. Necessary licences can include banking licences, licences for providing financial services, payment services licences and insurance licences.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

At present, German law does not provide for any special rules for cryptocurrencies or cryptoassets. The general regulations are valid as far as they are applicable. However, there are many legal uncertainties on this issue. Moreover, the practice of BaFin deviates from the court rulings in certain respects. For this reason, the qualification of a token as a regulated financial instrument requires careful examination in each individual case. However, reform discussions are taking place. The German Government is working on a comprehensive blockchain strategy to be presented by summer 2019 (please see <https://www.bundesregierung.de/breg-de/themen/digital-made-in-de/blockchain-strategie-1546662>).

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

While there is no fintech "privilege", German financial regulators and policy-makers are still receptive to fintech innovation and committed to providing new entrants to regulated financial services markets with support in their endeavours. This can be derived from the numerous measures BaFin has taken in this regard.

In late 2015, BaFin implemented a project group focusing on fintechs. One objective was to ensure that BaFin treats fintech companies and their supervisory concerns appropriately. Another aim was to provide the companies with guidance and to enable them to better understand BaFin's supervisory viewpoint. As of 1 January 2017, the project group's responsibilities were transferred to an organisational unit in the President's Directorate, specifically set up for this purpose.

BaFin also tries to pursue a technology- and innovation-friendly administrative practice; for example, by communicating clearly and promptly. BaFin's website at www.bafin.de offers customised, compact information for fintech companies. Furthermore, BaFin supports direct dialogue by hosting and participating in various events, as well as being available to answer questions.

In June 2016, BaFin hosted its own conference called BaFin-Tech in order to exchange ideas and opinions with founders and company representatives. BaFin President Felix Hufeld received much approval when he pointed out that fintech companies increase the diversity of the financial sector. He also made it clear that BaFin does not want to forestall the development of the market while promising that intensive dialogue with the industry would continue.

In June 2018, Felix Hufeld declared in a speech on blockchain and ICOs that the potential of new technology must not be undermined by over-regulation. Also, in practice, BaFin is prepared to understand and cooperate with blockchain-based projects. The supervisory authority is making an effort to consider specific needs to the extent possible. In the past, BaFin has issued no action letters for various ICOs.

There are currently no regulatory sandboxes in Germany. BaFin has repeatedly stated that all players entering the regulated market must comply with the relevant regulations. Meanwhile, BaFin is also endeavouring to meet the needs of start-ups through target group-oriented communication and cooperation.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

Fintechs which have been established abroad but are looking to expand their business to Germany are subject to the German regulatory regime. This generally includes the various licensing requirements described above. For this reason, it is important to assess in advance whether a licensing requirement applies to the fintech's planned activities in Germany.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

The collection, use and transmission of personal data are regulated by several German and European laws, the most fundamental being the German Federal Data Protection Act (FDPA) and the European General Data Protection Regulation (GDPR). With the European GDPR in effect, the national regime of the FDPA is subsidiary. Therefore, the following explanation is primarily focussed on the provisions of the GDPR.

Generally, the data protection regime of the GDPR is very strict. The processing of personal data is only permitted if mandated by law or with the prior consent of the affected individual. Individuals are entitled to withdraw their consent and request the deletion of their personal data at any time. They can also request detailed information from every data processing organisation about whether and to what extent their personal data is or has been used. If the security of any stored personal data is breached, the processing organisation is obliged to inform the authorities within 72 hours. In order to comply with these obligations, fintech entities may have to appoint a data protection official (DPO). Pursuant to the revised German FDPA, the appointment of a DPO is mandatory if a fintech entity has 10 or more employees (including freelancers).

Additional data protection regulations can be applicable depending on the operating mode of the individual fintech business.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

The GDPR is applicable if data is collected, processed or used inside

the European Union, irrespective of the established location of the data processor. It is also applicable if the data is processed or used outside of the European Union in order to offer services and goods to citizens of the European Union or to monitor their behaviour.

Transferring personal data to jurisdictions outside of the European Union or the European Economic Area is, with few exceptions, only permitted if either the receiving jurisdiction has been approved by a so-called "adequacy decision" of the European Commission or if the parties to the data transfer have provided appropriate safeguards for data protection. The latter can be accomplished by entering into a data protection agreement with the data recipient, using standard data protection clauses officially adopted by the European Commission.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

There are several possible consequences:

- Regulatory fines: Failure to comply with data protection regulation can result in a fine of up to EUR 20 million or 4% of the company's worldwide annual turnover, whichever is higher. The ultimate amount of the fine will be determined in each individual case with respect to, *inter alia*, the duration and severity of the violation, number of affected individuals, possible prior violations against data protection regulations and the cooperation of the respective business with the relevant authorities.
- Criminal penalties: Certain violations of data protection provisions – for example, intentional and unlawful processing of data committed with the intent to cause damage or to gain personal enrichment – are considered criminal offences. Criminal liability for such offences is restricted to natural persons, but where a criminal offence is committed within a business organisation, this can often lead to additional regulatory fines.
- Damage claims: All affected individuals are entitled to claim damages for both material and immaterial damages caused by the violation of data protection regulations. Liability for damages can only be avoided if the organisation committing the violation can provide proof that it bears no responsibility whatsoever for the damage claimed.
- Cease and desist claims: Cease and desist claims can be filed by consumer protection organisations or comparable groups if the data protection practice of an entity violates data protection regulations.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

The German IT Security Act (*IT-Sicherheitsgesetz*) provides a general framework of regulations for the IT security of critical infrastructures. Entities in certain parts of the financial system are considered critical organisations and are therefore subject to these regulations.

Also important are the circulars and interpretation guidelines provided by the BaFin as the general supervisory authority for financial service providers. These circulars and guidelines often set out minimum requirements regarding IT security of financial service providers. For example, the revised version of the Minimum Requirements for Risk Management (MaRisk) and the Banking Supervisory Requirements for IT (BAIT) were both published in November 2017. The BAIT specify expectations towards the management boards of institutions with regard to the secure design of IT systems and corresponding processes, in addition to the relevant requirements placed on IT governance.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

In Germany, the anti-money laundering regulations are codified in the German Anti-Money Laundering Act (*Geldwäschegesetz*). However, the AML Act has recently been amended by an act to transpose the Fourth EU Money Laundering Directive into German law and at the same time to transfer and restructure the Financial Intelligence Unit (FIU). In the course of this process, the AML Act from 2008 was reformulated with the aim of preventing and combatting money laundering and terrorist financing even more effectively.

The AML Act contains a list of entities subject to anti-money laundering requirements, including credit institutions, alternative payment services providers and investment firms. As far as fintech firms fall under one of the categories listed in the Anti-Money Laundering Act, the AML requirements apply to them in the same way as they would to any other financial services institution. The German Anti-Money Laundering Act requires the mentioned entities to identify their contractual partners and to continuously monitor their business relationships. Furthermore, it obliges the entities to report suspicious transactions and to establish measures which support the prevention of money laundering.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

There is no other specific regulatory regime that applies to fintech firms in Germany.

However, the general German laws and codes, such as the German Civil Code, the German Commercial Code and the competition and antitrust rules also apply to fintechs operating in Germany.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

Businesses primarily must decide whether to hire staff on the basis of dependent employment relationships or as freelancers. While employees enjoy certain legal rights (such as protection against unfair dismissal, paid vacation and sick pay), as well as social security protection (i.e. employee and employer both have to pay social security contributions), the structuring of freelance relationships is more flexible. The legal qualification of a contractual relationship (i.e. freelance relationship or employment relationship) relies, first of all, on an overall assessment of all characteristics of the contract. However, the structure and wording of the respective contract is only one aspect to be considered. The second aspect is the actual implementation of the service relationship. The main criteria for making this differentiation are whether the business instructs staff as to when, where and how to perform services, if staff are integrated into the work organisation of the business, have regular working times and a regular monthly income and essentially work for only one business. If so, then an employment relationship exists with these staff members. A similar distinction must be determined when third-party contractors are commissioned; a line must be drawn between contracts of work/services (*Werk-/Dienstverträge*) and personnel leasing

(*Arbeitnehmerüberlassung*). A false categorisation of an employee as a freelancer or contractor can be asserted by individual staff members or ascertained by the authorities. The consequences for such violations can be substantial, including the legal fiction of an employment relationship, payment of additional salary, income tax and social security contributions, as well as criminal prosecution. In cases of doubt, the relationship should be carefully examined. In order to clarify whether or not an employment relationship exists, a voluntary status determination procedure can be initiated with the German Pension Insurance Association (*Deutsche Rentenversicherung Bund*).

When hiring staff and in the course of the employment relationship, just as in other European Union Member States, businesses may not discriminate on account of racial or ethnic origin, gender, religion or belief, disability, age or sexual identity. For example, when interviewing job applicants, an employer may not ask any questions which do not legitimately relate to the envisaged relationship. Otherwise, an applicant is allowed to misstate facts in order to safeguard his or her privacy rights and may claim financial compensation in case of discrimination.

An employer's ability to terminate an employment relationship unilaterally is severely restricted by the German Protection against Unfair Dismissal Act, which essentially applies to all establishments with more than 10 employees, for employees who have been employed at the same company for more than six months. Where applicable, an ordinary dismissal will only be effective on one of three legally recognised grounds: personal grounds; conduct-related grounds; or for operational reasons. If a dismissal is invalid, the employee has a right to be reinstated. German law does not provide for mandatory severance payments, but it is quite common to agree on a severance payment in order to reach a mutual termination agreement or to settle a court proceeding. Furthermore, any termination of an employment relationship must be in written form and in compliance with certain minimum (statutory and/or contractual) notice periods.

Employment relationships are generally concluded for an unlimited term. Fixed-term agreements are only valid if they are (i) justified on objective grounds, or (ii) limited to a maximum total term of up to two years (with three extension agreements within this two-year term at maximum). This two-year term can be extended to up to four years (with unlimited extension agreements within this four-year term) within the first four years after setting up a company (not including restructurings of existing companies or groups).

5.2 What, if any, mandatory employment benefits must be provided to staff?

German employees enjoy far-reaching employment protection laws. The social security system provides for health, nursing care, unemployment, pension and employee accident insurance. The employer is obligated to pay the total sum to the competent authority, while internally the contributions are roughly split evenly between the employer and the employee (i.e. the employer deducts the employee's part of social security contributions from the employee's gross monthly salary). The joint social security contributions amount to around 40% of the employee's gross monthly salary up to certain income thresholds. The employer's part is paid on top of the employee's gross monthly salary.

Mandatory employment benefits further include paid annual vacation leave (statutory minimum of four weeks, often voluntarily extended to five or six weeks), sick pay (up to six weeks for the same illness), minimum wage (currently EUR 9.19 gross per hour/EUR 9.35 effective from 1 January 2020), maternity leave (generally six weeks prior to the expected date of birth and eight weeks after the date of

birth), parental leave (up to three years) and special protection against dismissal for certain groups (severely disabled employees, pregnant women, employees on parental leave, works council members).

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

There are generally no specific regulations for obtaining permission for employees of fintechs. Only members of the management body must fulfil certain requirements regarding knowledge, skills and experience (equivalent to the management in old economy credit institutes, but with a stronger focus on IT skills with regard to the BAIT – see question 4.4 above).

As in all businesses, citizens of the EU, EEC and Switzerland do not require work permits/visas in order to be employed in Germany. Citizens of other countries require a work permit explicitly allowing employment with a specific employer in Germany. Citizens from the USA, Australia, Israel, Canada, Japan, New Zealand and South Korea are privileged, as they are entitled to apply for such a work permit after they have entered Germany. Privileges may also apply to highly qualified third-country nationals.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Inventions are mainly protected by patent law. Patent protection principally requires that three criteria be met, namely novelty (not previously available to the public), inventive step (differs from prior art) and industrial applicability (can be made or used in any kind of industry, including agriculture). Furthermore, under German law, a patent is only granted for a technical invention. This means that mathematical methods, schemes for doing business or computer programs as such are not patentable. It should be noted, however, that computer programs may be protected under copyright law and that certain software-related inventions may be patentable.

In contrast to patents, protection of a copyright does not require that the relevant right be registered. Secret innovations can also be protected as business secrets and know-how. Under EU Directive 2016/943, the protection of know-how has recently been substantially extended.

Branding and domains can be protected by trademark and trademark law, while certain optic and design elements of websites can be protected by design rights or copyrights.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

A patent, trademark or design is originally owned by the respective applicant, but can be sold, assigned or licensed to third parties. For patentable inventions made by employees in the scope of their employment, the German Act on Employee Inventions (*Arbeitnehmererfindergesetz*) provides special provisions. The employer has to decide whether to claim the invention or to leave it to the employee. If the employer decides to claim the invention as its own, it may have to financially compensate the employee.

Copyright protection as such is permanently linked to the individual creator (which must be a natural person) of the protected work and cannot be assigned. It is possible, however, to grant exclusive or non-exclusive licences to third parties, and rights in employee works are interpreted by statutory rules to be licensed to the respective employer by virtue of the employment contract unless the contract indicates otherwise. With regard to computer programs that have been created by an employee within the scope of his or her employment contract, it is deemed by the German Copyright Act (*Urheberrechtsgesetz*) that the employer can exercise all economic rights in such program (again: unless indicated otherwise in the employment contract). Please note, however, that this does not apply to managing directors, shareholders (who are not employees) or freelancers, such that rights in software created by these persons must be specifically secured by agreement.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

IP rights are generally territorial rights. There are, however, some multi-jurisdictional rights and several applicable treaties. The respective IP rights are distinguished as follows:

- Both trademarks and designs can be registered as unitary European Union Community rights, which provide protection in every Member State of the European Union. The proprietors of these Community rights can protect and enforce their rights in the national courts of all Member States of the European Union. Trademarks may additionally or alternatively be internationally registered through the Madrid system provided by the WIPO. An international trademark is not a unitary right, but consists of a multitude of national trademark rights. International registration alone allows applicants to simultaneously apply to several jurisdictions of their choice.
- Patents may be registered as so-called European patents at the European Patent Office (EPO) pursuant to the European Patent Convention (EPC). Unlike a European trademark, a European patent is not a unitary right, but a group of essentially independent nationally enforceable patents, comparable to an international trademark. As Germany is also a member of the Patent Cooperation Treaty (PCT), an international patent application can be filed with WIPO in accordance with the PCT. The result is once again a group of independent, nationally enforceable patents. The long-planned Unitary Patent for the European Union has not yet come into force.
- Copyright protection in Germany does not require registration of the copyright. Citizens of EU Member States and the European Economic Area states (Iceland, Liechtenstein and Norway) enjoy full copyright protection in Germany. For this, it is irrelevant where the work was created or whether and where it has been published. Citizens of other countries enjoy the rights granted under international treaties if their home country is a member of those treaties. The most important treaties are the Berne Convention for the Protection of Literary and Artistic Works, the WTO Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS) and the WIPO Copyright Agreement (WTC). These grant protection relatively close to German copyright laws. Citizens of countries which are not party to said treaties only enjoy full copyright protection for their work if it has been published in Germany within 30 days of its first publication in the world.

The relevant rights may then be enforced in Germany using the German civil, administrative and criminal enforcement remedies.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

The most common forms of exploitation of IP rights are selling (assignment), licensing and use as a security interest. For patents, trademarks and designs, none of these options requires any contractual formalities or registration with their respective registers.

For patents, a registration of an exclusive licence, and for trademarks, a registration of any licence is possible. As copyrights cannot be transferred themselves, licences are used as the prevalent method of exploitation. Copyright licences that cover currently unknown forms of exploitation require written form.

Exploitation of IP rights is restricted by the general rules of competition and antitrust law, which are heavily determined by European Union regulations.



Dr. Stefan Weidert

Gleiss Lutz
Friedrichstraße 71
Berlin, 10117
Germany

Tel: +49 30 800 979 190
Email: stefan.weidert@gleisslutz.com
URL: www.gleisslutz.com

Stefan Weidert is a partner at Gleiss Lutz and the head of their ICT and digital economy practice. Stefan mainly advises and represents clients in connection with complex ICT projects (e.g. outsourcings, carve-outs, procurement projects), and on e-commerce, digitalisation and licensing issues. He regularly advises start-ups and investors on IP, IT, commercial and competition matters of their businesses and investments.



Dr. Martin Viciano Gofferje

Gleiss Lutz
Friedrichstraße 71
Berlin, 10117
Germany

Tel: +49 30 800 979 175
Email: martin.viciano-gofferje@gleisslutz.com
URL: www.gleisslutz.com

Martin Viciano Gofferje is a partner at Gleiss Lutz and co-heads the Gleiss Lutz focus group Venture Capital as well as the Gleiss Lutz focus group Healthcare and Life Sciences. His practice areas are M&A, private equity, venture capital and corporate law. This includes advising clients in complex national and cross-border M&A transactions and joint ventures, as well as advising start-ups and investors in financing rounds and exits.

Gleiss Lutz

Gleiss Lutz is one of the leading full-service law firms in Germany. With over 300 lawyers, including 86 partners, and offices in Berlin, Düsseldorf, Frankfurt, Hamburg, Munich, Stuttgart and Brussels, our practice covers all areas of commercial law.

We are known for using efficient team structures, and have one of the lowest leverage ratios in the German market. It is a principle of ours to avoid overstaffing. Our lawyers are committed to providing legal advice that is practical, commercial and in line with our clients' corporate strategy.

Our clients can rely on us to assist them anywhere in the world: we have close ties to independent leading law firms from all over the world. These excellent relations enable us to put together international project teams, pooling expertise and know-how across borders to provide seamless client service of the highest quality.

Gibraltar



Javi Triay



Jay Gomez

Triay & Triay

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Gibraltar's economy continues to grow year on year and this has largely been due to the financial services and gaming sectors. Gibraltar is well known as a gaming and e-gaming jurisdiction, being home to numerous blue-chip gaming companies (such as Bwin Party, Ladbrokes, Coral, Bet365, etc.).

Since the Government's announcement, in 2017, that it would be establishing a regulatory regime to regulate providers that store or transmit value belonging to others using DLT, Gibraltar has seen an astonishing growth in the DLT sector and has cemented its position as a blockchain-friendly jurisdiction. This has included companies establishing Gibraltar vehicles for Initial Coin Offerings ("ICOs") and seeking licensing in Gibraltar as crypto exchanges or crypto wallet providers.

The Financial Services (Distributed Ledger Technology) Regulations 2017 ("DLT Regulations") came into force on the 1st January 2018 and regulates any entity which, by way of business, stores or transmits value belonging to others using DLT. This licensing regime was the first of its kind, worldwide. Gibraltar led the way when it came to the creation of a tailored licensing regime engineered for DLT businesses.

As at the date of this publication, the Gibraltar Financial Services Commission ("GFSC") has received over 40 applications and has issued seven DLT providers licences. Whilst Gibraltar is at the vanguard of the DLT revolution, Gibraltar's traditional fintech businesses continue to evolve and grow despite the uncertainty with Brexit. Two new gaming companies have recently been established: MoPlay and LottoMart. Furthermore, companies such as Easy Payment Gateway Limited continue to push the boundaries in the online payments' software space, amassing countless awards in Spain and elsewhere for their innovative and technological solutions.

This melting pot of innovative entrepreneurs and savvy individuals with technological background, a pool of service providers that understand the industry, and a welcoming regulatory and taxation environment have created the ecosystem for Gibraltar to establish itself as the fintech jurisdiction of choice.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

Whilst there are no legislative restrictions on the type of fintech business that can be established in Gibraltar, the activity may require licensing under either 'traditional' financial services legislation, the DLT regulations or the token offering regulations, which are scheduled to be published imminently. Advice should be sought in this regard.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

There are a variety of funding mechanisms available to fintech businesses in Gibraltar. Due to the size of Gibraltar's population, and thus there being a relatively small number of angel/cornerstone investors, the option of venture capital funding is limited. This is also the case as a result of a lack of risk that banks are willing to take on. Gibraltar fintech businesses seeking to undertake a VC round will typically look to the UK, and in particular, London, given the cultural and political closeness to the UK.

Many fintech businesses also seek investment via a public offering pursuant to the EU's prospectus directive and/or raise funds through an ICO or STO. The raising of funds through an ICO or STO will also be subject to the token offering regulations which are due to be published shortly. These will require that the issuing company comply with certain risk disclosures and that the smart contract has been audited.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

Corporation tax is set at 10% of profits which accrue or derive from Gibraltar. It should be noted that a firm which is licensed by the GFSC is deemed to be deriving its income from Gibraltar for the purposes of tax. It should be noted that Gibraltar does not have VAT, capital gains tax or withholding taxes. In light of this, there has not been a need to create a special incentive scheme or tax incentive for fintech or small/medium-sized businesses.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

The business would need to produce a prospectus which would need to comply with the Prospectuses Act (which transposes the provisions of the Prospectuses Directive) and the Companies Act (if relevant). The business can, if it so chooses, rely on the specific provisions exempting it from producing a prospectus. If an exemption is not available, then the prospectus would need to be approved by the GFSC. Following the GFSC's approval and relevant passporting notifications, the company would be able to passport into other EU jurisdictions.

If the business is going to list on an exchange, then the listing rules for that exchange would also apply, and in such circumstances it is unlikely that it would be able to rely on any of the exemptions contained under Gibraltar law regarding the publication of the prospectus.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

The fintech sector is still relatively young and whilst there have been a number of private sales of fintech businesses in the last 12 months, the figures in question have not been made public. We expect the trend of private sales to continue within the next six to 12 months, with IPOs to also start during that same period.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

As mentioned above, the applicable licensing regime is completely dependent on the business's activities. It should be noted that traditional financial services regimes may continue to apply notwithstanding that the relevant business may be using blockchain technology. Traditional financial services licences that stem from European Law typically would permit the licensee to passport throughout the European Union.

In the case of firms operating within the blockchain space and not falling into a traditional financial services regime, generally the DLT Regulations will apply. It should be noted that the DLT regime is domestic legislation and therefore does not provide passporting rights. This is the case with all other EU countries that have followed Gibraltar's DLT Regulations.

The DLT Regulations are a principle-based regulation and therefore allow for technological advances without hopefully having to amend and update the law. The GFSC have issued guidance to assist with interpretation of the principles. The DLT Regulations seek to regulate businesses that are "carrying out by way of business, in or from Gibraltar, the use of distributed ledger technology for storing or transmitting value belonging to others". If you fall into this category whilst not falling into traditional financial services legislation, you will need to seek authorisation from the GFSC to be a licensed DLT Provider.

The application process takes in the region of three to four months and will involve an initial assessment by the GFSC, whereby they will determine the complexity level of the business.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

The Government has released for public consultation the draft token bill which will seek to govern the issuance of tokens from in or within Gibraltar. These regulations will apply to both utility token offerings and security token offerings ("STOs"). Consequently, an STO will be required to comply with the provisions of the Prospectus Act and these new provisions.

The regulations are not burdensome, and at their core is the ultimate protection of consumers and the reputation of the jurisdiction. The regulations will apply to all token sales which are seeking to raise funds in excess of a specific level.

They will require the token issuing company to either:

- a. appoint an authorised sponsor (who is licensed by the GFSC to act as the Authorised Sponsor) who will ensure that the risk and legal disclosures are included in the offeror's documentation and that the smart contract has been verified; or
- b. two independent parties, who are verified by the GFSC and who will be required to each confirm one of the following:
 - i) that the risk and legal disclosures are included in the offeror's documentation; and
 - ii) that the smart contract has been audited.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

One must remember that Gibraltar is a small jurisdiction and therefore has the ability to move relatively quickly when necessary. Approximately four to five years ago, industry lobbied HM Government of Gibraltar with the intention of creating another branch to Gibraltar's vibrant economy, and thereby sought to recreate a similar environment that it did with the Gaming sector within the DLT space. What followed was several years of preparation, collaboration and coordination with DLT practitioners to create a regulatory framework that would enable what was, until then, an unregulated industry, to thrive whilst protecting consumers and the good reputation of Gibraltar. Following on from this, the Government has recently released the public consultation for the token offering regulations. This continued desire to be at the forefront of the DLT and crypto revolution is clear evidence of the receptive and innovative approach we in Gibraltar take.

The GFSC prides itself on being approachable and ensures it has proximity to the industry and its practitioners. This has meant that there has been no need to create a sandbox, and instead the GFSC has permitted a sandbox type arrangement with applicants on a case by case basis as and when required.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

Please see the responses at questions 3.1 and 3.2. This will be largely dependent on the exact activities and nature of the business, whether they fall into an existing licensing regime and whether they are seeking to rely on the passporting rights which enable them to provide their services in Gibraltar. With Brexit, it is unknown how these rights will continue, if at all.

The United Kingdom is in the process of enacting a statutory instrument which permits Gibraltar-licensed firms to passport into the UK following Brexit, as they do currently. The same will apply for UK firms wishing to passport into Gibraltar. Gibraltar will be the only country with this unencumbered UK access, unless a deal is reached.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

The collection, use and transmission of personal data (being any information or data from which an individual can be identified) is regulated in Gibraltar. The legal framework consists of: (i) Regulation EU 2016/679 (“GDPR”) (which takes direct effect in Gibraltar by virtue of Gibraltar being a territory to which the regulations of the European Union apply); (ii) the Data Protection Act 2004 (the “DPA”); and (iii) the Communications (Personal Data and Privacy) Regulations 2006 (“data privacy laws”).

Collecting, using and transmitting personal data would each fall within the broad definition of “processing” (defined in each of the GDPR and the DPA). As such, where an individual’s personal data is collected/used/transmitted by a “controller” or “processor” (more on these below), the data privacy laws require that it must be done so lawfully, fairly and in a transparent manner. Some of the legal bases include circumstances where the personal data is processed: (i) with the consent of the individual (whose personal data is being processed); (ii) for the performance of a contract (between the business and the individual); and (iii) for the purpose of complying with a legal obligation (in statute or in an order of the court). Ultimately, the specific lawful basis relied upon by an organisation will be fact-specific, and businesses will need to consider on which basis it may process personal data. Additional consideration should be given where the business is processing “special categories of personal data” (such as data which identifies religious, political or philosophical beliefs).

With data fast becoming the world’s most valuable commodity, most business models will need to consider its compliance with data protection legislation. Fintech businesses will be particularly susceptible to these requirements given the mass amounts of data they will be collecting as part of their business and in order to provide services to their clients. A fintech business will (depending on its specific business model) either be a “controller” (the organisation that decides how and why personal data is used/collected/transmitted) or a “processor” (the organisation that uses/collects/transmits personal data on the controller’s behalf).

By way of additional information, if and when Brexit occurs, the GDPR, along with other EU regulations, will cease to have direct effect. As at the date of writing this chapter, there is no deal to govern the relationship between the United Kingdom (and consequently Gibraltar) and the EU. To ensure the Gibraltar data protection framework continues to operate effectively when the UK is no longer an EU Member State, HM Government of Gibraltar will make appropriate changes to the DPA to absorb the GDPR in its entirety into local legislation.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

The data privacy laws can apply to controllers or processors that may be incorporated/registered outside of Gibraltar, but conducts part of its processing activities through Gibraltar.

The transfer of personal data outside of Gibraltar to a jurisdiction that is outside of the EU/EEA (referred to as a “third country”) is restricted, save for circumstances where one of the following apply:

- i. Adequacy decision: this means that the European Commission has decided that the third country in which the data importer (the entity receiving the personal data) is based ensures an adequate level of protection in respect of that personal data. The effect of an adequacy decision is that personal data can be freely transferred from Gibraltar (or indeed the EEA generally) to that third country without restriction.
- ii. Transfers subject to appropriate safeguards: these are circumstances where the relevant data importer can prove that it maintains appropriate safeguards in respect of personal data. Such appropriate safeguards most commonly take the form of an agreement entered into between the data importer and the data exporter (the entity transferring the personal data) which adopts the EU’s “standard contractual clauses”. These clauses create legally binding obligations on the data importer to provide for such safeguards. Other common forms are the use of “Binding Corporate Rules” (essentially an intra-group code of conduct with regard to data privacy).
- iii. Consent: this includes circumstances where the data subject has given their consent to the transfer of personal data to a third country. This is a less desirable option given that the threshold for the provision of consent is now very high – it must be freely given, fully informed and unambiguous.

It should be noted that when Brexit takes effect, the United Kingdom (and Gibraltar) will no longer be a part of the European Union and, as such, will technically be deemed to be a third country for the purposes of data protection. This means that post-Brexit, data transfers from the EU/EEA to Gibraltar will be restricted and subject to the criteria highlighted above. As at the date of writing, it is unclear whether an adequacy decision will be given in respect of Gibraltar.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

There are a range of sanctions applicable for failure to comply with data privacy laws. Briefly, these include:

- i. Fines: under the DPA, controllers/processors can be issued with fines of up to level five on the standard scale for certain breaches. Under the GDPR, controllers/processors can be issued administrative fines of up to €20,000,000, or to 4% of the controller/processors total worldwide annual turnover (whichever is higher). The fine will depend on the nature, gravity and continuation of the breach that has occurred.
- ii. Criminal liability: the DPA includes a number of criminal offences including the unlawful obtaining, disclosure or procurement of personal data. Where an offence is committed by a company, the company’s directors, secretary or other officers may be personally liable for prosecution.
- iii. Notices: controllers/processors in breach of data protection laws may also be issued with certain notices, including notices that restrict the controller/processor’s ability to process data, and a notice ordering that controller/processor to rectify incorrect personal data.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

The legal framework for cybersecurity in Gibraltar is largely derived from the regulations and directives of the European Union. In addition to the legislation already referred to in this section, fintech businesses should also consider any requirements under the Proceeds of Crime Act 2015 (see question 4.5 below for more). Fintech firms should also take note of any specific licence requirement or other (non-legislative) guidance that might be required of it in connection with the conduct of its business.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

The Proceeds of Crime Act 2015 (“POCA”) transposes into Gibraltar law the 4th Anti-Money Laundering Directive. It imposes certain obligations on relevant financial businesses to seek to prevent the financial system from being used for the laundering of illicit money and the financing of terrorism.

POCA outlines the measures that relevant financial businesses must adopt to prevent money laundering and terrorist financing. A relevant financial business includes, amongst others, all firms that holds a financial services licence issued by the GFSC and more recently token offering companies.

POCA defines relevant financial businesses as:

“Undertakings that receive, whether on their own account or on behalf of another person, proceeds in any form from the sale of tokenised digital assets involving the use of distributed ledger technology or a similar means of recording a digital representation of an asset.”

It should be noted that the GFSC has also issued Guidance Notes which apply to relevant financial businesses.

Accordingly, a fintech business operating in Gibraltar would have to comply with the provisions of both POCA and the GFSC Guidance Notes if it is to be considered a “relevant financial business”.

What does POCA require?

Relevant financial businesses must:

1. appoint a director, senior manager or partner to ensure compliance with the provisions of POCA;
2. carry out customer due diligence measures;
3. conduct ongoing monitoring of its clientele;
4. have internal reporting procedures to enable reporting to senior management and then externally to the GFIU of actual knowledge or suspicions of money laundering or terrorist financing;
5. keep records for at least five years of all business relationships and transactions;
6. take appropriate steps to identify and assess the risks of money laundering and terrorist financing; and
7. have in place appropriate and risk-sensitive policies, controls and procedures proportionate to its nature and size of the business. This should consider and include:
 - (a) customer due diligence measures and ongoing monitoring;
 - (b) reporting;
 - (c) record-keeping;
 - (d) internal control;
 - (e) risk assessment and management;

(f) compliance management including, where appropriate with regard to the size and nature of the business, the allocation of overall responsibility for the establishment and maintenance of effective systems of control to a compliance officer at management level (being a director or senior manager); and

(g) employee training and screening.

Furthermore, and where appropriate having regard to the size and nature of the business, the firm must undertake an independent audit function of the CDD and AML practices for the purposes of testing policies, controls and procedures.

What do the GFSC Guidance Notes require?

The GFSC’s statements of principle for regulated firms are the following:

- Whilst the senior management of a firm is responsible for ensuring that the systems of control appropriately address the requirements of both POCA and the GFSC Guidance NoteS, the GFSC Guidance Notes require that the firm appoint a Money Laundering Reporting Officer (“MLRO”).
- Firms must adopt a documented risk-based approach. The firm should adopt a risk profile and take into account the following four risk elements prior to entering into a business relationship: (i) customer risk; (ii) product risk; (iii) interface risk; and (iv) country risk.
- The GFSC Guidance Notes require that all firms must know their customer to such an extent as is appropriate for the risk profile of that customer.
- The firm must ensure that effective measures are put in place to have both internal and external reporting requirements whenever money laundering or terrorist financing is known or suspected by the firm.
- The firm will establish and maintain effective training regimes for all of its officers and employees to ensure that they understand their obligations under POCA.

POCA and the GFSC Guidance Notes therefore apply to fintech businesses generally when licensed by the GFSC or if they are undertaking a token sale.

Token offering companies must also appoint an MLRO. The policies and procedures required by firms undertaking a token sale should, mainly, focus on the AML/CFT procedural policy adopting the risk-based approach.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

As mentioned throughout, this will depend on the business activities of the fintech business. If, for example, an entity is providing remote gaming services or lending services, then other legislation may also apply. Furthermore, with the incoming token offering regulations soon to be enacted, a fintech business may well also fall within the parameters of the new regime.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

In order for a company to register with the Department of Employment as an employer in Gibraltar, it must have a licence in

place. Depending on the business activity of that particular company, the licence may be issued by the GFSC, the Gambling Commissioner or Business Licensing Authority.

The company is obliged to register all of the vacancies in the company with the Employment Service; these will be advertised for a period of two weeks. It follows that there must be a minimum period of two weeks between the date the vacancy is advertised and the start date of employment. Once a prospective employee is identified the company must provide each prospective employee with a “Terms of Engagement” form, setting out the required details of the employment arrangements. Such Terms must be agreed on and signed by both the company and the employee, and then filed with the Employment Service.

If during the course of the employment relationship there are variations to the initial terms of engagement, the company is required to agree such variations with the employee in writing, and to provide those details to the Employment Service on the appropriate form. Failure to register as an employer and to notify the Employment Service of the employment and/or dismissal of an employee within specific periods of time will be subject to the issue of fixed penalty notices and/or prosecution by the Labour Inspectorate.

If a prospective employee is not an EU national, they are classified as “non-entitled” workers, and as such will require a work permit issued by the Director of Employment on application by the company seeking to employ the individual. Employment cannot commence until such time as the work permit is obtained and any additional immigration requirements are satisfied (please refer to question 5.3 below).

Notwithstanding any contractual periods of notice between the parties, Gibraltar legislation provides for minimum periods of notice dependant on the years of employment. There is also statutory protection for an employee not to be unfairly dismissed and, as such, it shall be for the employer to demonstrate whether the dismissal was fair or unfair. The onus on the employer shall be to show the reason, or if there is more than one, the principal reason for the dismissal, and that it was for one of the reasons that would justify the dismissal such as capability, conduct, redundancy, statutory illegality or breach of a statutory restriction.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Annual Holiday – the entitlement to annual leave starts at a minimum of 15 working days for a five-day working week if employed for less than three years, and increases *pro rata* to 25 days if employed for more than eight years.

Sick Pay – provided that the employee has been continuously employed by the company for at least three months, the illness is reported to the company within three days of the absence and a medical certificate is produced, the entitlement is to two weeks’ full pay and four weeks’ half pay in any 12-month period.

Maternity Leave – the entitlement is to 14 weeks’ unpaid maternity leave.

Parental/Adoption Leave – provided that the employee has been continuously employed by the company for at least one year, the entitlement is to four months’ unpaid leave to be taken up to the child’s fifth birthday or up to five years following adoption. A maximum period of four weeks’ parental leave may be taken in respect of any individual child in any one year, subject to notification requirements.

Time off work for urgent family reasons – the entitlement is to five days unpaid leave in any one year, without prior notice, intended to allow employees to deal with emergencies that may arise in relation

to “immediate family” members, which includes a child under the age of 18, parent, spouse or dependant of the employee who has no other means of support or assistance.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

Persons who are not EU nationals are classified as non-entitled workers, and, as such, require a work permit issued by the Director of Employment on application by the company seeking to employ the individual. Applications are considered on a case by case basis. Employment cannot commence until such time as the work permit is obtained and any additional immigration requirements are satisfied. If the non-entitled worker is issued with the work permit and/or takes up residence in Gibraltar, additional immigration formalities such as visa requirements and permits of residence will need to be obtained.

Work permits will not be issued for a period in excess of one year and will require to be renewed. The Director of Employment may request such additional information as may be required for him to be satisfied that the provisions of the regulations are satisfied. The employer will need to satisfy the Director of Employment that there are no suitable entitled workers – that is to say, EU nationals – capable of undertaking the role. The employer will need to deposit an amount of money with the Director of Employment, equal to the costs of repatriating the worker to his/her place of origin.

The Liaison Department of HM Government of Gibraltar provides assistance and support to the financial services and gaming sectors regarding queries with the Employment Service, Civil Status and Registration Office, Income Tax and Social Security Departments and any other stakeholders.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Gibraltar is not an originating registry for the purposes of patent registrations. Consequently, a patent must be successfully registered in the United Kingdom and one would thereafter apply to have it extended in Gibraltar.

One can also protect brand names and logos as trademarks. However, as is the case with patents, Gibraltar is not an originating registry; therefore, trademarks must be registered in the UK. In a recent addition to this, trademarks that have been registered in the EU have also been permitted to be registered in Gibraltar.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Due to the fact that Gibraltar is not an originating registry, the ownership of the IP must be established in the UK. Following registration, in the UK the rights can be extended to Gibraltar.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

One must ensure ownership of the IP in the originating jurisdiction.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

This is not applicable in Gibraltar as we are not an originating registry.

Acknowledgments

The authors would like to thank Chris Davis, Joseph Gomez and Marta Babiano for their assistance with this chapter. Their input and guidance have been invaluable.

Chris is an associate in the Corporate & Commercial team and regularly advises regulated entities, financial services companies and technology companies on a range of transactions.

With an extensive understanding of data privacy laws, Chris has advised a host of internet-based businesses, regulated financial services companies and online gaming companies with data privacy/protection related issues.

Joseph is a consultant at the firm and forms part of the Employment and Dispute Resolution teams. He regularly advises clients on a wide range of employment matters (contentious and non-contentious). His reputation, commercial acumen, local knowledge and contact base mean that he represents a mix of both national and international employers and Gibraltar employees on all aspects of employment law and human resources matters.

Marta is an associate in the Fintech team and specifically has expertise in relation to AML and CFT. Marta is also qualified as a Spanish lawyer.



Javi Triay

Triay & Triay
28 Irish Town
GX11 1AA
Gibraltar

Tel: +350 200 72020
Email: javi.triay@triay.com
URL: www.triay.com

Javi has advised on a wide variety of financial services matters which include establishing regulated entities and advising them on their applications to the GFSC. He also regularly advises licensed entities with regulatory issues and has advised a number of clients on the establishment of crypto funds in Gibraltar. Notably, Javi was actively involved in the establishment of the first Gibraltar crypto fund to list on a recognised ESMA stock exchange.

Javi has been instrumental in establishing the Fintech team as one of the most highly regarded teams in Gibraltar, and since the enactment of the DLT Regulations, he has been advising numerous blockchain start-ups (to include DLT licences and ICOs) and traditional financial services firms using blockchain technology on their establishment and regulatory position in Gibraltar.

Javi was elected onto the executive committee of the Gibraltar Association of New Technologies and has been consulted by the Government on regulations to govern token sales.



Jay Gomez

Triay & Triay
28 Irish Town
GX11 1AA
Gibraltar

Tel: +350 200 72020
Email: jay.gomez@triay.com
URL: www.triay.com

Jay has developed a strong reputation as an expert in financial services and regularly advises prospective funds, investment managers, insurance companies, insurance intermediaries, banks, e-money institutions, payment service providers, fintech businesses and DLT businesses on licensing requirements and regulatory, operational, passporting and distribution matters.

He has been elected on numerous occasions by the legal community in Gibraltar to represent them on the executive body of the Gibraltar Funds and Investment Association (GFIA) and is the Deputy Chairman of GFIA.

Jay was instrumental in establishing the Fintech team as one of the most highly regarded teams in Gibraltar, and has been described by legal directories as “a rising star”, an “experienced figure in the world of cryptocurrency and blockchain technology”, and as “highly regarded within Gibraltar for his work with crypto funds, as well as on token offerings”, “really knowledgeable in crypto and blockchain”, “super-cooperative” and as understanding “the start-up life and the pain of founders”.

TRIAY & TRIAY

LAWYERS

Triay & Triay was established in 1905 and is a full-practice law firm with offices in Gibraltar and Spain.

Our Fintech team has been instrumental in establishing Gibraltar as a key jurisdiction for fintech and DLT businesses, and is one of the most highly regarded teams in Gibraltar. The team forms part of Triay & Triay’s traditional financial services team and has the experience, industry knowledge and commercial understanding to assist these bold entrepreneurs. The lawyers have also assisted clients, such as payment service providers, with licensing applications and therefore understand the requirements of the licensing process. The team has leveraged its existing knowledge of traditional financial services to assist clients in understanding their regulatory obligations under Gibraltar’s world-leading DLT Regulations.

Hong Kong



Benita Yu



Jason Webber

Slaughter and May

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

As an international financial centre and a gateway to Mainland China, Hong Kong has been continuing to establish itself as a launch pad for fintechs looking for opportunities in Asia and Mainland Chinese fintechs looking to expand internationally. Fintech businesses cover a range of sub-sectors and it is common to see collaborations between established financial institutions and fintech start-ups in this space.

Hong Kong was one of the early adopters of device-based “stored value facilities” (prepaid instruments with monetary value) and has granted 13 stored value facility (“SVF”) licences to non-bank payment service providers to date. More recently, the government has focused on moving Hong Kong to a new era of “smart banking” with numerous initiatives. In September 2018, the Hong Kong Monetary Authority (“HKMA”) launched the Faster Payment System – a round-the-clock real-time payment platform, allowing banks and SVF providers to offer their customers almost instant HKD and RMB payment and fund transfer services supported by the use of mobile phone numbers, QR codes or email addresses. 2018 also saw the grant of Hong Kong’s first virtual insurer licence. The first batch of virtual banking licences was granted in March 2019 to three virtual banks, with another five applications being processed at the time of writing. It is understood that virtual banking applicants ranged from telecommunication operators, fintech companies to global banks. The HKMA also launched in July 2018 an Open Application Programming Interface (“API”) Framework for the banking sector.

In relation to distributed ledger technology (“DLT”), in keeping with Hong Kong’s role as a global trading hub, various major banks have worked with the HKMA to launch (in October 2018) a blockchain-based trade finance platform called eTradeConnect, and will explore opportunities to connect it with trade platforms in other regions.

The HKMA, Office of Commissioner of Insurance (“OCI”) and the Securities and Futures Commission (“SFC”) each operate regulatory sandboxes. Since its launch in September 2016, the HKMA’s sandbox has piloted 43 fintech products – seven in biometric

authentication, five in each of DLT, API and regtech, four in soft token, two in chatbot and 15 in miscellaneous technologies.

Finally, it is notable that Hong Kong is one of the key cities in the Guangdong-Hong Kong-Macau “Greater Bay Area” roadmap announced by the Chinese government in February 2019 to develop and integrate an area in southern Mainland China, Hong Kong and Macau into an innovation and technology hub.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

No particular fintech businesses are prohibited or restricted (except that fintech businesses in the gambling sector are effectively prohibited under Hong Kong’s gambling legislation).

Cryptocurrencies as such are not prohibited, but the offer of cryptocurrencies to investors in Hong Kong (typically as part of an initial coin offering) may, depending on the features of the offering, be subject to Hong Kong’s existing securities law regime. In addition, intermediaries providing services to Hong Kong investors in relation to investments in cryptocurrency-related investment products (such as Bitcoin futures) or funds may be regulated by the existing regulatory regime. See section 3 below for further detail.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

Generally speaking, equity funding by a small number of investors for a private company in Hong Kong is relatively simple and straightforward. However, existing regulatory restrictions in Hong Kong will need to be considered in the context of crowd funding in Hong Kong (including restrictions regarding the public offer of shares and the issue of advertisements/invitations to the public to acquire securities). See section 3 for further detail.

Most new and growing businesses can obtain debt financing from banks and money lenders operating in Hong Kong. Peer-to-peer lending in Hong Kong may be subject to certain restrictions under the current regulatory regime – for example, under the Money Lenders Ordinance and the “regulated activities” regime under Hong Kong’s securities legislation (see section 3 below).

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

The SME Funding Scheme provides financial assistance to SMEs looking to expand their markets outside of Hong Kong and The Innovation and Technology Fund (into which the government injected HK\$10 billion last year) provides financial support for businesses that contribute to innovation and technology in Hong Kong.

Other facilitation measures include the incubation programmes at Cyberport and the Hong Kong Science & Technology Parks (“HKSTP”), both of which provide funding and other support for technology start-ups.

From the 2018/2019 tax year, a two-tier profits tax regime applies (profits tax rate for the first HK\$2 million of profits is lowered to 8.25 per cent, with the standard tax rate of 16.5 per cent for profits exceeding that amount) and enhanced tax deductions are available for eligible R&D expenditure. Key initiatives proposed in the 2019/2020 budget include allocating HK\$5.5 billion to expand the Cyberport programme and expanding the corporate venture fund of the HKSTP to HK\$200 million. Fintech was stated to be one of four key areas of focus (the others being biotechnology, AI and smart city development).

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

The listing criteria depends on whether a business intends to list on the Main Board or the GEM Board (designed for growth companies) of The Stock Exchange of Hong Kong Limited (“SEHK”), and whether the company intends to list with weighted voting rights (“WVR”).

Main Board

For a listing on the Main Board, an applicant without weighted voting rights must meet the following key requirements (amongst others):

Financial Requirements

The applicant should generally have a trading record of at least three financial years and fulfil one of the following three criteria:

1. Profit Test:
 - a. profits attributable to shareholders of at least HK\$50 million in the last three financial years (with profits of at least HK\$20 million recorded in the most recent year and aggregate profits of at least HK\$30 million recorded in the two years before that); and
 - b. market capitalisation of at least HK\$500 million at the time of listing.
2. Market Capitalisation/Revenue/Cashflow Test:
 - a. market capitalisation of at least HK\$2 billion at the time of listing;
 - b. revenue of at least HK\$500 million for the most recent audited financial year; and
 - c. positive cashflow from operating activities of at least HK\$100 million in aggregate for the three preceding financial years.
3. Market Capitalisation/Revenue Test:
 - a. market capitalisation of at least HK\$4 billion at the time of listing; and
 - b. revenue of at least HK\$500 million for the most recent audited financial year.

Accounting Standards

Accounts must be prepared according to HKFRS, IFRS or (in the case of applicants from the Mainland of the People’s Republic of China (“PRC”)) China Accounting Standards for Business Enterprises.

Suitability for Listing

The business must be considered suitable for listing by the SEHK.

Public Float

Normally, at least 25% of the company’s total number of issued shares must be in public hands, with market capitalisation of at least HK\$125 million in public hands.

GEM Board

The same requirements on accounting standards and suitability for listing apply to the GEM Board, but there are less onerous financial requirements compared with the Main Board (given GEM is designed for growth companies), with the key differences being:

Financial Requirements

The applicant must have a trading record of at least two financial years comprising:

1. positive cashflow generated from the ordinary course of business of at least HK\$30 million in aggregate in the last two financial years; and
2. market capitalisation of at least HK\$150 million at the time of listing.

Public Float

The same 25% public holding applies, but with market capitalisation of at least HK\$45 million in public hands.

Weighted Voting Rights

Subject to adopting certain investor protection safeguards, a company is permitted to list with WVRs on the Main Board if (amongst other things) it is considered “innovative” by the SEHK, has a minimum expected market capitalisation of HK\$10 billion and at least HK\$1 billion of revenue for the most recent audited financial year. If its revenue is below this, then it must have a minimum expected market capitalisation of HK\$40 billion.

Xiaomi and Meituan Dianping have listed under the new WVR regime and it is hoped that more high-profile new economy companies will follow suit.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

2018 saw the Hong Kong IPOs of several China-based fintech firms – 51 Credit Card Inc (an online credit card management platform), VCredit Holdings Limited (an online consumer finance provider) and Huifu Payment Limited (a mobile payment provider). In terms of Hong Kong fintech businesses, WeLab Limited (a Hong Kong-based online lending platform) has filed for a Hong Kong listing (since delayed) and it has been reported that TNG FinTech Group Inc. (a Hong Kong-based digital wallet operator) is planning a US listing in 2019.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

There is no specific regulatory framework for fintech businesses

operating in Hong Kong. Such businesses are subject to the existing body of Hong Kong financial laws and regulations.

Fintech firms which carry out “regulated activities” in Hong Kong must be licensed by the SFC unless they fall within an exemption. Types of regulated activities under the Securities and Futures Ordinance (“SFO”) which are more relevant to fintech businesses include: dealing in securities or futures contracts; advising on securities, futures contracts or corporate finance; leveraged foreign exchange trading (which broadly covers forwards); providing automated trading services; securities margin financing; and asset management. In addition, the new regulated activities relating to OTC derivatives (dealing in or advising on OTC derivative products and providing client clearing services for OTC derivative transactions), which are not yet in force, may be relevant to fintech businesses operating in Hong Kong once brought into effect (the timing for this remains unclear).

The SFO regime applies to all types of entities carrying out a regulated activity, whether they provide traditional financial services or activities more typically associated with fintech start-ups, such as crowdfunding, peer-to-peer lending and automated trading platforms. For the regulation of virtual assets, see question 3.2 below.

In addition to the SFO regulated activities regime, other potentially relevant regulatory regimes are summarised below:

- **Banking Ordinance (“BO”)**
The BO provides:
 - (i) no person shall act as a “money broker” unless approved by the HKMA – broadly this covers entities that negotiate, arrange or facilitate the entry by clients into arrangements with banks (or the entry by banks into arrangements with third parties);
 - (ii) no “banking business” shall be carried on in Hong Kong except by a licensed bank – this covers: (a) receiving from the general public money on current, deposit, savings or other similar account repayable on demand or within less than a specified period; and (b) paying or collecting cheques drawn by or paid in by customers; and
 - (iii) no business of taking deposits can be carried on in Hong Kong except by an authorized institution.
- **Money Lenders Ordinance (“MLO”)**
A person carrying on business as a “money lender” in Hong Kong requires a money lender’s licence under the MLO. Broadly, a “money lender” is a person whose business is that of making loans or who holds himself out in any way as carrying on that business. Certain types of loan are exempted, including loans made by a company, or an individual whose ordinary business does not primarily involve money lending in the ordinary course of that business.
- **Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (“AMLO”)**
Under the AMLO, the Hong Kong Customs and Excise Department requires any person who wishes to operate a “money service” in Hong Kong to apply for a Money Service Operator licence.
“Money service” covers: (i) a money changing service (a service for exchanging currencies that is operated in Hong Kong as a business); and (ii) a remittance service (a service operated in Hong Kong as a business for: sending money (or arranging for such) to a place outside Hong Kong, receiving money (or arranging for such) from outside Hong Kong, or arranging for the receipt of money outside Hong Kong).
- **Payment Systems and Stored Value Facilities Ordinance (“PSSVFO”)**
The PSSVFO provides a licensing regime for the issue of “stored value facilities”. Broadly, these are facilities that can

be used to store the value of an amount of money that is paid into the facility from time to time as a means of making payments for goods or services. The regime covers both device-based and network-based facilities.

The PSSVFO also regulates retail payment systems, but only where the failure of a particular system may result in systemic issues for the Hong Kong financial system. It is therefore not relevant to the majority of retail payment systems.

- **Insurance Companies Ordinance (“IO”)**
The IO provides no person shall carry on any class of insurance business in or from Hong Kong unless authorised to do so.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

There are currently no laws in Hong Kong that specifically regulate virtual assets. However, the SFC has issued a number of circulars clarifying its regulatory stance.

The first was a statement published in September 2017 in relation to initial coin offerings (“ICOs”), in which the SFC warned that:

- where the digital tokens involved in an ICO fall within the definition of “securities” in the SFO, dealing in or advising on the digital tokens, or managing or marketing a fund investing in such digital tokens, may constitute a “regulated activity”;
- where an ICO involves an offer to the Hong Kong public to acquire “securities” or participate in a collective investment scheme, registration or authorisation requirements may be triggered unless an exemption applies;
- parties engaging in the secondary trading of such tokens (e.g. on cryptocurrency exchanges) may also be subject to the SFC’s licensing and conduct requirements; and
- certain requirements relating to automated trading services and recognised exchange companies may be applicable to the business activities of cryptocurrency exchanges.

This was followed by a circular published in December 2017 in relation to Bitcoin futures contracts and other cryptocurrency-related investment products, in which the SFC warned that:

- Bitcoin futures contracts traded on and subject to the rules of a futures exchange are regarded as “futures contracts” for the purposes of the SFO, even though the underlying assets of such contracts may not be regulated under the SFO;
- other cryptocurrency-related investment products may, depending on their terms and features, be regarded as “securities” as defined under the SFO; and
- parties dealing in, advising on, or managing or marketing a fund investing in such contracts or products may therefore be subject to the SFC’s licensing, conduct and authorisation requirements under the SFO.

In November 2018, the SFC published a statement and a circular containing measures which aim to regulate the management and distribution of virtual asset funds so that investors’ interests are protected at the fund management or distribution level (or both). The measures do not amend the law or the definitions of “securities” or “futures contracts” – they are intended to clarify the existing law whilst imposing new requirements on intermediaries in the form of licensing conditions.

The November 2018 statement clarified that managing funds solely investing in, or operating platforms which only provide trading services for, virtual assets that are not “securities” or “futures contracts” are outside the scope of SFC regulation. However, the statement provides that the following types of virtual asset portfolio managers and fund distributors will be subject to SFC supervision:

- Firms managing funds which solely invest in virtual assets that do not constitute “securities” or “futures contracts” and which distribute the same in Hong Kong. These firms will typically require a licence for Type 1 regulated activity (dealing in securities) because they distribute these funds in Hong Kong. The management of these funds will also be subject to SFC oversight through the imposition of licensing conditions.
- Firms which are licensed or are to be licensed for Type 9 regulated activity (asset management) for managing portfolios in “securities”, “futures contracts” or both and which manage portfolios which invest solely or partially (subject to a *de minimis* requirement) in virtual assets that do not constitute “securities” or “futures contracts”. Such management will also be subject to SFC oversight through the imposition of licensing conditions.
- Firms which distribute funds that invest (solely or partially) in virtual assets in Hong Kong, irrespective of whether such funds are authorised by the SFC. These firms will require a licence for Type 1 regulated activity (dealing in securities) and are therefore subject to existing requirements, including suitability obligations, when distributing these funds.

The SFC has also released details of a conceptual framework to explore the regulation of virtual asset trading platforms.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

Financial regulators and policy-makers in Hong Kong are receptive to fintech. Banking, securities and insurance regulators have each set up dedicated fintech offices and sandboxes to deal with regulatory enquiries and handle pilot trials respectively. The sandboxes of the three regulators are linked up so that there is a single point of entry for pilot trials of cross-sector fintech products.

The HKMA’s supervisory approach to fintech is risk-based and technology-neutral. It has established a Fintech Facilitation Office to act as an interface between market participants and the HKMA. The HKMA’s sandbox allows banks (together with their partnering technology firms) to conduct pilot trials of their fintech initiatives involving a limited number of participating customers without the need to achieve full compliance with the HKMA’s supervisory requirements. See question 1.1 above for a summary of the pilot trials so far.

The SFC’s approach to fintech is also technology-neutral. It has established a Fintech Contact Point and a regulatory sandbox. The SFC’s sandbox is open to SFC-licensed corporations and start-ups that intend to carry on an SFO-regulated activity to test the activities in a confined regulatory environment before the fintech is used on a fuller scale.

The OCI has also established a sandbox for authorised insurers, as well as a Fintech Liaison Team to enhance communication with businesses involved in the development and application of fintech.

The HKMA and the SFC are members of the Global Financial Innovation Network, to which firms can apply to conduct cross-border tests of innovative financial products or services.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

The SFO licensing regime applies to all businesses carrying out

regulated activities in Hong Kong, whether they are established in Hong Kong or not. A fintech business based overseas which actively markets, to the Hong Kong public, services which constitute a regulated activity, will *prima facie* be regarded as carrying on business in a regulated activity, for which a licence is required. An overseas-based fintech firm would be caught whether it is marketing by itself or through another entity, and whether in Hong Kong or otherwise.

There are various exemptions from the licensing regime, including (for certain regulated activities) dealing only with professional investors, or targeting/carrying on business with a small number of investors in Hong Kong (not constituting the “public”). An overseas fintech firm may also be able to “deal in securities” through another entity licensed to deal in securities or which is a Hong Kong-licensed bank. There are specific requirements in order to fall within the exemptions and specific legal advice in the context of the particular facts should be sought.

The SFO also prohibits overseas firms issuing to the Hong Kong public any advertisement or invitation to acquire securities and other specified products unless prior SFC authorisation is obtained. The definition of “advertisement” is very broad and includes every form of advertising, whether made orally, electronically or by any other means. There are a number of exemptions, including one relating to professional investors. Again, specific legal advice in the context of the particular facts should be sought.

In addition to the SFO regime, fintech businesses intending to operate in Hong Kong, whether or not they are established here, should comply with (or fall within an exemption to) the regulatory regimes under the BO (which includes restrictions on deposit advertisements), MLO, AMLO, PSSVFO and the IO referred to in question 3.1. The extent to which these regimes apply to a fintech firm will depend on the specific nature of the firm’s operations.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

The Personal Data (Privacy) Ordinance (“PDPO”) establishes a principles-based regime which regulates the collection, holding, processing and use of personal data in Hong Kong.

Fintech businesses in Hong Kong which are “data users” (defined as persons who control the collection, holding, processing or use of personal data) are regulated by the PDPO. The principles which data users must observe mainly relate to notification requirements at the time of collection of personal data, accuracy and duration of retention of personal data and security and access to personal data. There are also particular restrictions regarding the use of client lists to market products.

In addition to the PDPO, the Privacy Commissioner for Personal Data (“Commissioner”) has published industry guidance on the proper handling of customers’ personal data, including for those in the banking industry. The Commissioner has issued guidance in relation to the collection and use of personal data through the internet, use of portable storage devices, online behavioural tracking and “cloud computing”, and has issued an information leaflet on physical tracking and monitoring through electronic devices.

Unsolicited direct marketing by electronic means is also covered by the Unsolicited Electronic Messages Ordinance, which applies to

electronic commercial messages with a “Hong Kong link” including those to which the PDPO does not apply. This would cover messages sent by fintech entities to promote their services or investment opportunities over a public telecommunications service to electronic addresses.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

Although the PDPO does not have extraterritorial application, it applies to foreign organisations to the extent they have offices or an operation in (including agents located in) Hong Kong. The PDPO applies to data users that are able to control the collection, holding, processing or use of personal data in or from Hong Kong.

The PDPO contains a restriction on the transfer of personal data outside Hong Kong and transfers between two other jurisdictions where the transfer is controlled by a Hong Kong data user, although this restriction has not yet been brought into force. The restriction, once in force, will prohibit the transfer of personal data from Hong Kong to a place outside Hong Kong unless one of a number of conditions is met, including: the data user taking all reasonable precautions and due diligence to ensure the data will not be dealt with in a manner that would contravene the PDPO; transferring to a place which has data protection laws similar to the PDPO; or where the data subject has consented in writing to the transfer.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

Failure to comply with the PDPO could potentially result in the following sanctions:

- Regulatory action: the Commissioner may investigate complaints of breaches of the PDPO, initiate investigations and issue enforcement notices. A data user who contravenes an enforcement notice is liable to a fine and imprisonment.
- Criminal liability: the PDPO contains a number of criminal offences; for example, failure to comply with requirements of the Commissioner, disclosing personal data without consent for gain or causing loss, and in relation to direct marketing. Maximum penalties for breaches under the PDPO are fines of up to HK\$1 million and five years’ imprisonment.
- Civil claims: individuals who suffer loss as a result of their personal data being used in contravention of the PDPO are entitled to compensation by the data user. The Commissioner may also institute civil proceedings against any data user that fails to comply with an enforcement notice.
- Reputational risk: the results of any investigation, the name of the organisation involved and details of the breaches may be published by the Commissioner.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

In Hong Kong, cybersecurity is dealt with through a range of laws and regulations, including the PDPO and criminal law. There are various criminal offences relating to cybersecurity, such as: damaging or misusing property (computer program or data); making false entries in banks’ books of accounts by electronic means; unauthorised access to a computer with intent to commit an offence or with dishonest intent; and unlawfully altering, adding or erasing the function or records of a computer. Although there is currently no mandatory data breach notification requirement in Hong Kong, the

Commissioner has provided data users with guidance on practical steps in handling data breaches and mitigating the loss and damage caused to the individuals involved.

The Cyber Security and Technology Crime Bureau of the Hong Kong Police Force is the department responsible for handling cybersecurity issues and carrying out technology crime investigations and prevention. It has established close links with local and overseas law enforcement agencies to combat cross-border technology crime.

Cybersecurity remains a key priority for the regulators. The HKMA has launched several significant measures to strengthen cyber resilience in the banking sector, including an enhanced competency framework on cybersecurity. Entities that are regulated as licensed corporations by the SFC are equally expected to take appropriate measures to critically review and assess the effectiveness of their cybersecurity controls. The SFC has issued a circular setting out certain key areas that licensed corporations should pay close attention to when reviewing and controlling their cybersecurity risks, as well as certain controls that such corporations should consider implementing where applicable, and has also recently issued guidelines to mitigate hacking risks associated with internet trading.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

International standards of anti-money laundering and counter-terrorist financing are set by the Financial Action Task Force (“FATF”). As a member of the FATF, Hong Kong implements recommendations promulgated by this inter-government body to combat money laundering and terrorist financing.

Local legislation dealing with money laundering and terrorist financing includes: AMLO; Drug Trafficking (Recovery of Proceeds) Ordinance (“DTROP”); Organized and Serious Crimes Ordinance (“OSCO”); and United Nations (Anti-Terrorism Measures) Ordinance (“UNATMO”).

In addition to the requirements discussed under question 3.1 above, the AMLO imposes customer due diligence and record-keeping requirements on financial institutions (including licensed corporations, banks and other authorized institutions and insurance companies) and certain professions, while DTROP, OSCO and UNATMO require the reporting of suspicious transactions regarding money laundering or terrorist financing and prohibit related dealing activities.

The SFC, HKMA and the OCI have each issued guidance to financial institutions on designing and implementing anti-money laundering and counter-terrorist financing policies and controls to meet AMLO and other relevant requirements.

The Prevention of Bribery Ordinance is the primary anti-corruption legislation in Hong Kong. It is directed at the corruption of public officers (public sector offences) and corrupt transactions with agents which includes employees of private companies (private sector offences).

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

In addition to the legal and regulatory regimes described above, fintech businesses will, depending on the nature and structure of their operations, also be subject to other laws, including: business registration (if carrying on business in Hong Kong); Hong Kong Companies Registry registration (if having a place of business in Hong Kong); and Hong Kong tax laws (noting that corporate income tax applies only to locally sourced profits – not worldwide profits).

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

The requirements for the hiring or dismissal of employees in Hong Kong are not particularly onerous. In relation to hiring employees, a written employment contract is advisable but not strictly required in most cases (although a written notice of certain key terms may be required upon request by an employee). Notification to the Inland Revenue Department is required within three months of commencement of employment. Collective agreements and trade union arrangements are not compulsory and are relatively uncommon in Hong Kong.

Unless there are grounds for summary dismissal (such as habitual neglect of duties), a statutory minimum notice period (or payment *in lieu*) will apply to a notice of termination of an employment contract, and statutory severance or long service payment (but not both) may be payable up to a statutory maximum amount of HK\$390,000. Statutory severance is payable to an employee (with minimum two years' continuous service) who is made redundant. Long service payment is payable to an employee (with minimum five years' continuous service) who is dismissed for any reason other than summary dismissal unless he is already entitled to severance payment.

The employer must notify the Inland Revenue Department (and the Immigration Department if the employee's working visa is sponsored by the employer) of the dismissal. There are no other particular dismissal procedures which must be observed under Hong Kong legislation, but employers must follow any internal company procedures that may form part of the employment terms.

Employers must not dismiss certain protected categories of employees (such as pregnant employees) or in contravention of anti-discrimination laws (e.g. on gender, race and disability). Employees with a minimum of two years' continuous service have a right to make a claim in a labour tribunal for dismissal without a "valid reason", being: the conduct of the employee; his or her capability or qualifications to perform the role; redundancy or other genuine operational requirements; continued employment would be unlawful; or any other reason of substance in the opinion of the tribunal. In practice, unless the dismissal is of a protected category of employee, the remedy which a tribunal may award is usually limited to any unpaid termination entitlements the employee should have received.

5.2 What, if any, mandatory employment benefits must be provided to staff?

The statutory minimum hourly wage (which, subject to approval by the Legislative Council, will be raised to HK\$37.50 from 1 May 2019) applies to most workers in Hong Kong.

Key mandatory employment benefits include:

- enrolment in a mandatory provident fund, with a monthly contribution from each of the employer and employee of 5% of the employee's income. The mandatory element of the monthly contribution by each of the employer and employee is currently capped at HK\$1,500. The requirement does not apply to foreign nationals with an employment visa who are either working in Hong Kong for 13 months or less, or belong to an overseas retirement scheme;

- maternity leave (10 weeks) and paternity leave (three days). Employees with more than 40 weeks' continuous service are entitled to 80% pay during such leave;
- paid annual leave and sickness allowance for qualifying employees; and
- employers must take out insurance in relation to employees' work-related injuries, but there are no compulsory medical benefits.

Certain statutory rights are applicable only to "continuous" employees (those who have worked for 18 or more hours per week for at least four consecutive weeks).

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

Individuals who are not Hong Kong permanent residents would generally require an employment visa to enter Hong Kong for employment purposes under the General Employment Policy ("GEP") (or the Admission Scheme for Mainland Talents and Professionals for nationals of the PRC). The GEP is quota-free and non-sector-specific. The visa must be sponsored by the employer in Hong Kong, who must demonstrate the application fulfils certain criteria, including that the applicant is employed in a job relevant to his academic qualifications or work experience that cannot be readily taken up by the local work force.

More sector-specific is the Technology Talent Admission Scheme, which the government announced in May 2018 to meet demand for talent in the innovation and technology sector. The scheme provides a fast-track arrangement for eligible companies to admit overseas and Mainland talent to undertake R&D work for them and will run on a pilot basis for three years. Eligible companies are tenants and incubates of the HKSTP or Cyberport that are engaged in fintech, biotechnology, AI, cybersecurity, robotics, data analytics or material science. There is a cap of 1,000 people in the scheme's first year.

Individuals who wish to establish or join fintech businesses or start-ups in Hong Kong may also consider an "investment as entrepreneur" visa. Such applications may be favourably considered if the applicant can demonstrate they: (i) are in a position to make a substantial contribution to the Hong Kong economy (by reference to, for example, their business plan, financial resources, investment sum and introduction of new technology or skills); or (ii) wish to start or join a start-up that is supported by a Hong Kong government-backed programme and the applicant is the proprietor or partner of the start-up or a key researcher.

Finally, there is also a quota-based Quality Migrant Admission Scheme which seeks to attract highly skilled or talented persons to settle in Hong Kong in order to enhance Hong Kong's economic competitiveness. Applicants are not required to have secured an offer of local employment but are required to fulfil a set of prerequisites under a point-based test.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Fintech products based on computer programs are protected by copyright in Hong Kong. The Copyright Ordinance recognises

computer programs, and preparatory design materials for computer programs, as types of literary works which can be protected by copyright. Copyright in the source code arises automatically, and registration is not needed or possible.

A database will be protected as a literary work if it falls under the general copyright law in Hong Kong. There are no separate database protection rights in Hong Kong.

In terms of patents, computer programs and business methods “as such” cannot be patented. However, patent protection may be available for software-related inventions that produce a further technical effect. Given the potential difficulties, the common law of confidence may be useful in preventing the disclosure of technical information which is trade secrets.

It is possible to register a trade mark in Hong Kong, which will protect the branding applied to a fintech product.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

No registration of copyright is required or possible in Hong Kong. The general rule is the author is the first owner of copyright. In the case of a computer-generated work, the author will be the person who undertakes the arrangements necessary for the creation of the work.

However, first copyright to works: (i) made by an employee in the course of his employment will belong to the employer (unless a contrary agreement has been made); and (ii) which have been commissioned will belong to the commissioner provided there is an express agreement with the contractor to this effect. The legislation provides: (i) in the case of work produced in the course of employment, further reward for an employee if the use of the work is beyond the parties’ reasonable contemplation at the time it was created (the parties can contract out of this); and (ii) in the case of commissioned work, that even where the contractor is the party entitled to the copyright under the agreement, the commissioner will still have an exclusive licence to exploit the work for purposes reasonably contemplated at the time of commissioning it, as well as the power to stop it from being used for purposes against which the commissioner could reasonably object.

The general rule is that the right to a patent belongs to the inventor. The exception is where the inventor is an employee – in which case, ownership will belong to the employer if certain conditions are met. However, compensation may be awarded to the employee where the invention is of outstanding benefit to the employer (parties cannot contract out of this).

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

For copyright, Hong Kong has an “open qualification” system whereby works can qualify for protection irrespective of the nationality or residence of the author and where the work was first published. This extends the reciprocal protection under various international copyright conventions applicable to Hong Kong (which include the Berne Convention and WIPO (Copyright) Treaty).

Patent registration in the PRC or overseas will not give automatic protection in Hong Kong (and *vice versa*). However, a UK, EU (designating UK) or PRC patent forms the basis of a standard patent application in Hong Kong. Patent protection for Hong Kong via the

international patent system under the Patent Cooperation Treaty can be obtained on the basis of an international application designating the PRC, followed by a further application in Hong Kong after the international application has entered its national phase in the PRC. A short-term patent in Hong Kong is possible in the absence of such designated overseas patents. There is no substantive examination of any patent applications in Hong Kong.

Trade mark protection will require national registration as the international registration of marks under the Madrid Protocol does not currently apply to Hong Kong. However, a bill has been introduced to the Legislative Council in 2019 which, if passed, will apply the Madrid Protocol to Hong Kong (in 2022–23 at the earliest).

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

IP is usually exploited by means of assignment, licensing or the granting of security interests.

Depending on the type of IP right, the formalities for assignments and licences are different. Generally, an assignment must be in writing and signed by the assignor. An exclusive copyright licence should be in writing and signed by or on behalf of the copyright owner. There is no formal written requirement for non-exclusive copyright licences. Patent licences do not need to be in writing but it is encouraged for registration (see below). Trade mark licences must be in writing and signed.

It is important to register transactions (assignments, licences and security interests) concerning registered rights (such as patents and trade marks) on the relevant IP register in order to maintain priority as against third-party interests registered in the interim. Failure to register a patent assignment or exclusive licence, or trade mark assignment or licence, within six months will result in the assignee/licensee being unable to claim damages for any infringement relating to the period before their registration.

In addition to any registration at the relevant IP registry, certain security interests over unregistered or registered rights (copyrights, patents or trade marks) granted by Hong Kong companies should be registered at the Companies Registry within a month in order to protect against creditors.

Acknowledgments

The authors would like to thank their colleague Peter Lake for his contribution to this chapter. Peter is a Partner in the firm’s Hong Kong office and is involved in a range of corporate work, advising companies, financial institutions and fund management groups. He read law at Cambridge University and is qualified to practise Hong Kong and English law. Peter is a member of the APLMA Hong Kong Documentation Committee and The Law Society of Hong Kong’s Investment Products and Financial Services Committee.

Peter is listed in the 2019 edition of *Who’s Who Legal Banking: Finance* in Hong Kong, and as a highly regarded lawyer in the *IFLR 1000 Asia-Pacific 2019* for Banking in Hong Kong. He is recommended in *Chambers Asia-Pacific 2019* for Banking & Finance, and *Financial Services: Non-contentious Regulatory (International Firms)*, China.

The authors would also like to acknowledge their colleagues Lydia Kungsen and Mike Ringer for their contribution to this chapter.

**Benita Yu**

Slaughter and May
47/F Jardine House
One Connaught Place, Central
Hong Kong

Tel: +852 2521 0551
Email: benita.yu@slaughterandmay.com
URL: www.slaughterandmay.com

Benita Yu is a Partner at Slaughter and May. Benita has substantial experience in securities transactions, including cross-border listings and share offerings by overseas corporations and PRC state-owned enterprises, mergers and acquisitions and joint ventures. She also advises on banking and international debt securities transactions.

Benita is a member of the Takeovers and Mergers Panel, the Takeovers Appeal Committee and the SFC (HKEC Listing) Committee of the SFC in Hong Kong and is a member of the Technical Panel and chairs the Company Law Interest Group of the Institute of Chartered Secretaries.

Benita read law at Oxford University and is admitted as a solicitor in England and Wales and Hong Kong, and speaks fluent English, Mandarin and Cantonese. She is listed as a leading lawyer in the *IFLR 1000 Asia-Pacific 2019* for Capital Markets: Equity and for M&A in Hong Kong, *The Legal 500 Asia-Pacific 2019* for Capital Markets (Equity) in Hong Kong, and *Chambers Asia-Pacific 2019* for Capital Markets: Equity and Corporate/M&A (Hong Kong-based international firms, China).

**Jason Webber**

Slaughter and May
47/F Jardine House
One Connaught Place, Central
Hong Kong

Tel: +852 2521 0551
Email: jason.webber@slaughterandmay.com
URL: www.slaughterandmay.com

Jason has been with Slaughter and May for more than 27 years and is a Partner in our corporate, commercial and financing department. He is involved in a wide range of corporate, commercial, financing and asset management work.

Jason is listed as a leading lawyer for Corporate/M&A (Hong Kong-based international firms, China) in *Chambers Asia-Pacific 2018* and in the *IFLR 1000 Asia-Pacific 2019* for Private Equity.

Jason co-authored the Hong Kong chapters of *The Asset Management Review* and *The Mergers and Acquisitions Review*. Jason has sat on one of the disciplinary committees of the Hong Kong Securities and Futures Committee.

Jason is admitted as a solicitor in England and Wales, Hong Kong and the Republic of Ireland.

SLAUGHTER AND MAY

Slaughter and May has a long-standing presence in Asia. Our office in Hong Kong was opened in 1974 and we have extensive experience of a wide range of work throughout Asia.

In particular, we are familiar with the challenges facing clients in the fintech sector, having been involved in numerous transactions for financial institutions, global technology companies, trading platforms, investors and start-ups. Our experience includes advising: ARM on the acquisition of its share capital by SoftBank Group; SoftBank Vision Fund's investment in Ping An Healthcare and Technology and Ping An Medical and Healthcare; Zhong An Online P&C Insurance (China's first internet insurance company) in its first round of fundraising – one of the biggest fundraisings by a Chinese fintech company in 2015; and Alibaba Group on (amongst others) its cornerstone investment in Fosun Tourism Group, privatisation of Intime Retail and acquisition of SCMP Group Limited.

Iceland

Stefán Reykjálín



BBA

Baldvin Björn Haraldsson



1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

In recent years the finance industry has changed rapidly in Iceland with fintech solutions at the forefront of those changes. Fintech solutions are provided by the three largest commercial banks in Iceland: Landsbankinn; Íslandsbanki; and Arion Bank, as well as other independent businesses. Icelanders are generally considered to have a high adoption rate towards new solutions in the financial industry, for example online banking, which quickly became the norm. All of the banks have an online presence and online banking apps. The apps are all being widely used by Icelanders. A very high percentage of online banking users use specific electronic certificates to log in to their online banks. Banks have also offered instant loans with the borrowing process conducted solely by electronic means and interest rates based on the borrower's credit score.

Arion Bank has been hosting Fintech hackathons in cooperation with the payment solutions company Valitor, the information technology company Advania, the IT service centre for Icelandic financial markets RB, as well as Meniga, covered below. Íslandsbanki has also been influencing the fintech market with the mobile app, Kass, as described later, and recently announced a partnership with the global fintech hub LATTICE80.

Besides the three banks, the most notable Icelandic fintech companies include Meniga, Aur, Kass, Netgíró, Pei, Authenteq, Karolina Fund, Creditinfo and Payday. Meniga is the largest of the aforementioned, founded in 2009 and serving over 50 million digital banking users across 20 countries, with offices in Reykjavík, London, Stockholm and Warsaw. The company assists financial institutions worldwide to utilise their data to personalise digital channels and drive customer engagement; for example, by focusing on persons' finance histories and comparing highly-detailed spending breakdowns with other domestic groups.

The most notable fintech innovation trend of the past year is the growth of the mobile apps, Aur and Kass, which are now being very commonly used in Iceland. Kass is operated and offered by Íslandsbanki, in cooperation with the company Memento, while Aur is majority-owned by Iceland's largest mobile phone operator, Nova. To use these apps, the user must link his card details (debit or

credit card) to the app, creating a user profile. Once there, the user can pay, charge or split amounts, by using only cell phone numbers. These amounts are often trivial transactions, such as when buying lunch, reimbursing gas money, splitting restaurant cheques, etc. Aur has also expanded its line of business by starting to offer its own credit cards and instant loans, and was recently nominated as the Best Fintech Startup at the Nordic Startup Awards. Other nominees from Iceland have included Authenteq (electronic certificates), Karolina Fund (crowdfunding), Memento (Kass app), and Payday (invoicing etc.). Furthermore, it is worth mentioning that the second-largest mobile phone operator in Iceland, Siminn, has begun offering a payment solution, Siminn Pay, with similar attributes as Apple Pay.

In January 2018, the Association of Fintech Companies was established as a lobbying group to improve the current operating environment for fintech companies in Iceland. In August 2018, the Fintech Cluster was also established to strengthen cooperation and innovation within the field. Also, it is worth mentioning that, in December 2018, a fintech research centre was established within the University of Reykjavík.

Of course, these are only a few noteworthy fintech innovation trends of the past year, but as can be seen, the focus on fintech businesses in Iceland seems to be on making the banking experience as user-friendly as possible and improving certain banking functions. Other factors, such as peer-to-peer lending or fintech solutions within the insurance market, have yet to have as much of an impact on the market.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

Currently, there are no regulations which specifically govern fintech businesses. However, each fintech business must operate in conformity with any applicable law, especially the general financial regulatory framework. The governmental authority mainly responsible for the supervision of the financial industry, including any fintech business, is the Icelandic Financial Supervisory Authority ("FSA").

Within this financial regulatory framework, restrictions and requirements do apply. For example, this can be seen from a case concerning the company Aktiva, which intended to operate a platform for peer-to-peer lending. The FSA concluded that Aktiva had been operating as a payment service provider without having the relevant licences *cf.* the Payment Service Act (based on PSD I). The FSA suspended Aktiva's operations immediately and Aktiva has since refocused its business.

Last year, the FSA advised the public to be cautious of cryptocurrency-based businesses and issued general warnings against the use and trading of cryptocurrency. Since cryptocurrency is not specifically regulated in Iceland, the FSA reiterated that there is no consumer protection, no backer such as the Central Bank of Iceland, and that its market was showing clear signs of a bubble.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

New and growing businesses have different alternatives to fund their operations. Debt financing is commonly used; for example: bank loans; issuing a bond; or having a line of credit. Usually, security would have to be provided as well. Equity funding can also be obtained; for example, through venture funds or angel investors. Crowdfunding is also utilised in Iceland through platforms such as Kickstarter and the Icelandic Karolina Fund. For new businesses, Iceland also has start-up incubators or accelerators, the most noteworthy being Startup Reykjavík, which is a 10-week long mentorship-driven seed-stage accelerator programme, running from June to August each year. Additionally, there are some public grants and investment mechanisms available to new and growing businesses, for example, from the Icelandic Innovation Center. Finally, there are other available funding sources such as the Enterprise Investment Fund (*i. Framtakssjóður*), the technical development fund operated by The Icelandic Center for Research (*i. RANNÍS*) and innovation grants from the Icelandic Innovation Center (*i. Nýsköpunarmiðstöð Íslands*) and from the three major banks.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

There are no special incentive schemes for investment in tech/fintech businesses. There are, however, general incentives in place for small/medium-sized businesses, for example, for rural areas, i.e., areas outside the capital area, which include reduced tax burdens, exemptions from customs and more. However, the incentives do not apply to investments in companies which provide services on the basis of legislation on financial undertakings, insurance operations or securities. Also, worth mentioning is the New Business Venture Fund (*i. Nýsköpunarsjóður atvinnulífsins*) which invests at the seed and early stages in promising growth companies. The fund is a state-owned investment fund.

There are also tax incentives for foreign experts and incentives for research and development. Foreign experts enjoy a tax exemption for 25% of their salary for the first three years of employment, on fulfilment of certain conditions which include not having been a resident of Iceland for five years. Research and development incentives entail that such costs can be used as a tax deduction.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

Stock market listings in Iceland take place at its two regulated markets: Nasdaq Main Market; and Nasdaq First North, with the former for larger companies and the latter for smaller to medium-

sized companies. Nasdaq has its own rules which state what requirements apply to companies that intend to IPO within the Main Market and First North. Companies wishing to admit their shares at the Nasdaq Main Market must meet the listing requirements set forth in the rules of Nasdaq. Companies wishing to issue on the First North market are also subject to the relevant rules of First North. The listing requirements for the Main Market are largely harmonised between Nasdaq in Helsinki, Stockholm, Copenhagen and Iceland, despite some differences between the locations. Additionally, the rules are based on the European regulatory framework, especially relating to the prospectus.

The requirements include three years of financial statements and operating history, documented earning capacity and a market value of shares of EUR 1 million; with these requirements only applying at the time of admission to trading. Other requirements apply at the time the shares of the company are admitted to trading; as well as continuously after the admission to trading, for example: the company must be duly incorporated or otherwise validly established according to the relevant laws of its place of incorporation or establishment; have a valid signed agreement in place with Nasdaq; and the shares must conform with the laws of the company's place of incorporation, and have the necessary statutory or other consents, and be freely negotiable insofar that any limitations do not interfere with the day-to-day business of buying and selling shares.

Finally, an application for the admission of shares to trading must cover all shares of the same class that have been issued and that are issued in an IPO preceding the first day of trading. There are also requirements relating to the quality of the management and the board of directors, the procedures and controls as well as the mandatory issuance of a prospectus.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

To our knowledge, there have not been any notable exits (sale of business or IPO) by founders of fintech businesses in Iceland. However, the previously-mentioned mobile app Kass was in fact a product originating from the start-up incubator Startup Reykjavík, created by the company Memento. In 2016, Memento founders announced the company's cooperation with the bank, Íslandsbanki. However, the Icelandic fintech market is of course new and emerging, and as such, notable exits by fintech founders could increase soon. However, Fintech companies have recently received extensive funding, e.g. the blockchain identity verification start-up Authenteq which raised USD 5 million, and the crypto fintech start-up Monerium with a USD 2 million round, both in January 2019.

Despite the lack of notable exits, there have been a few acquisitions on behalf of Icelandic fintech companies such as Meniga's recent acquisition of the Swedish fintech company Wrapp in January 2019.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

In general, fintech businesses need to operate within the general financial regulatory framework much like other financial businesses. There is no specific legislation aimed at fintech activities and therefore, the relevant fintech business must align itself to the existing legal framework. The key legislation, in this regard,

includes the Act on Financial Undertakings, the Securities Act and the Payment Services Act. The Payment Services Act awaits the implementation of Directive (“EU”) 2015/2366, PSD II, which is currently under scrutiny by the EEA Joint Committee. Further, companies wishing to provide financial services are subject to the supervision of the FSA and generally must obtain operating licences/authorisations from the FSA to provide their services.

Iceland implements most of its financial regulatory framework from the EU, through its participation in the European Economic Area (“EEA”). In that regard, it is worth mentioning that on 8 March 2018, the European Commission adopted a specific action plan in the field of fintech which might cause amendments that might take effect in Iceland, due to its membership to the EEA.

Despite the legal framework generally predating the fintech changes, there have been initiatives on behalf of the government to respond to this innovation trend, as seen from the answer to question 3.3.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

Cryptocurrency and cryptoassets are not heavily regulated in Iceland. However, on 29 June 2018, a bill was passed amending the Money Laundering Act with respect to the European Union’s 4th Anti-Money Laundering Directive no. 2015/849 approving a registration requirement for parties operating with cryptocurrencies or cryptoassets. The amendment obliges service providers who already offer transactions with virtual money, electronic money and currencies, as well as service providers of digital wallets, to register with the FSA no later than one month after the Act’s entry into force, i.e. before the end of July 2018. The FSA then submits its stance on the relevant registration within 30 days from the receipt of the application.

Also, as mentioned in the answer to question 1.2, the FSA has advised the public to be cautious towards cryptocurrency and cryptoassets and issued general warnings against the use and trading of cryptocurrency.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

The financial regulators and policy-makers in Iceland are generally receptive to fintech innovation and the expected changes to the financial services market. In December 2018, the White Paper on the Future of Iceland’s Financial System was published. It stressed, among other things, the importance of the role of fintech in the future of Iceland’s banking system and its possible effects.

The most noteworthy initiatives have been set forth by the FSA, who set up a specific Fintech Help Desk. The Fintech Help Desk assists those who provide, or aim to provide, new financial services classified as fintech. The Fintech Help Desk operates as an internal fintech task force within the FSA, assisting individuals and companies with regulatory issues or business-specific questions. It is intended to support and promote communication with fintech parties and analyse whether the financial services in question are in accordance with the applicable law and regulations, as well as whether any licences and/or authorisations are required. The procedure operates in a way that a fintech party sends the “FSA

Fintech Questionnaire” to the Fintech Help Desk and then receives a response from the FSA within 10 business days. Subsequently, the relevant fintech party may receive counselling from the Fintech Help Desk by phone (maximum 30 minutes) or request a meeting in person with the fintech task force (maximum one hour).

Despite the FSA being the main governmental driving force within the fintech industry in Iceland, other pertinent governmental institutions may influence the market; for example, the Consumer Agency, the Icelandic Competition Authority and the Icelandic Data Protection Authority. For example, in a decision by the Icelandic Competition Authority, regarding the three commercial banks, aimed at increasing competition between the banks, it concluded that information about the banks’ commission, rates, terms and conditions should be publicly issued on the banks’ websites through an open API interface, of which third parties may benefit. This might increase business opportunities for businesses within the fintech industry. The so-called *access-to-accounts provisions* entailed in PSD II will also influence this aspect considerably.

As concerns regulatory sandboxes, they have not been implemented in Iceland. However, the White Paper on the Future of Iceland’s Financial System does suggest it as one measure to deal with the rapid fintech innovation. To do so, changes to the regulatory framework would be required to authorise the FSA to grant exemptions in those cases.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

The regulatory hurdles are generally the same as for fintech businesses established within Iceland. Fintech businesses operate within the financial market regulatory regime and as such may not provide products or services without the relevant operating licences, authorisations or passporting rights, if applicable. The process is more complex for businesses outside the EEA due to the mutual EU regulatory framework.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/ transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

The regulatory framework concerning data protection in Iceland, is mainly based on secondary legislation from the EU. Iceland regulates the collection, use and transmission of personal data with the Act on Data Protection and Processing no. 90/2018 (“**Act on Data Protection**”) which implements the General Data Protection Regulation no. 2019/679 (“**GDPR**”). The Icelandic Data Protection Authority (“**DPA**”) is the governmental authority responsible for monitoring the application of the Act on Data Protection and administrative regulations based on it. The Act on Data Protection applies to all fintech businesses, much like other businesses, and is especially meaningful within the fintech market as many of these businesses often deal with personal information such as individuals’ financial information.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

The Act on Data Protection applies to the processing of personal data on behalf of a data controller or a data processor established in Iceland irrespective of whether the processing is conducted within the EEA. Further, the Act on Data Protection also applies to data subjects located in Iceland irrespective of whether the data controller or data processor is located within the EEA when either services or goods are provided to a data subject within the EEA or when the behaviour of a data subject conducted within the EEA is monitored.

The Act on Data Protection also covers the transfer of personal data out of Iceland. The transfer of personal data to a country which does not provide an adequate level of personal data protection is generally prohibited, or dependent on exemptions. The Act on Data Protection offers certain points for consideration when assessing whether the level of personal data protection is at an adequate level or not.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

Infringements of the provisions of the Act on Data Protection, and of regulations issued pursuant to it, are punishable by daily fines, cessation or processing, administrative fines ranging from ISK 100,000 to ISK 2.4 billion or a possible prison term of up to three years, unless more severe sanctions are provided for in other legislation. In case of legal entities, it is possible to fine them up to 2–4% of their total turnover. The same punishment shall apply if one does not comply with instructions from the DPA. If the relevant offence is committed as part of the operations of a legal entity, then the relevant legal entity may be fined as provided for in the General Penal Code.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

The Icelandic government issued its policy on cyber security in April 2015. The policy's period ranges from 2015 to 2026 and has the objective of increasing public awareness and the government's capacity in fighting cyber crimes by improving the analysis, preparation and reactions to such crimes, as well as improving the regulatory framework and related law enforcement. In relation to the policy, Iceland will also implement Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information system, also known as the NIS Directive.

Additionally, the Icelandic Post and Telecom Administration runs a special cyber security team, CERT-IS, which officially started operations in June 2013. The team's objective is to mitigate the risk of cyber attacks and other related security incidents in its territory as well as to counteract and minimise any related damage. Finally, Iceland has signed an agreement with the NATO Cyber Defence Management Board while maintaining a generally close relationship with NATO in these matters along with implementing the EU legislation relating to cyber security. Cyber security in Iceland is a field which is closely correlated with the European framework and set to change in line with any changes thereof.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

The applicable legislation is the Money Laundering Act, which has the objective of preventing money laundering and terrorist financing by imposing on parties, engaging in activities which may be used for the purposes of money laundering and terrorist financing, the obligation to obtain knowledge of their customers and their business activities and report to the competent authorities any knowledge of such illegal activities.

The Money Laundering Act implements the EU Directive 2005/60/EC on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing. The Act covers, *inter alia*: financial undertakings, pursuant to the definition in the Act on Financial Undertakings and branches of such foreign undertakings located in Iceland; natural or legal persons which, by way of business, engage in foreign exchange trading or the transfer of funds and other assets; and payment institutions and their agents pursuant to the Payment Services Act, etc. Money laundering is also criminalised under the General Penal Code.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

As with any other business, there are several regulatory regimes that may apply to fintech businesses operating within Iceland and a complete summary depends on the type of fintech business in question; for example, the framework differs for an insurance company compared to a blockchain trader. The following is only a brief outline of any general legislation that might apply for fintech businesses.

For example, the business in question must select its corporate structure with the two types of limited companies available in Iceland: public limited companies; and private limited companies, with the latter being the most common structure. The governing legislation is the Act on Private Limited Companies and the Act on Public Limited Companies. Other structures include publicly owned companies, sole proprietorships/firms, co-operative societies, partnerships and self-governing corporate entities. Foreign limited companies may also establish branches in Iceland.

Regarding tax matters, Iceland has an income tax on limited liability companies of 20% and 37.6% on partnerships and other legal entities other than limited liability companies. Capital gains are added to other taxable income and are taxed at the regular corporate rate. Additional tax is levied on certain companies which carry out financial activity, such as financial institutions, insurance companies, banks and other financial organisations. This additional tax is a financial activity tax of 5.5% based on total salary payments by the relevant entity. Furthermore, there is a specific financial activity tax of 6% levied on the same entities which is calculated on the entity's income tax base of ISK 1 billion or more. Lastly, a specific tax, generally called the bank tax, of 0.376% of companies' debts, is levied on financial undertakings which are authorised as commercial banks, savings banks or credit undertakings. A 24% value-added tax is levied on any sale of goods or services, with various exceptions such as all export sales and services to foreign entities rendered outside of Iceland, as well as services of commercial banks, savings banks, credit undertakings and stock brokerage.

As many fintech products deal directly with consumers, it is worth noting that consumer rights are protected with the relevant consumer legislation, mostly implemented from the EU. If the relevant fintech business is operating within the insurance market, the applicable legal framework is the insurance legal framework. Finally, there are several governmental regulations, issued by the FSA and other institutions within the general financial regulatory framework, which could be applicable to fintech businesses.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

One could say that the Icelandic legal framework around the hiring and dismissal of staff consists of general rules of contractual law, tempered by collective bargaining agreements. In fact, the Icelandic labour market is mainly regulated by collective bargaining agreements. The collective bargaining agreements contain mandatory provisions of minimum rights, such as minimum wages, maximum working hours, paid holidays, paid sick leave, maternity and paternity leave as well as a duty for employers to insure their employees, just to name a few.

Employers and employees are usually authorised to terminate employment agreements, but the agreements generally contain a certain termination notice, most commonly being three months, but a longer termination notice can apply. There are not any particular onerous requirements or restrictions when hiring employees. In case of headhunting employees, especially with key employees, non-compete provisions may prohibit an employee from entering or starting a similar profession or trade in competition with the original employer. Such restrictive covenants could be altered or invalidated by courts if the relevant period is too long or if the covenant is too restrictive.

5.2 What, if any, mandatory employment benefits must be provided to staff?

The most important significant employment benefits that must be provided to employees in Iceland are the rights afforded to employees through the aforementioned collective bargaining agreements. The collective bargaining agreements are governed by the Act on Trade Unions and Labor Disputes, which permits unions to collectively negotiate employment terms, wages, etc. on behalf of their union members, as mentioned above. Such collective agreements are automatically binding for all workers and employers operating within an occupational and geographical area, as stated in the Act on Employee Benefits and Compulsory Pension. The legislation applies to both domestic and foreign entities operating in the Icelandic labour market and is binding upon all workers and employers within the applicable agreement. The benefits include minimum wages, maximum working time, minimum pension fund contributions, holiday and holiday allowance, sickness and accidents leave, gender equality, maternity and paternity rights, etc.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

In general, with Iceland being a party to the EEA, citizens of the EEA are authorised to be employed in Iceland without a specific work permit or a visa. These employees would, however, need residence permits from the Icelandic Directorate of Immigration within the first three months of the working period. Citizens from outside the EEA are required to have both work and residence permits.

Furthermore, it is worth mentioning that the Posted Workers Act applies to companies established in another EEA Member State, another EFTA State or the Faroe Islands, which intend to post workers to Iceland, providing services on a temporary basis. During the time these workers are working in Iceland, Icelandic law applies to their terms of service, including the aforementioned collective bargaining agreements containing minimum wages and other employment-related rights.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Innovations and inventions may be protected by the Icelandic IP legislation; for example, through the means of patenting according to the patent legislation. Patenting protects the technical realisation of an idea, such as equipment and products, as well as methods or applications. A basic requirement for granting a patent for an invention is that it is new, inventive and capable of industrial application. IP rights (such as a computer code not eligible for a patent) may be protected through copyright. Generally, applications are submitted to the Icelandic Patent Office in order to receive the relevant protection.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Once the relevant IP right has been obtained, the owner may utilise those rights and prohibit others from doing so. The duration of registered IP rights differs on the relevant rights. For example, general copyright lasts for 70 years, patents for 20 years and trademarks for 10 years.

If such rights are infringed, the owner of the IP rights can initiate court proceedings in order to receive damages and injunctive relief. Applications for design, patent and trademark rights are submitted to the Icelandic Patent Office as mentioned before. Specific rules apply to employees' inventions, *cf.* Act on Employees' Inventions where a distinction is made on whether the invention is indeed related to the employee's employment.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

Yes, other rights can be enforced as Iceland is a member of numerous treaties and conventions, such as the European Patent Convention, which Iceland became a party to on 1 November 2004, as well as the Paris Convention for the Protection of Industrial Property (WIPO), which took effect in Iceland on 5 May 1962. According to the Paris Convention, if an application for a patent has been filed within a country which is party to the Convention, the applicant may, within a year from the date of application, file an application relating to the same matter in another country, including Iceland, and claim right of priority with reference to the original application. Additionally, Iceland has been a party to the Patent Cooperation Treaty since 1995 and several WIPO-administered treaties, IP-related Multilateral Treaties, and IP regional treaties as well as relevant derived EU legislation. Regarding trademarks, it is also possible to apply for an international registration at WIPO or apply for a European Union Trade Mark. The same applies to patents insofar it is possible to apply for protection at WIPO or according to the European Patent Convention. To sum it up, Iceland's regulatory framework concerning IP rights is in many ways correlative to other states within the EEA.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

IP rights may generally be sold or licensed through specific licensing agreements. Such agreements can contain limitations to the extent of the sale or licensing. Trademarks and patents can also be pledged as security and registered as such at the Icelandic Patent Office and the District Commissioner. However, it is worth noting the difference between moral rights and economic rights contained in copyrights, with only the latter being transferable.

Acknowledgment

The authors would like to thank Sigvaldi Fannar Jónsson for his invaluable assistance in the writing of this chapter. Sigvaldi joined BBA in 2016 as a trainee, and after his graduation from the University of Iceland in 2017 he became a full-time member of the team. Sigvaldi took courses at Columbia University as part of his Master's degree in law. Sigvaldi's primary practice areas are in Commercial and Company law. Sigvaldi has participated in various cross-border and domestic M&A deals, through his time at BBA and other law firms and has extensive teaching experience for the University of Iceland and other institutions.

Tel: +354 550 0521 / +354 691 7901 / Email: sigvaldi@bba.is

**Stefán Reykjalin**

BBA
Höfðatorg, 19. hæð
105 Reykjavík
Iceland

Tel: +354 550 0522 / +354 862 3082
Email: stefan@bba.is
URL: www.bba.is

Stefán joined BBA in 2014. He became a member of the Icelandic Bar Association in 2011. Prior to joining BBA, Stefán was an in-house counsel at Landsbanki Íslands *hf.* where he principally worked in the field of corporate banking and corporate restructuring. At BBA, Stefán's practice areas are M&A as well as Capital Markets, Corporate and Commercial Law.

**Baldvin Björn Haraldsson**

BBA
Höfðatorg, 19. hæð
105 Reykjavík
Iceland

Tel: +354 550 0503 / +354 840 0400
Email: baldvin@bba.is
URL: www.bba.is

Baldvin is one of the two founding partners of BBA. He has been a member of the Icelandic Bar Association since 1994 and became a member of the Paris Bar in 1998 after having obtained a DESS and a Troisième Cycle degree in International Business Law from ILERI in Paris. Baldvin has actively advised clients throughout his career in M&A, Financing, Energy Law and PPPs, and has been involved in many of the largest M&A deals in Iceland in recent years. He advised the UK Deposit Guarantee Fund and HMT in their legal proceedings in Iceland relating to the Icesave deposits. He is admitted before the Supreme Court of Iceland and is the Chairman of the French-Icelandic Chamber of Commerce.

BBA

Founded in 1998, BBA was the first law firm in Iceland to build its practice exclusively on servicing the business sector. This focus has allowed our lawyers to gain substantial experience and a level of expertise which is second to none in Iceland in, among other areas, Corporate law, Finance law and General Business law. As a result of this, we have been trusted by our clients to provide advice in many of the largest and most complicated projects in the field of M&A, Corporate Finance, Project Finance, restructuring and PFI projects. In recent years, we have extended our practice and built up a substantial legal and practical know-how in the field of energy law, regarding renewable energy resources as well as oil and gas. BBA lawyers have from the founding of the firm advised on complex deals, the majority of which have an international aspect. As a result, we have emphasised that our team of lawyers is educated and experienced abroad, as well as having diverse backgrounds, which aids in providing our clients with a multi-angle approach to solving legal problems. Our lawyers have work experience stemming from local and foreign banks, listed companies, the competition authority, tax authorities and accounting firms, as well as education and practical experience from countries such as Denmark, England, France, Germany, Italy, Luxembourg, and the United States. BBA lawyers are admitted before the courts of Iceland, Paris and New York.

India

Kosturi Ghosh



Adhunika Premkumar



Trilegal

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

The fintech sector has generally adopted a careful approach towards innovation in India given the uncertainty in the regulatory space and the conventional approach taken by the Government towards such businesses. However, an increase in the access to technology and financial awareness has seen the Government making strong efforts to promote digitalisation, innovation and development in the fintech sector. Recently, the Government constituted a Joint Working Group on Fintech with Singapore for increasing cooperation in the area of fintech between the two countries, and excelling in the fields of development of Application Programming Interfaces (APIs), regulatory sandboxes, security in payment and digital cash flow, integration of RuPay-Network for Electronic Transfers (NETS), the UPI-FAST payment link, the AADHAAR Stack and e-KYC in the ASEAN region.

While blockchain technology and cryptocurrency continue to gain momentum, the Indian market has also seen an increase in: (i) payment companies morphing into financial services entities and entering the wealth management sector; and (ii) e-commerce entities entering the lending sector by itself or through collaborations with banks and non-banking financial institutions. Businesses have also explored the usage of technology for deploying algorithms that help a user ascertain the trade trends on the stock market. Reports indicate that the Indian fintech market will touch USD 2.4 billion by 2020.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

Currently, there are no express prohibitions on fintech businesses. The Government is looking to regulate virtual currencies, especially in relation to issues such as consumer protection and money laundering. For instance, the committee on financial and regulatory technology, formed by the Securities and Exchange Board of India (SEBI), concluded that it may be crucial to regulate bitcoin transactions to ensure that public interest is not breached. However, the Royal Bank of India (RBI) has issued several statements warning customers about

financial and regulatory risks associated with virtual currencies. In April 2018, the RBI in its policy statement stipulated that regulated entities (including banks and non-banking financial companies) must not deal with or provide any services to any individual or business entities dealing with or settling virtual currencies, and has confirmed that formal guidelines will be issued in this regard.

Not all market entrants may be able to participate in certain types of fintech businesses. One such example is the issuance of open pre-paid instruments (PPIs). Open PPI is a payment instrument which can be used for purchasing goods and services, and to withdraw cash at ATMs. Only banks which meet the eligibility criteria are permitted to issue open PPIs. Similarly, only certain market participants such as non-banking financial companies, mobile telephone companies, supermarket chains and companies that are owned and controlled by residents can make an application to set up payment banks in India.

The RBI has also issued regulations to regulate peer-to-peer lending in India. In accordance with the regulations, no non-banking institution other than a company, having a net-owned fund of not less than approximately USD 300,000, can undertake the business of peer-to-peer lending in India.

In September 2018, the Supreme Court read down certain provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 that impacted the use of Aadhaar (a unique identification number) authentication by private parties under a contract. While this decision affected the growth rate of Indian fintech start-ups by making the process of onboarding customers cumbersome, fintech companies were quick to introduce new KYC techniques (i.e., the process of verifying the identity and address of users) to capitalise on the growing consumer traction. The Government recently promulgated an ordinance and introduced amendments to the Prevention of Money Laundering Act, 2002 to allow Aadhaar holders to voluntarily disclose their Aadhaar to private entities for offline verification. This move is likely to bring some relief to fintech companies while verifying the identity of their users.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

New and growing businesses may fund their activities in different ways, including the following:

- (a) By issuing securities, such as equity shares, preference shares, debentures, etc. Given the current business landscape, venture capital, private equity and venture debt

are the preferred equity and debt funding options. Angel investors, incubators and accelerators have shown significant interest in funding start-ups. Start-ups recognised under the 'Start-up India' initiative of the Government are also eligible to issue convertible notes for raising funds.

- (b) By raising debt from banks and other financial institutions. Businesses also have the option of availing external commercial borrowing from eligible non-resident lenders.
- (c) By making public offerings and raising funds from the market. This is, however, dependent on the entity's economic scale and stage of development.
- (d) Through crowdfunding. This is, however, still an unconventional method of raising funds.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

The Government launched the 'Start-up India' initiative to develop an ecosystem conducive for the growth of start-ups and to provide assistance in funding. The Department of Industrial Promotion and Policy has recognised around 16,000 companies as start-ups, and about 129 start-ups have received assistance with respect to funding (February 2019). The Government has launched various tax relief schemes, which include three years of income tax exemption for recognised start-ups. The Government has been actively trying to make the process of registering companies in India easier to help businesses start their operations. In addition, the Government has launched the Digital India and Smart Cities initiatives to increase foreign investment, and to create and develop digital infrastructure in India.

Recently, the Government expanded the ambit of the definition of 'start-up' to extend the applicability of the scheme to more entities, and also eased tax norms by amending the provisions dealing with angel tax (i.e., income tax payable on amounts raised by the start-up in excess of its fair market value) with a view to drawing a clear distinction between genuine start-ups and shell companies engaging in money laundering. This move of the Government is likely to create a conducive environment for start-ups and bolster innovation.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

The SEBI, the Indian capital markets regulator, has, in addition to the general rules for capital raises, also prescribed regulations for the issue of specified securities by small and medium enterprises (SMEs) under Chapter XB of the Securities Exchange Board of India (Issue of Capital and Disclosure Requirements) Regulations, 2009 (ICDR Regulations). These regulations are applicable to an issuer whose post-issue face value capital does not exceed approximately USD 1.4 million, or whose post-issue face value capital is more than approximately USD 1.4 million and up to approximately USD 3.5 million.

As SMEs and start-ups play an important role in generating employment and income, the need for setting up an environment to enable them to raise funds from the public to fund innovation drove the SEBI to create an architecture separate from the main market. Through the ICDR Regulations, SMEs can now raise capital through the SME exchanges, thereby giving them better visibility and wider reach. The minimum application size in an SME IPO is fixed at approximately USD 1,500 per application. Further, the number of allottees in an SME IPO should be at least 50.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

2018 witnessed several notable exits for founders operating fintech businesses, including: (i) the Future Group acquiring a 55% stake in LivQuik Technology (India) Private Limited for approximately USD 7 million, with an intention of entering the payment gateway market; and (ii) Deutsche Bank acquiring Quantiguous Solutions (a four-year-old fintech start-up) to accelerate the bank's open banking strategy. Amazon.com Inc. also announced an increase in its investment in India from USD 5 billion to USD 7 billion, with a focus on capitalising on the Indian fintech market. The fintech sector continues to be a big bet for venture capital investors and has seen an investment of more than USD 4 billion in the last two years.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

Several regulations and regulators operate in this space, like the RBI, the SEBI for intermediaries in the securities market, the Insurance Regulatory and Development Authority (IRDA) for insurance-related businesses and the Telecom Regulatory Authority of India (TRAI) for telecom-related activities. The SEBI regulations such as the SEBI (Investment Advisors) Regulations, 2013 regulate investment advisors, the SEBI (Stock-Brokers and Sub-Brokers) Regulations, 1992 regulate stock brokers and the SEBI (Merchant Bankers) Regulations, 1992 regulate merchant bankers. The IRDA regulates, *inter alia*, web aggregators and insurance agents.

The regulation, and consequently, the regulator depends on the type of fintech business, and some fintech businesses may find themselves in an overlapping jurisdiction of different regulators. The payment space is one of the most regulated sectors in India. This sector is regulated by the RBI under the Payment and Settlement Systems Act, 2007 and the Payment and Settlement System Regulations, 2008. Payment systems, *inter alia*, include ATM networks, card payment networks and pre-paid instruments (wallets).

The RBI has also issued directions on Non-Banking Financial Companies – Peer-to-Peer Lending (P2P Master Directions) on 4 October 2017 which require the registration of a peer-to-peer lending platform with the Reserve Bank of India (NBFC P2P). The role of the NBFC P2P is to act as an intermediary providing an online market or platform to the participants involved in peer-to-peer lending. The NBFC P2P can also assist in the disbursement and repayment of loans availed on the NBFC P2P. However, the NBFC P2P is not permitted to lend on its own, to permit international flow of funds or facilitate or permit secured lending on the platform.

Recently, the Reserve Bank of India, recognising the emerging need for a dedicated, cost-free and expeditious grievance redressal mechanism for strengthening consumer confidence in digital payments, launched an Ombudsman Scheme for Digital Transactions (OSDT) for the redressal of complaints regarding digital transactions.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

Currently, there are no specific regulations directed at cryptocurrencies. As mentioned above, the Government is looking to regulate virtual currencies, especially in relation to issues such as consumer protection and money laundering. While the RBI in its policy statement has stipulated that regulated entities (including banks and non-banking financial companies) must not deal with or provide any services to any individual or business entities dealing with or settling virtual currencies, formal guidelines on the same are yet to be issued. The Finance Minister in the Union Budget speech of 2018–19 had said that the Government does not consider cryptocurrencies as legal tender. However, no formal ban has yet been placed on cryptocurrencies.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

The regulators are very conscious about any change in the financial services sector. Recognising the need for innovation and technology, especially concerning cyber security and money laundering, the regulators have been very perceptive to change and are working towards creating a fintech ecosystem which is beneficial to both the market participants and the customers. The regulators are proactively trying to engage with fintech businesses in order to improve the regulatory sphere. For instance, peer-to-peer lending platforms attracted the attention of the RBI given the potential benefits to the various stakeholders and the associated risks to the financial system. After various discussions with industry participants and the Government, the RBI released the P2P Master Directions on 4 October 2017.

The RBI set up an inter-regulatory working group in 2016 to study the entire gamut of regulatory issues relating to fintech and digital banking in India. The working group issued a report in February 2018 which recommended introducing a regulatory sandbox to encourage fintech innovation and a standalone data protection and privacy law in India. The Government has also released a report of the working group for setting up a computer emergency response team in the financial sector to tackle issues concerning cyber security.

Further, the Government has also undertaken a few initiatives to provide a strong infrastructure for fintech companies in India. The Pradhan Mantri Jan-Dhan Yojana scheme was launched in 2014 to enable financial inclusion and to ensure access to financial services in an affordable manner. The RBI has also introduced the Bharat Bill Payment System to enhance payment infrastructure in India and to provide easy payment options to customers without involving the physical movement of cash. Further, the Government has proposed the use of blockchain technology to encourage digital payments in the financial budget. The National Payments Corporation of India has also taken efforts to implement a Unified Payments Interface which is a single mobile application for accessing multiple bank accounts and merges several banking features to enable payments.

Recently, the Insurance Regulatory and Development Authority set up a committee on 'Regulatory Sandbox in the Insurance Sector in India' with an intent to encourage InsurTech innovations that help increase insurance penetration as well as seek to benefit policyholders at large. The committee recently released its final report and the draft guidelines for facilitating innovation in insurance through the regulatory sandbox.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

Most of the regulations require the entity to obtain a licence, approval, and authorisation from the applicable regulatory authority before commencing operations in India. The sometimes strenuous thresholds to cross to be eligible to apply, along with the time required to obtain such approvals, may deter certain fintech businesses from operating in India. In addition, some regulations require foreign entities to open an office in India and adhere to minimum capitalisation norms.

Since this sector is undergoing regulatory changes rapidly, it is important to keep an eye on business models and evolve with regulation.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

In India, the Information Technology (Reasonable Security Practises and Procedures and Sensitive Personal Data or Information) Rules, 2011 (**Privacy Rules**) regulate the manner in which personal data needs to be stored, processed, transferred and secured. The Privacy Rules are applicable to body corporates and any other person who, on behalf of a body corporate, collects, receives, possesses, stores, deals or handles any 'personal information' or 'sensitive personal data or information'. 'Personal information' is defined under the Privacy Rules to mean any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely available with a body corporate, is capable of identifying such person. On the other hand, 'sensitive personal data or information' as defined under the Privacy Rules includes, among other things, an individual's physical, physiological and mental health condition, sexual orientation, financial information and medical records and history.

With the significant boost in digital transactions, the Government also felt the need to specifically regulate the manner in which payment system providers and PPI issuers handle data collected by them. Accordingly, the Reserve Bank of India issued directions requiring: (i) PPI issuers to install adequate information and data security infrastructure and systems for ensuring consumer protection and preventing and detecting fraud; and (ii) payment system providers to ensure that they, along with their service providers, intermediaries, vendors and all other entities in the payment ecosystem, store data relating to payment systems only in India to enable unfettered supervisory access and monitoring of payments data operating in India. The Ministry of Electronics and Information Technology also issued draft Information Technology (Security of Prepaid Payment Instruments) Rules, 2017, for public comments, with a view to enhance consumer confidence in digital transactions and achieve a cashless economy.

Additionally, the Government has: (a) formulated a draft personal data protection bill that seeks to introduce a data protection regime

that can strike the appropriate balance between protecting the interests of individuals and the legitimate use of data by the state and private businesses; (b) sought to amend the guidelines applicable to intermediaries (i.e., online market places, online payment sites, etc.) (**Intermediary Guidelines**) to ensure better accountability from intermediaries; and (c) released the draft e-commerce policy, which, *inter alia*, lays down conditions for cross-border data flow, collection and storage of sensitive data.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

The Privacy Rules are applicable to any person located within India. Therefore, non-resident corporate entities that collect information from persons located in India will be liable to comply with the Privacy Rules even though they are located outside India. The Privacy Rules do not prevent international transfers of data to an entity in India or outside India. Personal information and sensitive personal data and information can be transferred subject to the conditions stipulated in the Privacy Rules. One such condition for transfer is that the entity to which the information is being transferred should adhere to the same level of data protection prescribed under the Privacy Rules.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

The Information Technology Act, 2000 (**IT Act**) does not stipulate the maximum compensation or penalty that is payable for breach of the Privacy Rules. However, the IT Act states that a body corporate that causes any wrongful loss or gain to any person, resulting from a failure to implement the required practices and procedures under the Privacy Rules, will have to pay damages by way of compensation to the person so affected. Further, disclosure of information, knowingly and with an intent to cause wrongful gain or loss to any person, without the consent of the person concerned and in breach of the lawful contract, has also been made punishable with imprisonment for a term extending to three years or with a fine extending to approximately USD 8,000, or both. In addition, there is a residuary penalty provision under the IT Act, which is applicable to contraventions for which no penalty has been separately provided. Under that section, the maximum compensation payable or penalty amount is approximately USD 400.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

The IT Act legislates offences relating to the use of or concerned with the abuse of computers or other electronic gadgets and is applicable to fintech businesses operating in India. Some of the offences under the IT Act include (a) computer-related offences, (b) sending offensive material through communication services, (c) violation of privacy, (d) cyber terrorism, and (e) identity theft. Further, the IT Act also empowers police officers to investigate offences under the IT Act. The Indian Penal Code, 1860, also prescribes punishment for cyber-crimes such as cyber-fraud, e-mail spoofing, web jacking and e-mail abuse. The Indian Computer Emergency Response Team (**CERT-In**) is the national agency responsible for responding to cyber security incidents. CERT-In currently operates (i) as the referral agency for Indian users to respond to cyber security incidents, and (ii) to assist in implementing measures to reduce the risk of cyber security incidents.

The IT Act also prescribes regulations that intermediaries need to follow if they do not want to be held liable for any third-party information, data, or communication links made available or hosted by it. These regulations require intermediaries to, *inter alia*: (i) observe due diligence while discharging their duties; (ii) inform their users to not display, upload or publish content on their platform which is misleading, harmful to minors, infringes any proprietary rights, etc.; and (iii) disable content that violates the regulations within 36 hours of receiving information of the violation in writing (including electronic communication).

Further, the draft Information Technology (Security of Prepaid Payment Instruments) Rules, 2017, requires every electronic PPI issuer to establish a mechanism to monitor, handle and follow up cyber security incidents and cyber security breaches. Certain cyber breaches may also have to be reported to CERT-In and to the customer.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

The Prevention of Money Laundering Act, 2002 (**PMLA**) prohibits and penalises money-laundering activities. In accordance with the PMLA, a 'Reporting Entity' is required to, *inter alia*, maintain records of clients and transactions, and furnish information to the authorities. A 'Reporting Entity' includes a banking company, financial institution and intermediaries such as investment advisors and merchant bankers. If a fintech company qualifies as a 'Reporting Entity' under the PMLA, it will need to comply with all obligations imposed on such entities. Additionally, as mentioned above, the fintech businesses will also need to comply with the know your customer requirements and develop adequate information and data security infrastructure to prevent and detect fraud, if the regulations introduced by the Reserve Bank of India are applicable to them.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

In addition to the regulatory regimes discussed earlier, the entities should also ensure compliance with the (Indian) Companies Act, 2013, the applicable tax and exchange control regulations whilst operating in India. Indian exchange control regulations govern all transactions between persons resident in India and persons resident outside India, including in relation to subscription and transfer of securities.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

Indian employment laws are generally employee-friendly. The employer and the employee are free to negotiate the terms of employment. In the event that a contract is less beneficial than an applicable statute, the statute would normally override the contractual provisions. The applicability of most employment statutes will vary depending on several factors, which include the number of employees in an establishment, the nature of the activity carried out by the organisation, the place of the establishment, the

type of workforce engaged by the establishment, and the wages earned by the employee. As many pieces of labour legislation cater to the concept of a ‘workman’, it is important to ascertain if an employee falls under the definition of a workman, as this plays a vital role for a variety of reasons; these include determining the terms and conditions of employment, termination compensation, formulating employment policies, etc. The Industrial Disputes Act, 1947 defines a ‘workman’ as any person employed in any industry to do any manual, unskilled, skilled, technical, operational, clerical or supervisory work for hire or reward, whether the terms of employment be express or implied, but does not include, *inter alia*, any such person in a managerial or supervisory capacity. Further, several pieces of labour legislation require employers to obtain various licences to operate, e.g. every commercial establishment is required to obtain a licence from the state-specific shops and establishments acts.

As regards termination, an employer is required to: (i) provide statutory minimum notice periods on termination of employment; and (ii) pay statutory severance payments such as gratuity and retrenchment compensation (if applicable). Courts in India do not normally recognise the concept of ‘at will’ termination of employment and require termination to be for a ‘reasonable cause’. Some pieces of state legislation expressly require an employer to provide a ‘reasonable cause’ for termination of employment. Therefore, termination of employment without reasonable cause is likely to be struck down by a court if challenged. Employment can be terminated (a) at the instance of the employer, (b) at the instance of the employee (resignation), (c) by mutual agreement, (d) employee’s retirement/superannuation, and (e) at the expiry of the term of the employment contract.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Indian social security legislation primarily addresses contingencies that may arise due to stoppage or reduction on earnings, maternity, employment injury, occupational diseases and death. The social security legislation covers both contributory and non-contributory payments. Contributory laws require social security programmes to be financed by both employees and employers and include employee state insurance and employee provident funds. Non-contributory labour statutes provide for compensation from the employer in the event of injury, disease or death of the employee during the course of the employment. Non-contributory payments include gratuity, which is a long service payment payable at the time of termination of employment to employees who have completed five years of continuous service. It is paid earlier in case of the death or disablement of an employee. Labour statutes in India also cover leave and holidays. Certain establishments must also comply with the maternity benefit laws which, *inter alia*, prescribe conditions regarding maternity leave and impose restrictions on employment.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

Foreign employees can be employed in India, either under a direct employment agreement with the Indian entity or through a secondment arrangement. In case of a secondment of employees, the foreign entity, the Indian entity and the employee would normally enter into a secondment agreement which would govern

the terms of secondment. In many cases, an employment contract between the employee and the entity in the host country is also entered into to ensure compliance with immigration laws and mitigate tax risks. The other major issue in relation to secondment agreement is compliance with immigration and tax laws. The foreign nationals should have a valid employment visa to be able to work in India. Further, if the foreign national works in an establishment to which the Employees Provident Fund and Miscellaneous Provisions Act, 1952 (**EPF Act**) applies, he would qualify as an ‘International Worker’ under the EPF Act, and the employer and the employee must make the prescribed provident fund contributions.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

The Patents Act, 1970 (**Patents Act**) protects an invention if it (i) is a new product or a new process, (ii) involves an inventive step, and (iii) is capable of industrial application. Additionally, certain inventions are not patentable and these include, among others (i) scientific principle or formulation, (ii) discovery of a new form of known substance, (iii) mathematical or business method, computer program or algorithm, (iv) performing a mental act or method of playing a game, (v) presentation of information, and (vi) topography of integrated circuits. Patent protection in the form of a monopoly is provided for a period of 20 years from the date of filing the patent application. The Controller of Patents heads the Patent Office and reviews and grants patents in India. Computer programs are protected as a ‘literary work’ under the Copyright Act, 1957 (**Copyright Act**) as they are not patentable.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

The legislative framework in India protects trademarks, patents, copyrights, designs and layout designs. While patents need to be registered under the Patents Act, copyrights do not require mandatory registration as the statutory law extends automatic protection to original works of authorship. Under the Berne Convention for Protection of Literary and Artistic Works (**Berne Convention**) and the Universal Copyright Convention, any work first published in a Member State is granted the same protection as if it were first published in India, to the extent the Member State provides reciprocal treatment to Indian works.

Common law protection is given to unregistered trademarks and designs. There is no statutory code in India for the protection of confidential information. Therefore, an action for breach of contract is commonly used to protect confidential information. In addition, protection can be sought by instituting a claim for breach of trust.

The Government also provides assistance to start-ups in obtaining IP registrations by, *inter alia*, providing a rebate on filing fees and expediting the applications.

The following protections are offered by each type of IP right: (a) trademarks protect brand names, logos, sounds, colours and 3D shapes; (b) patents protect patentable inventions; (c) copyright protects original literary, dramatic, musical works, computer programs, artistic works, cinematographic films, sound recordings; (d) designs protect the shape, configuration, pattern, and appearance of products; and (e) layout designs protect the layout design of semiconductor integrated circuits.

India is also a signatory to the following treaties and conventions concerning IP: (a) Berne Convention; (b) Patent Co-operation Treaty; (c) Universal Copyright Convention; (d) Paris Convention for the Protection of Industrial Property; and (e) Madrid Protocol for International Registration of Marks.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

India is a signatory to various treaties which facilitate filing international applications to seek protection in India for IP created in or by persons residing in Member States. India is working with the World Intellectual Property Organization (WIPO) to develop an effective and balanced IP enforcement system. India is compliant with the global standards on the protection and enforcement of IP rights as set out in the Agreement on Trade Related Aspects of Intellectual Property Rights.

For registered IP, claims can be initiated in the courts as provided in the applicable IP statute in India. In addition to the courts, IP tribunals have been set up to hear cases for the rectification and cancellation of registered IP.

Unregistered trademarks, get-up, names, images and trade dress are protected under common law. A claim for passing-off can be initiated in the courts for the protection of unregistered trademarks and designs. The courts have recognised trans-border reputation in passing off actions concerning trademarks.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

IP rights can be assigned or licensed to third parties. A licence and assignment of IP establishes the terms on which a third party may exercise the exclusive rights granted to an IP owner by a statute or by common law, without infringing the IP holder's rights. A licence can be used to generate a royalty-based income stream. An assignment can be made by the IP holder to those entities who maximise the value of the IP.

An agreement to license or assign generally depends on the commercial understanding between the parties. Adequate stamp duty will need to be paid on such agreements to ensure that it is admissible as evidence in a court of law. However, there are certain legal requirements to be met for a transfer to be a valid transfer. An assignment of a registered trademark needs to be filed with the Trade Marks Registry for it to be recognised as a valid assignment. The assignment or licensing of any interest in patents must be in writing and contain all the terms regarding the rights and obligations of the parties. This assignment or licence agreement must be registered with the patent office. Any unregistered assignment or licence agreement cannot be used as evidence of transfer of title. The Government may also grant compulsory licences under various situations which include national emergencies. The Copyright Act also stipulates certain conditions for assignment and licensing including, *inter alia*, the assignment or licence should be in writing, the consideration amount must be specified and, if the period of assignment is not stated, the assignment is valid for a period of five years. The cross-border assignment or licensing of IP is regulated under the foreign exchange regulations which may have implications on the arrangement.



Kosturi Ghosh

Trilegal
The Residency, 7th Floor
133/1, Residency Road
Bengaluru, Karnataka 560025
India

Tel: +91 80 4343 4603
Email: Kosturi.Ghosh@trilegal.com
URL: www.trilegal.com

Kosturi Ghosh is a Partner and the Deputy Head of the Corporate Practice group at Trilegal. Her primary areas of practice are general corporate advisory, M&A and Private Equity, and TMT.

She has a wealth of experience from advising on complex TMT matters including IP protection, software development, licensing and monetisation of IP, data protection, technology transfer, etc. In the fintech space, she has advised on products ranging from mobile wallets to closed and semi-closed payment systems. She also has advised on issues relating to cross-border payment systems and companies looking to deploy smartcard-based payment systems.

Recognised as a leading individual, she was given high praise for being "an intelligent, business-minded lawyer with exceptional negotiation skills and on-point experience" – *RSG India* 2015. She has recently won the special jury award – Women in Legal Leadership – at IDEX Legal Awards 2016 and was also featured in "40 Under 40" in Asia Pacific by *Asian Legal Business*. She has also been ranked as a leading lawyer in *Chambers & Partners* 2016.



Adhunika Premkumar

Trilegal
The Residency, 7th Floor
133/1, Residency Road
Bengaluru, Karnataka 560025
India

Tel: +91 80 4343 4612
Email: Adhunika.Premkumar@trilegal.com
URL: www.trilegal.com

Adhunika Premkumar is a Senior Associate with the corporate practice group at Trilegal. She focuses on acquisitions, joint ventures, private equity/venture capital transactions and other corporate and commercial matters. She has been involved in advising companies on structuring investments in India, conducting due diligence, drafting and reviewing transaction documents and advising private and public listed companies on general corporate matters.

TRILEGAL

Trilegal is one of India's top-tier law firms with offices in Mumbai, New Delhi, Gurgaon and Bangalore. We represent clients on a large number of the most complex and high-value transactions in India, leading our key practices to win top industry awards and accolades.

Trilegal has strong working relationships with various reputed law firms in jurisdictions across the world. As a result of our deep-rooted international network, Trilegal has executed various transactions for clients from different geographies, navigating complex Indian regulations and structuring innovative solutions appropriate to the clients' requirements.

Trilegal has worked extensively in the fintech space for over a decade, helping various international companies navigate the Indian financial regulations as they look to deploy fintech products in the country. In the recent past, we have been able to use that experience in developing solutions for e-commerce and app-based services companies.

The firm and its lawyers have been consistently ranked and recognised by leading legal publications across each of our practice areas. Our clients include many of the world's leading corporations, funds, banks and financial institutions.

Indonesia

Luky I. Walalangi



Walalangi & Partners
(in association with Nishimura & Asahi)

Hans Adiputra Kurniawan



1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

For the past two years, the Indonesian market has seen the rise of technology-based start-up companies that stimulate the rapid development of technology-based transactions (including technology-based “unicorn” companies such as Go-Jek, Tokopedia and Traveloka). The Indonesian Fintech Association indicates that there are 157 fintech start-up companies, as of 5 January 2019.

From a regulatory perspective, the Central Bank of Indonesia (*Bank Indonesia* or “BI”), through BI Regulation No. 19/12/PBI/2017 (“**BI Regulation 19/2017**”), recognises and classifies fintech activities into the following categories:

- Payment systems:** clearing; final settlement; and payment processing (e.g., blockchains or distributed ledgers technology for fund transfer, electronic money, electronic wallet and mobile payments). Notable companies include Go-Pay, OVO, Dana, and Midtrans.
- Market support:** facilitating the distribution of information related to financial products and/or services to the public (e.g., a data provider comparison of certain financial services/products).
- Investment management and risk management:** e.g., online investment products and online insurance.
- Lending, financing/funding and capital raising:** e.g., peer-to-peer lending (“**P2P**”), financing or crowdfunding. According to the Financial Services Authority (*Otoritas Jasa Keuangan* or “**OJK**”) website (the authority supervising P2P), as per December 2018, there are 88 P2P companies registered with OJK (among others, Investree, Modalku, Rupiah Plus, and Uang Teman), but only one P2P company with a definitive business licence (Danamas).
- Other financial services.**

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

Yes. In 2016 and 2018, BI issued BI Regulation No. 18/40/PBI/2016 on Payment Transaction Processing (“**BI Regulation 18/2016**”) and

BI Regulation No. 20/6/PBI/2018 on Electronic Money (“**BI Regulation 20/2018**”) strictly prohibiting the use of cryptocurrency as means of payment.

In addition, according to news articles, OJK shut down at least 19 cryptocurrency business practice operators in 2018.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

Other than equity, the typical funding alternatives are bank-loans, shareholders loans, corporate bonds, warrants or initial public offering (“**IPO**”).

The liquidity in the market allows start-up companies to receive private funding from big Venture Capital or Private Equity companies like Sequoia and Softbank Vision Fund. In 2018, DailySocialid reported the disclosed amount of fintech investment reached USD 182.3 million, most of it injected by Venture Capital or Private Equity companies. Recent rounds of funding include the USD 70 million led by Fanpujinke Group into Akulaku and USD 25 million led by Softbank Ventures Korea into Modalku in April 2018, which was claimed as the biggest series B funding ever received by a P2P platform in Southeast Asia.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

On 8 June 2018, the Indonesian government issued a new regulation, Government Regulation No. 23 of 2018 on Income Tax on Income from Business Received or Earned with Certain Gross Turnover (“**GR 23/2018**”), reducing the final tax rate of income tax for taxpayers (including certain SMEs) whose gross turnover does not exceed IDR 4.8 billion within one fiscal year from a 1.0% to 0.5% final tax rate for a certain period of time, depending on the type of legal entity of the taxpayer:

- Individual taxpayer: seven years.
- Cooperative (*koperasi*), *Comanditer Vennotschap* (“**CV**”), or firm (*firma*) taxpayer: four years.
- Limited liability company taxpayer: three years.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

Before an IPO, the company must first submit a registration statement (*pernyataan pendafitan*), together with its supporting documents (such as prospectus/information memorandum, audited financial statements, legal due diligence report and legal opinion from an independent legal consultant) to OJK. Once the registration statement is effective, the company must conduct certain public disclosure (among others, its group business conditions and risks) as a part of its public offering process.

After the IPO, the company is not automatically listed on the Indonesian Stock Exchange (“**IDX**”). To do so, the company must submit an application to and obtain a listing approval from the IDX.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

Considering the complex Indonesian capital market law requirements for an IPO, shareholders’ exits are mostly by way of M&A rather than IP; for example, the exit of Finch Capital and East Ventures from Cermati (a fintech company engaging in the market provisioning sector) through the acquisition by Djarum Group.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

Depending on their characteristics, fintech businesses are subject to the regulations of either BI or OJK. BI regulations cover payment system services while OJK regulations cover P2P lending, investment management, market aggregators, and crowdfunding.

A brief summary of the most highlighted matters is as follows:

- E-Money:** regulated under BI Regulation 20/2018, which classifies e-Money operators into two categories, namely (i) front-end, and (ii) back-end operators. Some of the key provisions are, among others: (a) paid-up capital requirements; (b) foreign shareholding limitation of maximum 49% for a non-bank issuer; and (c) restriction to become a controlling shareholder in more than one payment system operators.
- Payment Processing Operators:** regulated under BI Regulation 18/2016, which sets licensing requirements for payment processing operators and 20% maximum foreign shareholding.
- P2P Lending:** regulated under the OJK Regulation No. 77/POJK.01/2016 (“**OJKR 77/2016**”), which, among others, limits the foreign shareholding limitation to a maximum of 85%, prohibits the balance sheet lending model and sets a two-tier licensing mechanism.
- Digital Banking:** regulated under OJK Regulation No. 12/POJK.03/2018 (“**OJKR 12/2018**”), which sets requirements for conventional banks to provide digital banking services (including: (i) account administration; (ii) transaction authorisation; and (iii) finance management).
- Equity Crowdfunding:** regulated under OJK Regulation No. 37/POJK.04/2018 (“**OJKR 37/2018**”), which, among others, sets a minimum issued capital requirement of IDR 2.5 billion, limitation of business activities, crowdfunding amount, licensing and reporting requirement for equity crowdfunding platform operators.

- Regulatory Sandbox BI:** regulated under BI Regulation 19/2017, which requires fintech operators meeting the criteria under BI Regulation 19/2017 to be registered with BI.
- Regulatory Sandbox OJK:** regulated under OJK Regulation 13/POJK.02/2018 (“**OJKR 13/2018**”), which authorises OJK to require fintech operators to undergo the sandboxing under OJK’s supervision.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

BI Regulation 18/2016 and BI Regulation 20/2018 prohibits the use of cryptocurrency as means of payment.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

Yes. In 2016, BI launched a specific fintech office to focus on regulating and supervising the growing fintech industry followed by the issuance of BI Regulation 19/2017. BI Regulation 19/2017 provides regulatory sandboxing and testing mechanisms to ensure, among others, the fintech players’ risk and risk mitigation profile, reliability of business process, and technology proficiency.

The same approach was also adopted by OJK, where through OJKR 13/2018, the regulatory sandboxing and testing mechanisms were introduced.

Additionally, in several public seminars, the government openly supported the growth of fintech. In another example, on 20 August 2018, OJK launched OJK’s Innovation Centre for Digital Financial Technology, whose goal is to build a fintech ecosystem through the facilitation of a regulatory sandbox, innovation hub and an educational centre.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

Indonesian law requires a foreigner to conduct business in Indonesia through an Indonesian limited liability company (which can be done either by way of establishing a new company or acquiring an existing Indonesian limited liability company) and obtain business licences from either OJK or BI.

The foreign parties’ shares participation are also limited, depending on the contemplated businesses/industries, as follows:

- P2P Lending:** OJKR 77/2016 limits foreign shareholding in a P2P company up to 85%.
- Payment Processing Operators:** BI Regulation 18/2016 limits foreign shareholding in back-end operators (i.e. principals, switching operators, clearing operators, and final settlement operators) by up to 20%. Furthermore, BI Regulation 20/2018 prohibits a payment processing operator (bank and non-bank) to become a controlling shareholder (having more than 25% or less but having factual control) in (a) more than one non-bank payment processing operators engaging in the same business activities (e.g. controlling the shareholder in two switching operators (“**back-end operators**”)), and/or (b) in more than one non-bank payment processing operators under a different payment processing

operators group (e.g. controlling the shareholder in a switching operator and an e-wallet company (“**front-end operators**”)).

3. **E-Money:** BI Regulation 20/2018 limits foreign shareholding in an e-money issuer of up to 49%.

4 Other Regulatory Regimes / Non-Financial Regulation

- 4.1 Does your jurisdiction regulate the collection/use/ transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?**

Yes, collection/use/transmission of personal data is regulated under Law No. 11 of 2008 on Electronic Information and Transaction (as lastly amended in 2016) (“**EIT Law**”), as further implemented by Government Regulation No. 82 of 2012 on Electronic System and Transaction (“**GR 82/2012**”) and Minister of Communication and Informatics (“**MOCI**”) Regulation No. 20 of 2016 on Personal Data Protection in Electronic System (“**MOCI Regulation 20**”). These regulations apply to Electronic System Operators (“**ESOs**”), including fintech services operators.

- 4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?**

As a general rule, the Indonesian law system adopts a jurisdictional system, where the laws and regulations only apply in Indonesia and to organisations established in Indonesia, except for certain tax rules which may have extra-territorial affect.

Nonetheless, there have been news reports that the Indonesian government is currently preparing a bill on personal data protection, which will apply to foreign ESOs if their activities affect Indonesia’s interests.

Cross-border data transmission requires a prior written approval from the owners and reports to MOCI or other appointed authorities.

- 4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.**

MOCI Regulation 20 sets administrative sanctions in the form of either: (i) a verbal warning; (ii) a written warning; (iii) temporary suspension of activities; or (iv) online announcement of violation.

There are additional administrative sanctions under BI Regulation 18/2016 and/or OJKR 77/2016, including a revocation of licence.

- 4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?**

This is set under the EIT Law, which prohibits, among others: unauthorised access (hacking); unlawful interception towards private data; and data manipulation. The applicable sanctions include imprisonment and/or fines.

- 4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.**

AML under Law No. 8 of 2010 on the Prevention and Eradication of

Money Laundering (“**AML Law**”) requires financial services providers to implement certain know-your-customer (“**KYC**”) processes and report to the Financial Transaction Reports and Analysis Centre (“**PPATK**”) on any suspicious transaction and/or cross-border fund transfer transactions. This is further regulated under OJK Regulation No. 12/POJK.01/2017 (“**OJKR 12/2017**”) and BI Regulation No. 19/10/PBI/2017, which require the setting up of AML internal policy by the relevant financial services providers/operators.

- 4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?**

In addition to the regimes of MOCI/OJK/BI, fintech operators are also subject to general corporate laws, including the laws on limited liability companies, foreign investments and, as relevant, the capital markets.

5 Accessing Talent

- 5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?**

The basic rules of employment in Indonesian law is governed under Law No. 13 of 2003 on Employment (“**Employment Law**”).

The Employment Law requires an employment agreement to be made in writing in the Indonesian language, which can be divided into: (i) a definite term; and (ii) an indefinite term. In addition, it requires termination to be carried out only with a mutual consent (except under certain limited conditions). Under the Employment Law, termination will entail obligations such as payment of reward for service, severance, or compensation by the company for the terminated employee.

- 5.2 What, if any, mandatory employment benefits must be provided to staff?**

- (a) Allowance, comprising of fixed allowance, unfixed allowance, and religious holiday allowance.
- (b) Health Social Security and Manpower Social Security.
- (c) Overtime-Pay (as applicable).
- (d) At least 12 days of annual leave for employees who have worked for at least 12 consecutive months, as well as other certain special leave.

- 5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?**

To hire expatriates, the employers must firstly obtain: (a) Foreign Workers Recruitment Plans (“**RPTKA**”) containing reasons for hiring the expatriate, positions which will be filled by the expatriate, employment period, and the appointment of a local employee to assist know-how transfer from the expatriate; and (b) Notification (*Notifikasi*). There is no specific regulation to employ expatriates in fintech businesses, but note that OJK and BI have the discretionary power to require additional documents that they deem necessary.

It is to be noted that expatriates are prohibited from performing as a person in charge of human resources affairs.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Innovations and inventions are protected in Indonesia through IP rights and laws and regulations, which are divided into: (i) copyrights; (ii) trademarks; (iii) patents; (iv) trade secrets; (v) industrial designs; and (vi) integrated circuit layouts.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

For copyright, Indonesian law adopts the concept of “first to declare”, where registration is not mandatory, and the protection automatically exists when the creator declares its invention.

In contrast, for other IP rights, including trademarks, patents, industrial designs and integrated circuit layouts, Indonesian law adopts the *first to register* concept.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

The Indonesian government has ratified certain international treaties/conventions which in turn require the government to

acknowledge and protect certain IP rights registered overseas/in countries which have also ratified the same international treaties/conventions. For example, Indonesia has ratified the Berne Convention for the Protection of Artistic and Literary Works, as implemented in Article 2(c) of Law No. 28 of 2014 on Copyrights and has ratified the Paris Convention for the Protection of Industrial Property with respect to other IP rights (i.e. patents, trademarks and industrial designs), which were implemented through Law No. 31 of 2000 on Industrial Design, Law No. 20 of 2016 on Mark and Geographic Indication, and Law No. 13 of 2016 on Patents.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

In the context of monetising IP, Indonesian law provides the concept of licensing, which allows the IP rights holder to assign its rights and receive compensation in return.

Acknowledgment

The authors would like to thank Sinta Dwi Cestakarani for her invaluable assistance in the writing of this chapter. Ms. Sinta Dwi Cestakarani is a licensed lawyer with more than seven years of experience in assisting domestic and international clients. Her main areas of practice are banking and finance, M&A, multi-finance companies, mining and fintech. During her years of practice, Ms. Sinta Dwi Cestakarani assisted and advised domestic and foreign companies in various notable transactions predominantly in the areas of banking and finance, mergers and acquisitions, mining and fintech.

Tel: +62 21 5080 8600 / Email: Scestakarani@wplaws.com

**Luky I. Walalangi**

Walalangi & Partners
Pacific Century Place, 19th Floor
Jl. Jenderal Sudirman Kav. 52-53
Jakarta 12190
Indonesia

Tel: +62 21 5080 8600
Email: Lwalalangi@wplaws.com
URL: www.wplaws.com

Mr. Luky Walalangi is an Indonesian qualified lawyer, an expert and a leading lawyer in M&A, Banking and Finance and Real Estate transactions with more than 17 years of experience.

Mr. Luky Walalangi has been assisting various foreign companies in their complex investments and acquisitions and portfolio loans acquisitions, real property projects and corporate restructurings in Indonesia. He has also represented leading global banking and financial groups on major finance transactions, bond issuance, sophisticated fundraising projects as well as a number of major electricity projects in Indonesia.

Chambers Asia Pacific regards Mr. Luky Walalangi as a leading individual in Corporate/M&A, by *IFLR1000* as a leading lawyer and by *Asialaw Profiles* as one of the five Best Lawyers in Indonesia. *Asia Business Law Journal* lists him as part of the A-List Indonesia's Top 100 Lawyers.

**Hans Adiputra Kurniawan**

Walalangi & Partners
Pacific Century Place, 19th Floor
Jl. Jenderal Sudirman Kav. 52-53
Jakarta 12190
Indonesia

Tel: +62 21 5080 8600
Email: Hadiputra@wplaws.com
URL: www.wplaws.com

Mr. Hans Adiputra Kurniawan is a bright and talented Indonesian lawyer, with more than seven years of experience in banking and finance, FDI and M&A. In the areas of banking and finance, he has been involved in major syndication loans (including debt restructuring and power projects), bond issuances as well as general advisory. He has also been part of a team representing leading global banking and financial groups on major finance transactions, sophisticated fundraising projects as well as number of major electricity projects in Indonesia.

**Walalangi & Partners (in association with Nishimura & Asahi)**

Walalangi & Partners ("W&P") was founded by Mr. Luky I. Walalangi, a highly regarded lawyer with nearly two decades of experience. W&P is a corporate firm focusing on M&A, Banking & Finance, Real Property, FDI, Antitrust, Debt & Corporate Restructuring, Capital Markets, Employment, General Corporate and TMT.

W&P is regarded by *IFLR1000* as a recommended Firm, by *Asialaw Profiles* 2019 as a recommended Firm in Real Estate, TMT, Banking & Finance and Corporate M&A. In ALB 5th Annual ILA 2018, W&P is a finalist of Rising Law Firm and shortlisted in Banking, Real Estate & Construction Law Firm of the year.

Ireland

Claire Morrissey



Peter Walker



A&L Goodbody

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Fintech in Ireland covers the whole spectrum of financial services and technology industries. At its core, it is centred on the combination of both in order to develop innovative business models which are disrupting the parameters of traditional financial services. Homegrown success stories like TransferMate, Realex Payments, Stripe, CurrencyFair, Fenargo and FundRecs operate in Ireland alongside global financial services giants and leading technology companies. These include Google, Microsoft, SAP, First Data, Visa and Paypal in areas such as money transfer and payments, lending, wealth management, crowdfunding, distributed ledger technology and digital currencies.

Ireland continues to build on its long-established record in the financial services and technology sectors. 49% of fintechs surveyed in late 2018 are expecting revenue growth of 100% or greater, with 32% of those anticipating global revenue growth of between 100–500%. Currently, there are approximately 200–300 fintech businesses in Ireland employing approximately 7,000 people, and this number is expected to rise to 10,000 by 2020. Access to a skilled workforce has been a strong contributing factor to the development of the Irish fintech ecosystem. It has established Dublin as a “*booming Fintech hub*” and set its sights on matching the success of top global fintech players such as London, New York, Silicon Valley and Singapore.

One of the most notable trends that emerged over the past year, which has impacted large multinationals and SMEs alike in the fintech sector, has been the establishment of Ireland as a location of choice for fintech businesses looking for a post-Brexit base. Fintechs have been forced to consider the impact of Brexit on their business and Ireland has leveraged its relationship with the UK market in this regard. This has contributed to several fintechs, like challenger banks such as Starling and Monzo and payments companies like Soldo, stating their intention to establish operations in Ireland following Brexit. The Central Bank of Ireland (CBI), Ireland’s financial services regulator, increased its headcount in 2018 to specifically deal with Brexit-related issues. They also established a “Brexit Task Force” to monitor risks arising for the Irish economy and financial system.

Ireland has also taken steps to establish itself as a blockchain hub, and the Irish Government signalled its intention to support this area by creating Blockchain Ireland, an initiative to promote innovation and co-operation across companies working with the technology. This has led to ConsenSys and Deloitte developing innovation studios in Dublin, Circle expanding its business internationally and Coinbase announcing its intention to open an office in Ireland as part of its Brexit plans.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

At present, there are no categories of fintech businesses that are prohibited in Ireland. However, depending on the nature of the activities being carried out, certain fintech businesses may be subject to regulatory authorisation and related restrictions.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

Most Irish fintech start-ups are raising funding through traditional funding mechanisms such as venture funding, Government-supported funding and debt. For example, the Irish Department of Finance estimated that crowdfunding constitutes only 0.33–0.4% of the SME finance market in Ireland compared with 12% in the UK. Equally, despite the massive global surge in capital raising through initial coin offerings (ICOs) and token sales, there have been few ICOs and token sales carried out by Irish companies to date.

We have included further details on the various available funding options below:

Equity

Venture capital firms and private equity investors continue to focus on high potential fintech businesses. The Irish Venture Capital Association recently reported that fintech companies raised nearly €100 million in Ireland last year. While this is a decrease in the level of venture capital investment in fintech businesses from 2017, venture capital continues to make up the majority of funding in Irish fintech businesses. To further promote investment in early stage companies, Enterprise Ireland has recently announced a new €175 million Seed and Venture Scheme to develop a commercially viable and sustainable sector.

Debt

In addition to traditional lending from financial institutions for small and medium-sized businesses, there are many alternative funding options available for fintech businesses in Ireland. Online financing platforms, crowdfunding and peer-to-peer lending platforms are often used in combination with more traditional sources of funding. Peer-to-peer lending is beginning to gain pace through platforms such as LinkedFinance and Flender. The speed at which funds can be raised makes this a particularly attractive option. Plans by the Department of Finance to regulate crowdfunding could further develop the debt funding options for fintech businesses.

Crowdfunding

Ireland does not currently have a bespoke regulatory regime for crowdfunding. However, the EU Commission has published a proposal for an EU Crowdfunding Regulation which includes a comprehensive authorisation and passporting regime for crowdfunding platforms across Europe. Once this has been enacted at EU level, it will form part of Irish law. This is in line with recommendations set out in the CBI's Feedback Paper on the Regulation of Crowdfunding in Ireland, which indicated that respondents to a consultation process on crowdfunding generally favoured regulation, provided that it is "proportionate and... facilitates the development and growth of the industry as opposed to stifling or hindering it".

Also, as detailed in question 3.3, the most recent iteration of the strategy for Ireland's International Financial Services Sector (IFS2020), published in February 2019, included a proposal to regulate crowdfunding in Ireland through a domestic regime that would operate in parallel with European Commission proposals.

Initial Coin Offerings & Token Sales

A small handful of Irish blockchain companies have raised capital through ICOs. As with crowdfunding, Ireland does not currently have a bespoke regulatory regime for token sales and ICOs. However, the CBI has issued warnings to investors (echoing similar warnings from EU regulators) on the risks associated with virtual currencies and ICOs.

However, in March 2018 the Department of Finance published a discussion paper on Virtual Currencies and Blockchain Technology, in which it proposed the creation of an intra-departmental Working Group that would draw on the expertise of multiple state agencies to explore and oversee developments in virtual currencies and blockchain. The Working Group's stated mandate will include "monitoring developments" at EU and global levels in relation to virtual currencies and blockchain, identifying economic opportunities for Ireland in this area, and "considering whether suitable policy recommendations" are required. The tone of the paper is not dissimilar from the approach adopted recently at EU level by the European Commission in its Fintech Action Plan 2018, in which the Commission committed to "monitoring the developments of cryptoassets and Initial Coin Offerings" together with EU regulators and other international standard setters, with a view to "assessing whether regulatory action at EU level is required".

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

Taxation

The attractively low corporate tax rate in Ireland of 12.5% in respect of trading profits is a major incentive for start-ups or companies

looking for a location for their business investments. Some other attractive features of Ireland's tax code relevant for IP companies include the R&D tax credit regime, the stamp duty exemption available on the transfer of a wide range of IP, the key employee reward mechanism, Ireland's Double Taxation Agreement network (currently 74 agreements signed and 73 in effect) and the potential effective 6.25% tax rate, under Ireland's Knowledge Development Box, on profits arising from certain IP assets which are created as a result of qualifying R&D activity carried out in Ireland or the European Economic Area (the EEA).

Enterprise Ireland

Enterprise Ireland (the state agency responsible for supporting the development of manufacturing and internationally traded services companies) offers a number of supports:

- **Competitive Start Fund (CSF):** This fund offers equity investments of up to €50,000 in return for a 10% equity stake. Calls are made throughout the year for specific sectors, and, in June 2018, a specific fintech CSF was announced which was open to companies working in fintech, proptech, artificial intelligence, machine learning, augmented and virtual reality, the internet of things, blockchain and cloud. This resulted in equity investments being made in five fintech businesses. A further call was made at the beginning of 2019, which was open to businesses in all sectors.
- **Innovative High Potential Start-Up (HPSU) Fund:** Enterprise Ireland offers equity investment to HPSU clients on a co-funded basis (similar to a venture capital approach). The funding goes towards the achievement of an overall business plan, rather than funding towards discrete elements of a business plan, such as R&D or employment creation. In 2018, Enterprise Ireland provided HPSU funding to 15 fintech businesses.

Industrial Development Authority (IDA)

In addition to providing logistical and practical support to multinational companies (MNCs) investing in Ireland, the IDA can in certain circumstances offer grant assistance to MNCs establishing or expanding their Irish activities. For the most part, grant assistance is linked to job creation and is contingent on the company submitting a formal business plan to the IDA. Any potential grant aid is negotiated on a project-by-project basis and is subject to approval of the board of the IDA. Total grants are subject to ceilings as dictated by EU state aid rules.

Ireland Strategic Investment Fund

The Ireland Strategic Investment Fund (ISIF) is an €8 billion sovereign development fund with a statutory mandate to invest on a commercial basis to support economic activity and investment in Ireland. ISIF has a long-term investment strategy, and therefore can act as a source of "permanent" or "patient" capital that can work to a longer-term horizon than most participants in the market.

ISIF has made a number of high-profile investments in US companies and funds, including Silicon Valley Bank, Polaris Partners, Lightstone Ventures, Sofinnova Ventures, Highland Capital Partners and Arch Venture Partners. It has invested across a wide variety of sectors, including various funds targeting financial services and technology.

Other Government-Backed Schemes

- **Disruptive Technologies Innovation Fund:** €500 million has been made available through this fund for projects involving enterprises and research partners by the Department of Business, Enterprise and Innovation. The funding will be available for projects that develop disruptive technologies which transform businesses and have SME participation. The first call for funding has occurred and awards have been made to companies, several of which are relying on artificial intelligence, data analytics and blockchain technology.

- **Startup Refunds for Entrepreneurs (SURE):** This initiative allows individuals to obtain a refund from the Government of up to 41% of the capital they invest in establishing their own company over a six-year period.
- **Employment and Investment Incentive (EII) Scheme:** This scheme allows individual investors to claim tax relief of up to 40% on investments they make in other companies. The EII scheme is available to unquoted micro, small and medium-sized trading companies, subject to certain exceptions.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

The first step in an Irish IPO is to decide which market to list in, which essentially depends on the scale of the business and the funding required by the company. The precise listing rules differ in respect of different markets. The Irish Stock Exchanges (**ISE**) offers four markets: Euronext Dublin, which is suited to large companies and requires a minimum of 25% of its shares to be placed in the public and requires a three-year trading record; the Euronext Growth, which suits smaller companies (minimum market capitalisation of €5 million) in the early stages as no trading record is required; the Global Exchange Market (**GEM**), which is a specialist debt market; and finally, the Atlantic Securities Market (**ASM**), which is a market dedicated to companies who wish to dual list in both the EU and the US.

General requirements for listing securities on Euronext Dublin (the principal market in Ireland) include the following:

- an issuer must be duly incorporated or otherwise validly established and operating in conformity with its constitutional document;
- securities must conform with applicable laws of the place of incorporation and be duly authorised;
- securities must be freely transferable; however, the ISE may permit securities that are partly paid if there is no restriction;
- expected aggregate market value of all securities must be at least €1 million for shares and €200,000 for debt securities;
- the whole class of securities must be listed; and
- an approved prospectus must be published for the securities.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

Examples of notable exits include:

- the founder of Realex Payments, an Irish online payment technology, exiting the business in 2015 following a €115 million acquisition by US company Global Payments; and
- Irish financial compliance solutions company Kyckr listing on the Australian stock exchange in October 2016.

It is expected that 2019 will see increased M&A activity within the fintech space. In particular, further consolidation within the emerging payment and regulatory solutions sector is anticipated.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

Ireland does not have a specific regulatory framework for fintech businesses. In some cases, fintech businesses will fall outside of the regulatory ambit as they do not involve the provision of services or

undertaking of activities which fall within a regulated activity (as defined in legislation).

However, fintech businesses providing regulated activities (as defined in legislation) which cannot avail of an exemption will fall within the existing body of financial regulation and so require prior authorisation from the CBI to conduct business. If authorised, the firms will be subject to Irish legislation and various ongoing CBI requirements, but fintech companies authorised by the CBI can benefit from regulatory passporting across the EU. Payment institutions, electronic money institutions (**EMIs**), investment companies, money transmission businesses and payment initiation and account information service providers are examples of business models which may require authorisation, as will certain crowdfunding platforms when the EU Crowdfunding Regulation comes into force.

The legislation most likely to apply to fintech businesses are: the Electronic Money Regulations 2011, which authorise undertakings to issue E-money; the Payment Services Regulations 2018, which govern payment institutions and third-party payment services providers providing payment initiation and account information services; the Markets In Financial Instruments Regulations 2017, which provide a regulatory framework for businesses who are providing investment services and activities; and the Central Bank Act 1971 (as amended), which governs applications for banking licences such as the recent application by Starling Bank. Fintech businesses may also be subject to consumer protection legislation and CBI codes of conduct, as well as anti-money laundering and data protection legislation.

Fintech businesses may also be subject to consumer protection legislation, the CBI codes of conduct including the Consumer Protection Code, as well as anti-money laundering and data protection legislation, depending on the services that they are offering.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

Cryptocurrencies and cryptoassets are not subject to specific regulation in Ireland, and the CBI confirmed that such virtual currencies do not have legal tender status in Ireland. However, despite the lack of specific regulation, it should be noted that cryptocurrencies or cryptoassets may be subject to the existing regulatory frameworks that are in place. The General Scheme of the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Bill 2019, which will transpose the Fifth EU Anti-Money Laundering Directive (**5AMLD**) into Irish law, should also be considered by fintechs operating in this sector. This bill has been approved by the Irish Government, and when enacted, it will impose obligations on (certain types of) exchanges and wallet providers.

As discussed in question 2.1, the Department of Finance has created an internal working group to monitor further developments in the areas of virtual currencies and blockchain technology moving forward. However, the regulation of cryptoassets is currently being considered at an EU level and Ireland will likely follow their approach to ensure a uniform regulatory regime is implemented.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

Central Bank of Ireland engagement with new entrants

The CBI is mandated as Ireland's financial services regulator. As part of this role, the CBI has encouraged fintech development but

also recognises and warns against the potential to blur lines between regulated and unregulated activities and the challenges this may present. The CBI has sought to develop a clearer picture of fintech activity in Ireland with a view to better understanding the implications for regulatory policy and supervisory activity. It has identified a number of areas, including payments, regtech, markets and exchanges, deposits and lending, investment and advice, insurance, analytics, capital raising, crowdfunding virtual currencies, ICOs and the start-up support ecosystem, where they consider fintech to be prevalent. The CBI continues to review the sector and is closely following and actively contributing to the European Supervisory Authority's approach to fintech. However, the CBI's focus is on the risks to consumers from fintech developments and on protecting consumers where activity is not yet regulated.

As part of its fintech engagement, the CBI launched its *Innovation Hub* in April 2018. This initiative is aimed at providing entities with a point of contact to engage on innovation and fintech. The European Banking Authority has described both innovation hubs and regulatory sandboxes as "innovation facilitators", and the CBI opted to use the former in its bid to facilitate financial innovation instead of developing a regulatory sandbox. The CBI recently reported that the Innovation Hub has had a "steady flow of engagement" with regtech and payment businesses since its launch. As part of the CBI's engagement through the Innovation Hub, they have hosted industry events, including information sessions on consumer protection, authorisations and supervision, as well as a Regtech Sprint Roundtable to discuss machine-readable rules. The Innovation Hub has, however, proven to be mutually beneficial for both the participants and the CBI, as it has given fintech firms a platform to make presentations to the CBI on their business models and provide them with information on their use of technology. The CBI will continue to use the Innovation Hub as a tool to get better sight of innovation as it occurs in fintech businesses and has highlighted the importance of engaging with innovators early in their development cycle.

A recent speech from the Head of the CBI's Consumer Protection Division also outlined the CBI's intention to commence a significant review of its Consumer Protection Code in 2019 in order to address emerging risks arising from the impact of innovation on financial products and services.

In addition, the CBI also participates in a working group with Enterprise Ireland, the IDA and the Department of Finance, which is coordinated by the Fintech & Payment Association of Ireland. The group also includes industry stakeholders and has recently published a strategy report on the future for Ireland's Fintech industry (available at https://fpai.ie/downloads/FPAI_FinTech_Report.pdf).

Government Engagement with New Entrants

In 2015, the Irish Government launched the IFS2020, and their most recent Action Plan was published in February 2019. This aims to consolidate and grow Ireland's position as the global location of choice for specialist international financial services. A key element of this strategy is the recognition and promotion of fintech as a rapidly expanding area of innovative financial services. To this end, the IDA is working with its clients to determine what role Ireland can play as they plan their future technology requirements.

IFS2020 aims to develop and maintain an effective ecosystem which addresses the needs of start-ups and scaling companies in terms of funding, skills, mentors, accelerators, an innovation-friendly regulatory environment and access to key markets, while at the same time addressing the needs of foreign-owned international financial services (IFS) companies. A key strategy objective is facilitating collaboration between large IFS companies and the

indigenous base to create disruptive solutions based on innovative products and services. MNCs in Ireland will be able to access products and services from a growing cluster of indigenous start-up firms in software, payments, peer-to-peer lending and analytics, all of which are looking to revolutionise the way technology is used in financial services.

IFS2020 has identified three key actions to be implemented over the course of the strategy in relation to fintech: enhancing IFS and information and communications technology (ICT) through sectoral collaboration while engaging both Irish-owned and foreign-owned SMEs and MNCs; sourcing funding for fintech; and supporting fintech accelerators through partnership with Enterprise Ireland. An example of the latter is Accenture's FinTech Innovation Lab, which is now in its fourth year. IFS2020 has also led to the publication of a yearly action plan in line with the overall strategy in order to execute its particular goals each year. As noted in question 2.1, the most recent iteration of IFS2020 includes a proposal to regulate crowdfunding in Ireland through a domestic regime that would operate in parallel with European Commission proposals in this area.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

A fintech business wishing to provide regulated services in Ireland, regardless of whether the business is based in Ireland or not, must either obtain authorisation from the CBI, avail of an exemption or "passport" into Ireland from another EU Member State.

Some key points to note in this regard are:

- Firms wishing to establish a regulated fintech business in Ireland must engage in the CBI's authorisation process. The CBI's key principle is that the firm's "heart and mind" must be in Ireland, as shown by the firm having its principal place of business in Ireland, sufficient senior management presence and demonstrating a high level of decision-making. It is expected that key leadership positions will operate from Ireland, including roles such as chief executive, head of finance, head of operations and head of compliance.
- The CBI will require the board to be of a sufficient size and have sufficient expertise to enable it to adequately oversee the company's operations, and have at least one independent non-executive director (such role is often filled by an Irish resident).
- There is no set minimum number of staff. Headcount will be driven by the levels of business activity planned and is to be discussed with the regulator. Outsourcing arrangements are permitted but must be documented in clear legal agreements.
- The CBI also requires firms applying for authorisation to be adequately capitalised. The amount will vary depending on the precise nature and scope of services in respect of which authorisation is required.
- Finally, the CBI will require the applicant to submit a business plan and summary details of all the key policies, processes and procedures which will be put in place in the new business, including detailed anti-money laundering policies.
- Various exemptions apply to the performance of regulated services. These exemptions can be general or apply to a specific area.

Alternatively, a fintech business authorised to provide regulated services in another EU Member State can notify the CBI (via its home stake regulator) that it intends to rely on the EU "passporting" regime to provide those activities in Ireland.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

The Data Protection Act 2018 (DPA) and the General Data Protection Regulation 2016/679 (GDPR) (together the **Data Protection Legislation**) together regulate the processing of personal data and apply to data controllers and data processors in Ireland, in the EU and those outside the EU who offer goods and services to, or monitor, EU residents.

The GDPR, as a regulation, is directly applicable in Ireland and the DPA gives effect to, and provides derogations from, the GDPR under Irish law. A notable derogation is that the digital age of consent in Ireland will be set at 16.

The profile and influence of the Data Protection Commission (DPC), the independent authority responsible for dealing with data protection issues in Ireland, has developed an increased status since the implementation of the Data Protection Legislation. It has become the lead data protection regulator for many of the world's largest multinational tech companies under the GDPR's one stop shop mechanism.

In addition, the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011, which implement Directive 2002/58/EC (as amended by Directive 2006/24/EC and 2009/136/EC) (the **ePrivacy Regulations**), deal with data protection issues in relation to phone, email, SMS and internet use and will generally apply to data controllers which fall within the scope of the DPA. The ePrivacy Regulations will be repealed when the European Commission's proposed Regulation on Privacy and Electronic Communications is passed; however, the timeline for the publication of this regulation remains unclear.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

Yes to both questions. The Data Protection Legislation applies to organisations not established in the EEA who offer goods and services to, or monitor, EU residents.

The Data Protection Legislation restricts the transfer of personal data to countries outside the EEA, unless the third country provides an adequate level of protection for the privacy of an individual. Accessing personal data from a third country amounts to transferring the personal data outside the EEA. Businesses wishing to transfer personal data outside the EEA must invoke one or more of the factors that legitimise transfers outside the EEA. The options include:

- the use of legally enforceable privacy/data protection codes of practice ("**Binding Corporate Rules**") by MNCs;
- Privacy Shield (for transfers to the US): a standard by which US companies can self-certify the adequacy of their data protection measures;
- model clauses: Irish data controllers may put in place EU-approved contractual provisions (known as **Model Clauses**). The validity of the Model Clauses is currently being questioned following the Irish High Court's decision to make a reference to the Court of Justice of the European Union as

to the validity of this mechanism. This decision has since been appealed to the Supreme Court but the reference remains valid and pending (*Data Protection Commissioner v. Facebook Ireland Limited & Maximillian Schrems Record Number S:AP:IE:2018:000068*). For the time being, however, the Model Clauses remain valid for data transfers outside the EEA; or

- approved codes of conduct and certification mechanisms, together with binding and enforceable commitments of the data controller or processor in the non-EEA country to apply the appropriate safeguards.

Of particular importance in an Irish context is the effect that a "no-deal" Brexit scenario may have on transfers of data from Irish controllers and processors to those in the UK. In such a scenario, the UK will no longer be a member of the EU and will become a third country under the Data Protection Legislation. Transfers of personal data from Ireland to the UK will be treated in the same way as transfers of personal data to countries like Australia, India or Brazil. In order to comply with GDPR rules, an Irish company intending to transfer personal data to the UK will need to put in place specific safeguards to protect the data in the context of its transfer and subsequent processing. So, the manner in which data and data transfers to the UK are dealt with as a result of Brexit will need to be considered by Irish fintechs.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

Regulatory Action

The DPC is responsible for the enforcement of the Data Protection Legislation and the e-Privacy Regulations. The DPC has a proactive approach to identifying data protection issues and regularly engages with public and private sector organisations on these issues.

Under the GDPR, the DPC has the power to order controllers or processors to take corrective actions or to impose significant administrative fines on data controllers and processors for non-compliance. Two maximum thresholds for fines are provided for under the GDPR, which apply depending on which data protection obligation has been breached. Businesses may face administrative fines of up to: (a) €10 million or 2% of the total worldwide annual turnover of the preceding financial year; or (b) €20 million or 4% of the total worldwide annual turnover of the preceding financial year. Fines can be imposed in addition to, or instead of, any corrective measures such as reprimands or warnings.

The DPC's enhanced powers provide further protection to data subjects and increase the risk profile for companies processing personal data. Consequently, data protection should be a priority issue for fintech businesses. In their 2018 Annual Report, the DPC noted that they continue to monitor new developments in the fintech industry including the use of blockchain, security and big data processing. They have developed a "Technology Leadership Unit" to support and maximise the effectiveness of the DPC's regulation and supervision of complex technology.

In addition, the DPA has created a number of criminal offences which are punishable by a fine of up to €5,000 and/or 12 months' imprisonment on summary conviction, or a fine of up to €250,000 and/or five years' imprisonment on conviction or indictment, depending on the nature of the offence. Offences under the DPA include:

- enforced access requests;
- unauthorised disclosure by the processor;
- disclosure of personal data obtained without authority;
- offences by directors, etc. of bodies corporate;

- knowingly or recklessly processing data relating to criminal convictions or offences;
- failure to co-operate with authorised officers during inspections, audits, and investigations;
- failing to comply with an information or enforcement notice; and
- obstructing a reviewer in the preparation of a report.

Damages

The GDPR provides data subjects with a right to recover non-pecuniary loss (such as damages for distress) and the recitals to the GDPR note that the concept of damages is to be interpreted broadly. This is a significant change from the previous position under the Data Protection Acts 1988 and 2003, where non-pecuniary damage was not recoverable in an action for breach of the duty of care.

Joint and several liability between parties who engage in the same data processing has also been introduced. Claims can be taken against parties jointly where they are collectively responsible for the damage caused, and it will then be for the controller or processor to claim back from the other controller or processor that part of the compensation corresponding to their responsibility for the damage.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

The obvious growth in the fintech sector, while considered to be mainly positive, also increases the need for regulation to avoid the abuse of online financial payments.

- **Data Protection Legislation:** The GDPR contains enhanced security measures and requires data controllers and data processors to implement “appropriate technical and organisational measures” to ensure a level of security appropriate to the risks that are presented by the processing of the data. These measures, where appropriate, should include: (i) pseudonymisation and encryption of the data; (ii) integrity and resilience of processing systems; (iii) the ability to restore availability and access in the event of a physical or technical incident; and (iv) regular testing of security measures. The DPA also requires controllers and processors to take all reasonable steps to ensure their employees and other persons at their place of work are aware of the technical and organisational measures in place to prevent the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, data concerned.
- **Payment Services Regulations:** The Payment Services Regulations 2018, which came into force on 13 January 2018, enhance regulation in this area by: (i) increasing reporting obligations applicable to providers offering payment services; (ii) applying new authorisation requirements for providers offering payment services (payment initiation and account information service providers now require authorisation); and (iii) requiring that all remote and online payment transactions meet strong customer authentication requirements. The issue of strong customer authentication is subject to regulatory technical standards published by the European Banking Authority that will come into effect on 14 September 2019.
- **Measures for a High Common Level of Security of Network and Information Systems Regulations:** The European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018 were implemented in September 2018 and set out legal measures to boost the overall level of cybersecurity protection. These measures include imposing security requirements and incident notification obligations on banks and other “operators of essential services” together with certain digital service providers. While financial sanctions

are available under the Regulations, for corporates it is the possible criminal prosecution that is the main fact to consider. The Regulations provide that where offences are committed by companies, but have been committed with the consent or connivance of one of its directors or other officers, or where such person has been acting with wilful neglect, that person as well as the company is guilty of an offence and may be prosecuted.

- **Cybercrime:** The Criminal Justice (Offences relating to Information Systems) Act 2017 came into force on 12 June 2017. This Act creates a number of new cybercrime offences including unauthorised access to information systems (e.g. hacking), interference with information systems or data and use of tools to facilitate commission of these offences.
- **Criminal Law:** As noted in question 4.3, the DPA has created several new criminal offences including unauthorised disclosure of personal data by a processor and disclosure of personal data obtained without authority. The unlawful operation of a computer with the intent of making gain is also a criminal offence under the Criminal Justice (Theft and Fraud) Offences Act 2001.
- **Damages:** The GDPR provides data subjects with a right to recover non-pecuniary loss, and the recitals to the GDPR note that the concept of damages is to be interpreted broadly and lists the loss of control over personal data as an example of such damage. As such, controllers or processors may be subject to a claim for damages where a cybersecurity incident arises in causing such damages.
- **Regulatory Guidance:** Payment service providers must comply with the European Banking Authority Guidelines on security measures for operational and security risks under PSD2. Other categories of fintech businesses regulated by the CBI may need to comply with the CBI’s 2016 cross-industry guidance in respect of IT and cybersecurity risks (available at: <https://centralbank.ie/docs/default-source/Regulation/how-we-regulate/policy/cross-industry-guidance-information-technology-cybersecurity-risks.pdf?sfvrsn=2>).

An organisation which suffers a data security incident may also be subject to a number of separate incident notification obligations, including under financial and payment services regulations, data protection and/or information security regulations.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

Ireland’s key anti-money laundering and terrorist financing legislation is set out in Criminal Justice (Money Laundering and Terrorist Financing) Acts 2010 to 2018 (referred to collectively as the **CJA**). Designated persons under the CJA, including all financial institutions authorised by the CBI or businesses conducting certain activities, have statutory obligations to comply with the CJA provisions. The CJA involves a combination of risk-based and rules-based approaches to the prevention of money laundering and terrorist financing.

Designated persons must apply customer due diligence, report suspicious transactions and have specific procedures in place to prevent money laundering and terrorist financing. Failure to comply with the CJA is an offence.

Ireland implemented the Fourth EU Anti-Money Laundering Directive (**4MLD**) in November 2018 through amendments to the CJA. Key amendments include the introduction of requirements around business risk assessments, as well as enhancements to customer due diligence and transaction monitoring requirements.

As referenced in question 3.2, the Irish Government has taken initial steps in relation to the implementation of 5MLD and this legislation

will impose obligations on the usage of cryptocurrency exchanges and custodians in certain instances. The Sixth EU Anti-Money Laundering Directive (6MLD) has also come into effect and the transposition deadline has been set for 3 December 2020.

Bribery and corruption are criminalised in Ireland under the Prevention of Corruption Acts 1889 to 2010. However, there are weaknesses in the legislation which have sometimes made it difficult to enforce. Revised legislation is expected to be introduced shortly.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

There is no fintech-specific regulatory regime in Ireland. The applicable regimes and legislation are described above. Any other applicable regulatory regimes would probably be specific to the sector in which a particular fintech business operates.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

Hiring and Recruitment

Employees are entitled to receive written notification of certain core terms of employment (set out in the Employment Miscellaneous Provisions Act 2018) within five days of commencing employment. All other terms and conditions of employment must be provided within two months of commencement.

Employers must comply with equality legislation not only in the context of existing employees, but also in all aspects of recruitment, including job advertisements and candidate selection. Employers must ensure that in advertising and interviewing for a particular position, they do not give rise to an inference of discrimination on one of the nine protected grounds (gender, civil status, family status, sexual orientation, religion, race, age, disability, or membership of the Traveller Community). The maximum compensation available to non-employees who bring a successful discrimination claim in relation to a job application is €13,000.

Dismissing Staff

“Employment at will” does not exist as a concept in Ireland and employees are protected from dismissal without cause. Dismissal of employees is regulated in Ireland by statute and by the employee’s employment contract. All employers are obliged to have in place a disciplinary procedure setting out the steps to be followed by an employer in dealing with issues of concern, such as conduct or performance.

The Unfair Dismissals Acts 1977 to 2015 (the **UD Acts**) govern the dismissal of staff. The UD Acts provide that every dismissal is deemed to be unfair unless it is based on one of six fair grounds for dismissal:

- capability;
- conduct;
- qualification;
- redundancy of the role;
- competence of the employee;
- statutory prohibition; or
- some other substantial reason justifying dismissal.

The UD Acts provide that the onus is on employers to show the following: (i) substantial grounds justifying the dismissal based on one of the grounds set out above; and (ii) that fair procedures were followed in effecting the dismissal. The extent of fair procedures to be followed will depend on the circumstances and the reason for effecting the dismissal. Failure to follow fair procedures and/or establish a fair reason for dismissal may lead to a finding of unfair dismissal against the employer, notwithstanding the giving of notice.

The UD Acts apply to employees who have obtained one year’s service (there are limited exceptions to the one year’s service rule). Employees may also bring a claim for discriminatory dismissal under the Employment Equality Acts 1998 to 2015 (the **EE Acts**) where their dismissal is connected with one of the nine protected grounds listed above, but they have not obtained the requisite one year’s service to bring a claim under the UD Acts.

The maximum compensation available under the UD Acts (and the EE Acts for discriminatory dismissal) is: (i) two years’ remuneration (five years’ remuneration in the case of dismissal resulting from the making of a protected disclosure); (ii) re-engagement; or (iii) re-instatement.

In Ireland there is also a risk of an employee applying to the High Court for an employment injunction, often to prohibit their employer suspending, dismissing or otherwise disciplining them on the basis that fair process and/or natural justice has not been afforded to the employee.

Redundancy

Irish legislation provides specific protection for employees where their position ceases to exist and they are not replaced. In a genuine redundancy situation, fair procedures require employers to consult with employees whose roles are identified to be “at risk” of redundancy prior to any final decision to confirm the redundancy of that role. The purpose of the consultation process is to identify any alternatives to the redundancy, including redeployment, etc.

Irish law entitles employees (with over two years’ service) to a statutory redundancy payment which is tax-free. It is calculated on the basis of two weeks’ pay per year of service, plus a bonus week’s pay. A week’s pay is capped at €600 per week. Depending on the industry, employers may pay enhanced severance terms, subject to the employees signing waiver agreements; however, this is not mandatory. Any enhanced redundancy package provided will likely set a precedent (by way of custom and practice) for future redundancy situations.

Where a collective redundancy situation arises, specific statutory consultation obligations and notifications to the Minister for Employment Affairs and Social Protection (as well as to employees via employee representatives) are triggered for the employer. These obligations apply to employers with a workforce of 21 employees or more.

A collective redundancy situation is one that involves making a specified number of employees redundant within a 30 consecutive-day period. A failure to comply with the notification and consultation requirements could result in substantial penalties.

Notice Period

Employees are entitled to certain minimum statutory notice periods depending on their length of service (ranging from one to eight weeks). An employee who does not receive this notice period (or pay *in lieu*) may bring a claim for wrongful dismissal and loss of earnings during the notice period. In practice, depending on the employee’s role, their contract of employment may provide for a contractual notice period that is longer than their statutory entitlement.

In circumstances of gross misconduct, an employee may be summarily dismissed without notice or pay *in lieu* of notice.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Under Irish law, an employer can engage employees on such terms as it deems appropriate, provided the following mandatory benefits are protected:

- **Annual Leave:** employees accrue paid vacation based on time actually worked, subject to a statutory minimum of four working weeks (20 days) – pro-rated for part-time employees. Employees are also entitled to a paid day off or an additional day’s pay in respect of Irish public holidays.
- **Rates of Pay:** the national minimum wage for employees in Ireland is €9.80 per hour. However, this rate may vary in certain sectors of employment.
- **Pension:** outside of any contractual commitments, there is currently no legal obligation on an employer to establish a pension plan for employees based in Ireland. An employer is not required to contribute to a pension for an employee; however, it is required to provide employees with access to a pension scheme, which may include facilitating deductions to a personal retirement savings account (**PRSA**).
- **Protected Leave:** Ireland has the following protected leaves:

Leave	Entitlement	Obligation to pay
Maternity Leave	Up to 42 weeks (26 weeks’ basic leave (paid by the State) and 16 weeks’ unpaid leave).	No obligation to pay. However, many employers “top up” the State benefit during the basic 26 weeks’ entitlement.
Adoptive Leave	Up to 40 weeks (24 weeks’ basic leave (paid by the State) and an additional 16 weeks’ unpaid leave).	No obligation to pay. However, many employers “top up” the State benefit during the basic 24 weeks’ entitlement.
Paternity Leave	Up to two weeks’ leave (paid by the State).	No obligation to pay. However, many employers “top up” the State benefit during the paternity leave.
Carer’s Leave	Available to employees with over one years’ service to take care of a “relevant person”. Up to a maximum of 104 weeks’ unpaid leave.	No obligation to pay.
Parental Leave	Available to employees with over one years’ service. 18 weeks’ unpaid leave per child (up to the child’s age of eight with limited exceptions).	No obligation to pay.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

All EEA nationals have the right to work in Ireland. Non-EEA nationals must have a valid employment permit in order to work in the State. Permits are administered by the Employment Permit Section of the Department of Business, Enterprise and Innovation.

There are nine different types of permits which may be applied for depending on the type of employment involved.

Special Route for Obtaining Permission for Individuals Who Work for Fintech Businesses:

As part of a highly skilled workforce, many employees in the fintech industry can apply for a Critical Skills Employment Permit. In order to be eligible for such permits, the employee must have:

- a job offer of at least two years within the State; and
- an annual salary of €60,000 or more.

Jobs with annual salaries of €30,000 or more may also be eligible provided they are one of the occupations listed on the Highly Skilled Occupations List.

The permits are valid for two years, and on expiration, the employee may apply for a “Stamp 4” permission to remain and work in the State without an employment permit. This permission is renewable on an annual basis. Once the applicant has legally resided in Ireland for five years, they may then be eligible to apply for long-term residence permission.

Depending on the circumstances, the following permits may also be applied for in the context of fintech workers:

- **Intra-company Transfer Employment Permit:** Key management staff and management, as well as qualifying trainees, of a MNC can be transferred to an Irish branch of the company with this permit.
- **General Employment Permit:** This may be used where the job in question fails to satisfy the salary requirements of the Critical Skills Employment Permit. However, as applications for this permit must satisfy a “labour market means test”, it is not a particularly common form of work permit.
- **Contract for Services Employment Permit:** This enables the transfer of non-EEA employees to work in Ireland whilst remaining employed under their contract of employment outside of the State.
- **Internship Employment Permit:** This permit is available to full-time students enrolled in third-level education outside of the State who have been offered an internship or work experience in Ireland.

Legally resident dependants of employees with permits may also apply for Dependant/Partner/Spouse Employment Permits.

Employers and contractors in the fintech industry may also sign up to the Trusted Partner Initiative. Under this scheme, employers can apply for “Trusted Partner” status in order to fast track the permit application process.

Certain senior roleholders in fintech businesses providing regulated activities would also need to obtain the CBI’s approval prior to taking up that position, under the “Fitness and Probity” regime.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

The Irish legislative framework gives significant comfort to companies creating and managing their IP assets in Ireland. Patents, copyright, design rights, trade marks and confidential information can be used to protect inventions and innovations. All of the core Irish legislation in relation to these forms of protection has been introduced in the relatively recent past. The Commercial Court, a division of the Irish High Court, deals with major commercial and IP cases on an expedited basis and offers an effective way for fintech businesses to enforce their IP rights.

Copyright: Typically, copyright is the most useful protection for the kind of IP generated by fintech businesses, e.g. copyright protects the underlying code in software and computer programs. There is no system of registration for copyright protection in Ireland as copyright attaches automatically on the creation of an original work. Trade secrets can also be useful in protecting software.

Patents: There are two types of patent protection available under Irish patent legislation: a full-term patent and a short-term patent. In order for an invention to be patentable it must: (i) be new; (ii) involve an inventive step; and (iii) be capable of industrial application.

Trade marks and designs: Trade marks may be registered to protect the branding of fintech products and companies. Designs which are new and have individual character can be registered to protect the appearance of products.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Under Irish law, ownership of a patent rests with the inventor. If the invention is made by an employee in the course of their employment, the right to a patent will usually belong to the employer. In relation to copyright, the author of a work is the first owner. Similar to patent ownership, if a copyright work is made by an employee in the course of employment, the first owner of the work will be the employer, subject to any agreement to the contrary. Ownership of registered trade marks and designs will vest in the person who has applied for registration.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

Copyright: Ireland is a party to and incurs obligations under the Berne Convention (Paris Act), the Rome Convention, the TRIPS Agreement, the World Intellectual Property Organisation (WIPO) Copyright Treaty, and the WIPO Performances and Phonograms Treaty. These international agreements provide for automatic reciprocal protection for Irish copyright works in the territories of the signatories.

Patents: Patent protection may be secured by applying for (i) national protection in the Irish Patents Office, (ii) protection via the European Patent Convention (EPC), or (iii) protection under the Patent Cooperation Treaty (PCT) which provides for an international search and examination system. The outcome of a EPC or PCT application will, depending on the results of the search and examination process and application of national patent rules, result in national patents being granted which may be enforced in the jurisdictions in which they are registered.

Plans are at an advanced stage for the introduction of the EU Unitary Patent Package (UPP) which would provide: (i) a single unitary

patent offering protection across EU Member States; and (ii) a Unified Patent Court (UPC). A referendum in Ireland is expected to be scheduled on the proposed UPC which, if ratified, will establish a specialised patent court with exclusive jurisdiction for litigation in relation to both European patents and European patents with unitary effect in all participating Member States.

Trade marks: Trade marks may be secured by applying for: (i) a national registration; (ii) an EU trade mark (which offers protection across all 28 EU Member States); or (iii) a registration under the Madrid System which provides for a single application through the national office, resulting in a bundle of national trade mark registrations for the countries designated in the application. Irish and EU trade marks may be enforced in the Irish courts.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

Licensing: In Ireland, licensing IP rights creates revenue streams whilst retaining ownership. An important consideration is that of an exclusive *versus* non-exclusive licence which has the potential to limit the use of the IP to one third party. If for commercial reasons, an exclusive licence is granted, there are other options available that can be employed to maximise value; for example, by limiting exclusivity to a particular location or limiting the scope of use of the licence, thus retaining the ability to commercialise the same IP in other territories and/or other fields of use with other licensees. In any event, a licensor should retain sufficient control over its IP by ensuring sufficient obligations are imposed on the third party, including provisions allowing the licensor to monitor the licensee's use of the IP and appropriate termination rights. The granting of a licence for a patent, trade mark or design should be notified to the Controller of Patents, Designs and Trade Marks (the **Controller**).

Assignment: In general, assignments of IP must be in writing. One notable exception is that trade marks are now automatically transferred with a business under the European Union (Trade Marks) Regulations 2018 unless there is an agreement to the contrary, or circumstances clearly dictate otherwise. Assignment of patents, trade marks and designs must be registered with the Controller. Copyright may be freely assigned and is not subject to any specific registration requirement.

Granting a security interest: Security may be granted over IP (most commonly patents, trade marks and copyright) under Irish law. Particulars of a security interest which is granted by an Irish company must be registered with the Irish Companies Registration Office within 21 days of the granting of the interest. Security interests granted over patents, trade marks and designs must be notified to the Controller and an original or certified copy of the security interest evidencing the agreement between the parties must be submitted to support the application.

**Claire Morrissey**

A&L Goodbody
IFSC, North Wall Quay
Dublin 1
Ireland

Tel: +353 1 649 2246
Email: cmorrissey@algoodbody.com
URL: www.algoodbody.com

Claire Morrissey is a Partner in the Firm's IP & Technology Group. She advises on a broad range of commercial contracts with a particular focus on technology, IP and sourcing agreements. Claire also advises on the technology, IP and data aspects of joint ventures, mergers & acquisitions.

**Peter Walker**

A&L Goodbody
IFSC, North Wall Quay
Dublin 1
Ireland

Tel: +353 1 649 2000
Email: pwalker@algoodbody.com
URL: www.algoodbody.com

Peter Walker is a Partner in the Banking and Financial Services Department. His principal practice areas are asset-backed finance (including portfolio sales and acquisitions), debt capital markets, private equity finance, general banking & restructurings.

A&L Goodbody

With an established banking sector in Ireland and a rapidly evolving technology landscape, A&L Goodbody's FinTech Group's legal expertise facilitates a cutting-edge approach to advising companies in this sector. Our clients include domestic and international financial services and technology companies, and our team provides a complete legal service for related legal needs.

We advise a wide range of fintech matters including: the development; acquisition and use of technologies and services; strategic software development agreements; IT-managed and shared services arrangements; complex transitional services agreements; transactional advice; and business process outsourcing. We also advise clients in relation to technology, financial regulation, compliance, risk management, data privacy, financing, cyber risk and the implications of Brexit.

In addition, A&L Goodbody is a member of the Fintech and Payments Association of Ireland.

Israel



Ariel Rosenberg



Sharon Gazit

Goldfarb Seligman & Co.

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

The Israeli Fintech industry is characterised by a gap between the richness of technology existing in R&D centres, the varieties of active and prospering Fintech start-ups, and the global services offered by them, on the one hand, and the limited penetration level of Fintech-based services into the local retail market, on the other.

An innovative and entrepreneurial atmosphere and long-established technology and venture capital industries, in general, together with the abundance of financial-sector veterans and accelerators focusing on Fintech, position the Israeli market as a unique hot spot for Fintech development. The year of 2018 was another record-breaking year in terms of the investment raised by local Fintech companies.

Fintech solutions have found their way initially into the service offering of traditional financial institutions. Examples include the introduction of digital banking and payment solutions such as Bit, Pepper and Paybox by Bank Hapoalim, Bank Leumi and Bank Discount, respectively; the introduction of a digital-based investment advice platform (robo-advisor) offered to portfolio holders by certain banks; and digital-based portfolio management services offered by certain investment houses.

A significant innovation trend is the development of investment management algorithms and offerings of alternative asset management to institutional investors. One of the important players in that area is the start-up Pagaya, which is focused on the US consumer credit market through a big data machine-learning algorithm, and which has raised significant investments from Israeli and global financial institutions, sovereign funds and investment funds.

The local B2B lending market has continued its stride amidst the highly competitive Israeli lending market. In addition, the expected coming-into-effect of the new credit data regulation, which will provide a wider group of credit providers with access to a central credit registry, is expected to substantially increase the market share of new Fintech-based players in the consumer credit market, and in small business and receivables credit markets.

The payments market continues to be dominated by existing traditional banks and credit card companies. However, the separation of Leumi Card, one of the three leading credit card companies, from its former owner (Bank Leumi) through its acquisition by foreign

investors, and the forthcoming separation of another credit card from its current bank owner, is expected to result in the introduction of Fintech-based innovative services by those newly acquired credit card companies.

Newly introduced regulations, which apply to non-bank financial services, have created, together with challenges, various opportunities for new players. The recent regulation of formerly non-regulated or under-regulated financial services, such as electronic wallets and electronic payments-related services, has supported needed conditions for wider consumer confidence in the newly introduced Fintech-based financial services.

While Israel is an important hub for blockchain technology-based companies, blockchain technology and cryptocurrencies are yet to be present in daily activities.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

Many activities which are commonly referred to as financial services are subject to licensing requirements issuable by the relevant regulators, and to applicable regulations.

There is a general ban on businesses engaging in activities related to binary options or gambling.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

Generally speaking, the “traditional” types of funding, i.e., equity investments and convertible debt instruments, are the most dominant in the Fintech field. Very early-stage businesses have raised funding by way of convertible debt instruments, including SAFE agreements and CLAs, and have used the funds raised to demonstrate proof of concept and an MVP working model. More mature Fintech businesses opted for the equity financing path mainly from VCs and designated accelerators. There are quite a few Fintech-designated accelerators and innovation centres in Israel, most of them founded by Israeli banks as well as foreign banks, which consider the Israeli innovative ecosystem to be productive to the Fintech disruptive technologies. In the VC arena, most VCs invest, amongst other fields, in Fintech ventures.

It is also worth mentioning another funding path, via the Israeli Innovation Authority (“IIA”).

One of the IIA's support programmes intends to encourage R&D in the Fintech field (amongst other technology fields). The programme – R&D Fund – supports commercial Fintech companies by way of funding R&D of new Fintech products as well as upgrading existing Fintech technologies. The support amounts lie between 20% and 50% of the approved R&D expenses (and an additional 10% is granted to companies which operate in peripheral areas). The funding is repaid only by way of royalties from sales or other commercialisation revenues.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

Under the Encouragement of Capital Investments Law, companies may enjoy certain tax incentives and grants under the “Preferred Enterprise” regime or under the “Preferred Technology Enterprise” and “Special Preferred Technology Enterprise” regimes, if the relevant criteria are met. The Preferred Enterprise regime may be applicable to Fintech companies only where they engage in the sale of software products or licences or the development of software for others. This regime, therefore, is not relevant to Fintech companies which focus on providing financial services to end-users. The Preferred Technology and the Special Preferred Technology Enterprise regimes are relevant to companies which meet certain criteria relating to their investments in R&D, the scope of their R&D teams, certain revenues and employment growth; such status is subject to the approval of the National Authority for Technology and Innovation.

Under the Income Tax Ordinance, certain R&D costs incurred by a company may be recognised, subject to certain criteria, as deductible ongoing business costs rather than capital costs.

A special benefit may be provided to seed investments in qualified high-tech companies which meet certain criteria, under the law nicknamed the “Angels Law”. If the relevant criteria are met, such investments can be amortised through a defined period and deductible against the ongoing business income of the investors.

The tax authorities have issued a tax circular applicable to venture capital funds which meet certain qualifications. Under the circular, a special tax exemption applies to certain incomes (capital gains, dividends and interest) of such venture capital funds generated from qualified venture capital investments.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

According to the Israeli Securities Law, a public offering is subject to the publication of a prospectus (which includes the details set forth in the relevant regulations). The publication of the prospectus requires pre-approval by the Israeli Security Authority following a thorough review.

In order for a company to be listed in the Tel Aviv Stock Exchange (“TASE”), the company has to meet criteria which include equity value, the value of the shares held by the public, a minimum number of holders, previous activity period, and a market cap. There are various alternatives to measure whether the issuer meets the criteria; in each alternative, different thresholds (or no thresholds) apply with respect to the various criteria. Another alternative with criteria of lower thresholds applies to companies engaged in R&D or infrastructure.

Companies listed in the TASE should have only one class of shares. Preferred shares, with preference related to dividend distribution, are also allowed with certain limitations.

When a company's shares have been issued to the public in Israel, it is regarded as a “Public Company”. A Public Company is subject to laws and regulations, mostly related to corporate governance and reporting duties.

Note that many Israeli technology companies choose to be listed in foreign exchanges such as NASDAQ and AIM.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

Notable exits of Fintech businesses (with an Israeli nexus) in recent years include: Fundtech; SuperDrivates; Boarderfree (IPO and subsequent acquisition by Pitney Bowes); Sling (acquired by Avante); ActivePath (acquired by Broadridge); BillGuard (acquired by Prosper); Markets.com (acquired by Playtech); Zouz (acquired by PayU); and the significant financing rounds of Payoneer and BlueVine.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

Generally speaking, there is no single set of regulations which apply specifically to Fintech businesses; instead, several regulatory frameworks might apply, depending on the type of financial activity or financial services. Many activities are subject to licensing or permit requirements; permit requirements are applicable in most cases to shareholding (above a certain threshold) in a licensed entity. Banking activity and credit cards clearing are subject to the various banking laws and are supervised by the Supervisor of Banks at the Bank of Israel. Insurance Companies, pension funds and similar long-term saving schemes are subject to their respective regulatory framework and supervised by the Commissioner of Capital Markets, Insurance and Savings at the Ministry of Finance. Non-bank providers of “financial assets” (broadly defined to include various financial assets and currencies), related services (which include, *inter alia*, custody and exchange services), as well as lending, are subject to a newly introduced regulatory regime and licensing requirement and are supervised by the Ministry of Finance. Investment advice, investment marketing and portfolio management have their own regulatory framework and are supervised by the Israeli Securities Authority. Stock exchanges and trading venues are subject to their own regulatory regime and are supervised by the Israeli Security Authority.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

Cryptocurrencies are regarded as a “financial asset” for purposes of regulation of non-bank financial services. Accordingly, certain cryptocurrency-related services, such as custody and exchange services, are subject to a newly introduced regulatory regime and licensing requirement and are supervised by the Ministry of Finance.

Questions of ICOs and IPOs of companies focused on cryptocurrencies have been recently reviewed by the Israeli Securities Authority. A report issued by the ISA addressed the regulatory aspects of cryptocurrency-related activities. The report views the offering to the public of cryptocurrencies (and

cryptoassets) as a public offering of securities with all its entailed regulatory requirements, although it mentions that under certain circumstances utility tokens may be excluded from that rule. In addition, the report provides that cryptocurrency trading platforms may be subject to regulatory regimes applicable to stock exchanges or financial assets trading arenas.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

In recent years, the financial regulators have acted to encourage digitisation of financial services. Their policies have been implemented through public speeches and announcements, through supporting regulations, and through daily policy implementation. From our experience, financial regulators are open to dialogue, attend the needs of newly introduced Fintech businesses which offer new solutions, and encourage competition in the market.

The Supervisor of Banks at the Bank of Israel has published regulations facilitating the opening of online bank accounts, through an easier underwriting process. Another initiative of the banking regulator was a requirement that banks supply each customer with a digital "financial identity card" to facilitate the ability of customers to compare quality of services provided and their costs. A general credit database will become available shortly.

New regulations of non-bank financial services, recently introduced by the Ministry of Finance, reflect the declared policy of the MoF to open the financial services sector to new competition, including through service offerings by Fintech businesses. The new legislation does not, naturally, cater to all the needs derived from the *modus operandi* of the various Fintech solutions. However, practitioners attest to the regulator's willingness to find regulatory solutions required to encourage the introduction of new Fintech solutions, and competition in the market.

Recently, an inter-ministerial team has issued recommendations for the establishment of a regulatory sandbox in order to facilitate the activity of Fintech companies in general, and particularly companies engaged in blockchain and cryptocurrency-related activities.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

Most types of financial services are subject to licensing requirements. In some cases, it is required that the licence holder be an Israeli person/entity; for certain businesses, acting through a subsidiary instead of a local branch of a foreign company poses a hurdle for entering the local market. Tax issues, such as withholding tax imposed on interest payments to foreign persons, and VAT issues, can be another disadvantage.

From a business perspective, a very competitive consumer credit market together with a relatively small non-bank sector, and the limited scope of the market both geographically and in terms of the number of potential users, require newcomers to diligently search for the appropriate unexploited niches.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

The regulations that govern the collection, use and transmission of personal data in general are the Israeli Protection of Privacy Law, 574–1981 (hereinafter: the "Privacy Law"), the Privacy Protection Regulations (Data Security), 5772–2017, which came into effect on May 8, 2018 ("Data Security Regulations"), the Basic Law: Human Dignity and Liberty, 5752–1992 and the guidelines of The Israel Privacy Authority ("IPA"). The collection, processing or use of personal data is permitted, subject to obtaining the informed consent of the data subjects. Such consent should adhere to purpose, proportionality and transparency limitations. Any request for consent from a data subject to have his or her personal data stored and used within a database must be accompanied by a notice indicating: (i) whether there is a legal requirement to provide the information; (ii) the purpose for which the information is requested; (iii) the recipients of the data; and (iv) the purpose(s) of use of the data. As Israeli laws do not specifically address Fintech businesses, such businesses are also obligated to comply with the Privacy Law and its related regulations. According to the Privacy Law, some Fintech businesses such as banks, as well as other entities that are listed thereunder, are obligated to appoint a Data Security Supervisor. The Privacy Law does not state whether the Data Security Supervisor must be present in Israel.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

The Israeli Privacy Law remains unclear as to whether merely collecting and/or processing personal data from Israeli data subjects by organisations abroad is subject to Israeli data protection laws, if those activities are conducted exclusively outside Israel, by an entity incorporated outside Israel with no other nexus to Israel. Nevertheless, the transfer of personal information outside of Israel is permitted provided that: (i) the data is transferred to a country affording an adequate level of protection; or alternatively, if one of a set of listed conditions set forth in the Protection of Privacy (Transfer of Data to Databases Abroad) Regulations, 5761–2001 (hereinafter – "Transfer Regulations") applies (such as that the data subject's informed consent was obtained); and (ii) the recipient signs a data protection undertaking in accordance with the Transfer Regulations.

On October 19, 2015 the IPA stated that further to the European Union's decision, which declared the Safe Harbour arrangement to be invalid, the Safe Harbour shall no longer be deemed as meeting the preliminary conditions under the Transfer Regulations for transfer of personal information to the US. To date, the IPA has not stated its opinion regarding the status of the Privacy Shield and, therefore, it currently cannot be relied upon in itself as meeting the terms of the Transfer Regulations. However, the foregoing does not derogate from the right to transfer personal information to the US or elsewhere when complying with the conditions under the Transfer Regulations, as detailed above.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

Currently, the Privacy Law provides the following sanctions for failing to comply with said Law: (i) administrative fines, imposed by the IPA, up to approximately USD 1,415; (ii) criminal sanctions, imprisonment or fines, up to five years' imprisonment or up to approximately USD 72,954; and (iii) civil sanctions imposed by court, that may rise up to approximately USD 14,140, and may be doubled where the privacy violation was with intent to harm.

On March 5, 2018, the Israeli Parliament passed for first reading (out of three readings) a proposed amendment for the Protection of Privacy Law (Amendment No. 13), 5768–2018 (“Bill”). If such Bill passes, the IPA shall be able to impose administrative fines of up to approximately USD 905,000 (NIS 3.2 million) on an organisation that severely violates the Privacy Law.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

Israel does not currently have any laws dedicated to cyber security matters solely. However, there are several regulations and government resolutions that address cyber security issues:

1. The Data Security Regulations further broaden the Privacy Law by imposing additional data security requirements applicable to database managers and processors. Such additional requirements include, without limitation: having in place a broad list of manuals and policies; various physical, environmental and logical security measures; and regular audit, inspection and training obligations.
2. Israel's financial regulators have issued a number of directives that specifically address cyber security in the Fintech sector. These include Bank of Israel Directive 361 – Proper Conduct of Banking Business, which sets out a general framework for cyber risk management in the banking sector, and Directive 357 – Information Security Management, which details information security controls for banking corporations. The Supervisor of the Capital Market, Insurance and Saving Authority of the Israeli Ministry of Finance published guidelines for institutional entities on August 31, 2016 (Circular 2016-9-14), which address the issue of cyber security in institutional entities. The above-mentioned Circular requires that institutional entities, *inter alia*, assess the potential risks in their organisation, elect a steering committee to mitigate cyber risk, as well as put in place a set of policies and work plans to reduce potential cyber-attacks. The Credit Information Law, 5776–2016 authorises the Bank of Israel to promulgate information security requirements for credit bureaus.
3. The Computers Law, 5755–1995 sets the framework so that any change, distortion or harm to computer software, access and permission deviation using a computer, and presenting false output information can constitute as criminal crimes.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

Under the Prohibition on Money Laundering Law, a provider of defined financial services (“Currency Services”) is subject to a registration requirement as a “Currency Services Provider” and to KYC requirements imposed under the Money Laundering Prohibition Order (Requirements for Identification, Reporting and Administration of Currency Services Providers). The Order imposes several different

sets of KYC procedures (depending on the transaction requested, and the person receiving or requesting the services), which includes the customer identification process, registration of identification details, authentication and document procurement, declaration procurement, and face-to-face identification. The Currency Services Providers are also subject to reporting requirements. The Prohibition on Terrorist Financing Law, 5765–2004, which sets out a mechanism to declare an organisation as a terrorist organisation even if it is unconnected to Israel, may also be applicable. The law also widened the powers of seizure and forfeiture of monies suspected as being money involved in the financing of terror, and grants powers to the Minister of Defence, to order the administrative seizure of funds suspected of being terrorist funds.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

Other than the specific regulatory regimes described above, Fintech businesses are subject to the laws and regulations generally applicable to any business in Israel, such as the various tax laws or the obligation, under certain circumstances, to be issued a business licence by the relevant municipality. Fintech businesses that do not fall under the licensable financial services categories might be subject to general consumer protection laws and regulations.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

In general, no special licence or qualifications are required in order to employ people in Israel. However, an employer has to open a tax file with the Israeli tax authorities in connection with its obligations to transfer withholding taxes and compulsory payments.

As a general rule, an employer may dismiss an employee at will, subject to certain requirements such as advance hearing, advance notice and severance payment. Dismissal is not allowed in certain outstanding cases such as bad faith, where discriminatory circumstances exist, dismissal of a pregnant employee or an employee during (or immediately after) maternity leave or reserve military service.

Certain additional provisions might apply through collective agreements or collective arrangements, to the extent applicable to the employment sector or context.

While engagements between a business and a service provider on a non-employment basis exist in the technology sector, certain criteria must be met in order for the engagement to be deemed to create a contractual non-employment relationship; each case should be carefully reviewed based on the specific circumstances.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Employees are entitled to receive, at the beginning of their employment, a written notice specifying the terms and rights of their employment. The salary should exceed the legally defined minimum wage. Employees are entitled, *inter alia*, to a defined number of paid vacation days and sick leave, a break time during the day, reimbursement of commuting expenses, payment for overtime, and an

annual convalescence payment. An employer is required to provide pension and severance payment funds for the benefit of its employees. Certain additional provisions might apply through collective agreements or collective arrangements, to the extent applicable to the employment sector or context.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

Employment of a foreign person requires a special permit from the Population and Immigration Authority. Employees in the technology sector fall under the “experts” category, and the related permit is subject also to a recommendation of the Ministry of Economy and Industry. In order to obtain a permit, the requesting business has to demonstrate that the candidate has a special expertise and that local candidates with a similar expertise cannot be found. The salary of foreign employees should exceed a defined threshold, and the employer has to provide them with accommodation and medical insurance.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Israel’s laws for the protection of innovations and inventions are trying to live up to worldwide standards. Trademarks are protected under the Israeli trademark ordinance which was updated in 2010 (Trademarks Ordinance [New Version], 5732–1972) (hereinafter: the “Trademark Ordinance”). Copyrights are protected under the Israeli copyright law, which was updated in 2011 (Copyright Act, 5767–2007) (hereinafter: the “Copyright Act”). Patents are protected under the Israeli patent law, which was updated in 2014 (Patents Law, 5727–1967) (hereinafter: the “Patent Law”). On August 7, 2017, an ultramodern design protection law was published after being approved by the Israeli parliament (Design Law, 5777–2017) (hereinafter: the “Design Law”); most the provisions of this Law came into effect on August 7, 2018. The Commercial Torts Law, 5759–1999 (hereinafter: the “Commercial Torts Law”) is the main Israeli legislation governing the protection of trade secrets. The Unjust Enrichment Law, 5736–1979 provides a separate cause of action in the event that one party benefits at the expense of the other party in an unjust manner. Recently, on January 1, 2019, the Israeli Parliament passed an amendment to the Copyright Act, which enforces intellectual property rights in internet usage and, for the first time, permitted use of works whose owners are unknown or unidentified.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Under Israel’s Patent Law, the creator of an invention is the owner of such invention, unless such invention is developed by an employee as the result of and during the term of the employee’s employment – then, such invention is the property of the employer (and referred to under the Patent Law as “Service Inventions”).

Similar to the Patent Law, the Copyright Act grants the creator of a work the ownership of the work (automatically). Again, the

Copyright Act provides some exceptions to that rule. For instance, in the employment relationship, the default is that the employer shall be the owner of a copyrighted work if the work was made as the result of, and during the term of, the employee’s employment. However, the Copyright Act grants a “moral right”, which refers to the rights of the creator to receive credit over the work and a right that no third party can alter the work in a manner that will damage the work or the creator’s reputation. The moral right is independent from the economic right to the work. Therefore, even if the copyright ownership is transferred to a third party, the moral right remains with the creator.

In the case of trademarks and/or designs, only a registered mark or design in the relevant department of the Israeli Patent Office shall grant the owner the rights and protection against a third party’s claims.

Trade secrets are not registrable. Ownership is mostly governed by case law, and usually is determined according to the entity possessing such business information. The Commercial Torts Law defines trade secrets as business information, which: (i) is not in the public domain; (ii) is not easily discovered or detected by others; (iii) provides to its owners a business advantage over their competitors; and (iv) has been kept secret by its owners using means deemed reasonable under the circumstances.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

Israel is a member of the WTO and the World Intellectual Property Organization (“WIPO”). Israel is a signatory, *inter alia*, to the Berne Convention for the Protection of Literary and Artistic Works, the Universal Copyright Convention (the “Berne Convention”), the Paris Convention for the Protection of Industrial Property, the Patent Cooperation Treaty, as well as the Agreement on Trade Related Aspects of Intellectual Property (“TRIPS”), the Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations, the Nice Agreement Concerning the International Classification of Goods and Services for the Purposes of the Registration of Marks, the Lisbon Agreement for the Protection of Appellations of Origin and their International Registration, the Strasbourg Agreement Concerning the International Patent Classification, the Budapest Treaty on the International Recognition of the Deposit of Microorganisms for the Purposes of Patent Procedure, and the Universal Copyright Convention. The new Design Law includes provisions which will allow Israel to join the Hague Agreement Concerning the International Deposit of Industrial Designs, paving the way for Israeli applicants to file international design applications with WIPO and for foreign applicants to apply for design protection in Israel through an international design application.

Although the international treaties and conventions that Israel is party to do not automatically extend to protect the owner of intellectual property rights under Israeli laws, some rights do extend beyond the borders of Israel. Under the Berne Convention and the Israeli Copyright Act, most copyrights recognised in other modern countries shall be also protected in Israel. The Madrid Agreement Concerning the International Registration of Marks, which Israel is signatory to, provides an entity with an option to register its trademark in a few countries simultaneously.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

Intellectual property can be assigned, licensed (either exclusively or not) or pledged.

Under the Patent Law, the assignment of rights, licensing and/or pledge on patents must be submitted to the Patent Office. To register the assignment or the pledge or the licence, the relevant deed shall be submitted.

According to the new Design Law, the assignment of rights in designs or granting an exclusive licence for such rights must be submitted to the Patent Office. Non-registration means that the assignment of rights or licence is not valid against third parties. The assignment has to be in writing.

According to the Copyright Act, the assignment of copyrights or granting of an exclusive licence for such rights requires a written document.

Under the Trademark Ordinance, the assignment or licensing of rights in trademarks must be submitted to the Trademark Department. This request must include an original deed of assignment.



Ariel Rosenberg

Goldfarb Seligman & Co.
98 Yigal Alon Street
Tel Aviv, 6789141
Israel

Tel: +972 3608 9372
Email: ariel.rosenberg@goldfarb.com
URL: www.goldfarb.com

Ariel Rosenberg heads Goldfarb Seligman's Banking and Finance Practice. Adv. Rosenberg handles all types of financing transactions, domestic and international, and advises on the financing of corporate transactions and on the financing of projects, among others, in the energy, infrastructure and real estate fields.

Adv. Rosenberg specialises in the regulatory aspects and the legal framework of various financial activities, including bank and non-bank financial services, credit and payment cards, payment solutions and Fintech businesses; he also specialises in derivatives and structured financial assets.

Adv. Rosenberg advises regulatory authorities, domestic and foreign banks, credit card companies, payment solution operators and Fintech companies. He also represents Israel's largest companies in negotiations with financing entities.

In addition, Adv. Rosenberg advises international charitable foundations and non-profit organisations on all issues of their activity in Israel.



Sharon Gazit

Goldfarb Seligman & Co.
98 Yigal Alon Street
Tel Aviv, 6789141
Israel

Tel: +972 3710 1661
Email: sharon.gazit@goldfarb.com
URL: www.goldfarb.com

Attorney Sharon Gazit specialises in international corporate and commercial transactions with a dominant technology component. Adv. Gazit advises high-tech and technology companies with respect to their corporate financing, IP commercialisation and other commercial transactions, as well as mergers and acquisitions. In addition, Ms. Gazit serves as legal counsel to several venture funds.

Ms. Gazit has been recognised as a leading partner in the Israeli private equity and high-tech field since its early days. Ms. Gazit has represented a multitude of technology incubators, academic technology transfer offices and research centres.

Ms. Gazit is a member of Goldfarb Seligman's Executive Committee and serves as legal counsel to the IATI (Israel Advanced Technology Industry organisation – the leading organisation in the Israeli technology ecosystem) and also serves as Senior Vice Chair of the Healthcare and Life Sciences Committee of the International Bar Association.



Goldfarb Seligman
Law Offices | Established 1930

Goldfarb Seligman & Co., one of Israel's largest law firms, is among the elite group of firms that deliver top-tier legal services at international standards. The firm, which traces its history back over 80 years, offers clients extensive experience in various fields of law.

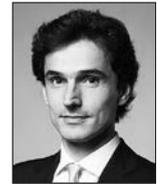
Goldfarb Seligman employs over 250 attorneys, among them over 90 partners, who offer clients a wide spectrum of legal services, including: corporate and capital markets in Israel and abroad; litigation of all types; real estate; taxation; finance; banking and financial services; Fintech; insurance; intellectual property; energy and infrastructure; planning and construction; environmental law; antitrust and competition; regulation; labour law; and more.

At the heart of Goldfarb Seligman's professional philosophy is the belief that every client is unique, with individual issues and considerations. Based on this philosophy, the firm strives to provide each client with comprehensive legal services that are tailored to his or her particular needs.

Italy

BonelliErede

Federico Vezzani



Tommaso Faelli



1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Fintech was in the spotlight in Italy in 2018, and this trend is going to continue in 2019.

The Italian market is considered quite attractive for fintech developers, especially for those who already have a worldwide business.

According to the most recent information, almost 150 fintech companies are based in Italy, and this number continues to grow. Crowdfunding is the largest sub-sector of the fintech industry, with 51 active companies that collected EUR 25 million in the first nine months of 2018, followed by payment services, asset management, blockchain, virtual currencies, insurance and peer-to-peer lending. In particular, the latter sector is materially growing: at the end of the third quarter, the total disbursement (since 2016) of the Italian alternative credit platforms amounted to EUR 948.1 million, an increase of 23.4% compared to the end of June 2018, and 209% compared to September 2017.

The insurance sector has also a significant role and, as a matter of fact, Prima Assicurazioni is the Italian start-up in the insurtech sector that, in 2018, collected the largest investment (equal to EUR 100 million).

Recently, the Bank of Italy conducted a survey of 93 intermediaries operating in the banking sector to understand the role of fintech projects in their business. Out of 283 fintech projects developed by the surveyed intermediaries (for an aggregate amount of approximately EUR 134 million): (a) 122 had already been approved or were under development; and (b) 82 were reported to be already in the execution phase. These projects cover different sub-sectors and primarily concern remote transactions; i.e., client identification and execution of contracts (25%), payment services (23%), supporting technologies (including big data, artificial intelligence and cloud computing; 23%) and automatic services (mainly robo-advice; 16%).

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

In Italy, no specific provisions prohibit or restrict the types of fintech business that a company may carry out. However, the Bank of Italy

has been warning Italian banks (and other supervised entities) over the past few years (following numerous bitcoin scandals) about operating with virtual currencies. European supervisory authorities have also expressed their concern over the growing volume of cryptocurrency transactions in 2018 and 2019 – it is thus reasonable to expect further regulatory action also in Italy, though it is still uncertain whether a RegTech covering all fintech areas is upcoming.

Furthermore, Consob (the government authority of Italy responsible for regulating the Italian securities market) recently published a warning to consumers on the risks of cryptocurrencies. Consob also adopted several measures in 2018 regarding companies that offer investments in cryptocurrencies, including investments through initial coin offerings (ICOs). Specifically, Consob qualified this activity as a public offering of financial products – i.e., financial instruments and any other form of financial investment – without the necessary authorisation.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

Both equity and debt financing can be used by fintech companies to start and develop their business. A useful tool developed in the past few years is issuing so-called mini-bonds that are designed for SMEs and can be traded on a dedicated segment of the Italian stock exchange. In 2018, 198 mini-bonds have been issued and EUR 668 million has been raised by SMEs through these bonds. Crowdfunding can be a form of financing for fintech start-ups and enterprises thanks to the amendment to the relevant regulation approved by Consob at the end of 2017 that enlarged the scope of the said regulation, allowing all SMEs (not just innovative SMEs) to access the crowdfunding channel. Peer-to-peer lending is also accessible to fintech businesses as an alternative to the traditional banking channel. Moreover, fintech start-ups can be financed by venture capitalists belonging to the asset management sector and business angels (that so far are not subject to specific regulation).

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

Italian legislation provides for several measures aimed at supporting investments in research, development and technological innovation:

the main legislation applicable to fintech businesses are (i) the “innovative SMEs and start-ups” regime, (ii) the R&D tax credit regime, (iii) the Patent Box regime, (iv) PIRs, and (v) Hyper-depreciation (*Iperammortamento*). The measure in favour of innovative SMEs and start-ups consists of a vast and diversified package of measures that includes more flexible corporate management tools, tax incentives for investments in innovative SMEs and start-ups (a deduction for income tax purposes of the 40% of the amount invested up to EUR 1 million for individual investors or EUR 1.8 million for corporate investors), liberalisation of remuneration schemes (e.g. work for equity schemes) and facilitation of the access to credit (e.g. equity crowdfunding and access to the SME Guaranteed Fund). The R&D tax credit regime provides for a tax credit, up to EUR 10 million per year, equal to 50% (or 25% depending on the kind of expense) of incremental R&D expenses. The Patent Box regime provides for an exclusion from taxation of 50% of the income arising from the exploitation of certain intangible assets (know-how and patents).

Furthermore, the PIRs provide for a tax exemption (from individual income tax and inheritance tax) in order to encourage individual investors to invest in Italian small and medium enterprises, and the investment must be maintained for at least five years. Moreover, loans granted through peer-to-peer platforms are admissible investments for PIRs, thus benefitting from the relevant favourable tax regime. Hyper-depreciation allows an extra depreciation from 50% to 170% calculated on the acquisition cost of certain high-tech tangible assets (as indicated in a specific list) in relation to digital and technological transformation. In addition, the acquisition cost of certain related intangible assets is also increased by 40% for depreciation purposes.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

A company wishing to launch an IPO on the Italian regulated market must meet the following requirements: a) it must comply with the Italian regulated market rules regarding, among other things, governance, management structure, business prospects, financial requirements and adequate distribution of the share capital among investors; and b) it must publish a prospectus approved by Consob. Start-up companies (i.e., companies that have been in business for fewer than three financial years) are also required to disclose additional information (e.g., profit estimates and forecasts) and to have a Consob-approved prospectus. Companies may also list their shares on a non-regulated market reserved, for professional investors with fewer requirements, to get the admission to trading by Borsa Italiana S.p.A.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

Recently, some notable exits in fintech businesses took place – or are still ongoing – by Italian fintech firms’ founders and/or investors.

In particular, in February 2019 Coinbase Inc., a U.S.-based digital currency wallet and platform, acquired Neutrino, an innovative Italian startup, which created a platform to track cryptocurrency transactions that allows the analysis, investigation and identification of illegal transactions in blockchain.

Furthermore, on 13 February 2019, the shareholders’ meeting and board of directors at Nexi S.p.A. – one of the most important Italian and European providers of digital payments and digital payment acceptance – resolved to launch the company’s initial public offering. The IPO is expected to be completed in April and has an overall value of more than EUR 7 billion.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

Currently, no clear and all-embracing regulatory framework exists for activities falling within the fintech sector. If the fintech company’s business – regardless of the technological means actually used to carry it out – falls within the definition of a reserved activity (thus requiring the authorisation of the competent Italian authority), the company must comply with the relevant requirements for that activity. This was clearly stated by the Bank of Italy with reference to social lending; the Bank of Italy also clarified that social lending transactions executed through online platforms should be limited to a small amount, but did not quantify the value of this amount.

Peer-to-peer lending may also fall within the scope of payment services regulation and thus require the Bank of Italy’s authorisation. Similarly, robo-advice and automated advice tools can be considered investment services, in which case Consob’s authorisation may be required. Furthermore, as mentioned above, Consob issued a specific crowdfunding regulation (Regulation No. 18592 of 26 June 2013, as amended). In this respect, Law No. 145/2018 (“2018 Budget Law”) recently introduced the possibility to also offer debt instruments, on condition that these offers are: (a) made through a separate section on the online portals; and (b) are addressed only to professional investors and other categories of investors specifically identified by Consob. To date, the relevant implementing regulation of the 2018 Budget Law has not yet been published.

In July 2018, the Italian supervisory authority for insurance companies (IVASS) issued a regulation requiring company boards of directors to approve a specific data governance policy, including as concerns data quality and cybersecurity.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

Legislative Decree No. 90 of 25 May 2017 amended Italian AML legislation by introducing a definition of “cryptocurrency” and “cryptocurrency providers” – cryptocurrency providers are thus now required to comply with AML laws.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

Cyber society, big data and technological developments are often included in the agenda of Italian authorities. However, the competent Italian regulators and policymakers have yet to issue an overall regulation in this respect.

In 2016 the Bank of Italy launched the “fintech channel” (*Canale Fintech*), which aims to strengthen the exchange of information between the Bank of Italy and stakeholders wishing to: (a) start a fintech business in Italy; or (b) integrate fintech technology into their existing business. Moreover, following the signing of an agreement between the Bank of Italy and the Italian banking association (ABI), a public-private association named CERTFin was founded to improve the ability of banks and other financial intermediaries to face cybersecurity threats.

In March 2018, the Italian Ministry of Economy and Finance (MEF) established a “coordination committee” following a memorandum of understanding between the MEF, the Bank of Italy, Consob and other national authorities. The purposes of this committee are to: (a) facilitate the introduction of innovative services and models in the financial and insurance sectors; (b) monitor the evolution of fintech; and (c) develop general principles and propose amendments to the current legal framework.

In February 2019, Law No. 12/2019 (that converted into law, with amendments, Decree Law 14 December 2018, No. 135) introduced a definition of distributed ledger technology (DLT) in the Italian legal framework in order to recognise the legal effects of electronic time stamps under Art. 41 of EU Regulation No. 910/2014 to the storage of an IT document in DLTs. To date, no implementing technical standards have been published that set out requirements for DLTs to ensure these legal effects. Nonetheless, this new law marks a significant step forward in the development of blockchain technology in Italy.

Furthermore, IVASS and other scientific and industrial partners have promoted an insurance blockchain sandbox that allows insurance companies and brokers to test products, services, processes, business models and distribution models in the real market with real stakeholders. Participation is based on the single use case to be developed, on condition that the use case is: (a) innovative; (b) blockchain-based; and (c) directly and indirectly beneficial to consumers.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

If a company is established in the EU, it can carry out its activity through a branch or under the freedom to provide services in the EU. If the company is an EU-supervised entity that carries out a reserved activity, the general rules of the home country apply (together with specific Italian rules if a branch is incorporated). One of the main regulatory hurdles to overcome for non-EU companies carrying out reserved activities is obtaining the necessary administrative authorisations. Specifically, in the wake of MiFID II, stricter rules apply to non-EU companies providing financial services. However, new provisions have been introduced for non-EU companies providing financial services, and indeed they can now provide investment services in Italy without authorisation if the services are provided at the exclusive initiative of the client (i.e., reverse solicitation).

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

GDPR and Legislative Decree No. 196 of 30 June 2003 (“Data Protection Code” or “DPC”) set out the rules for fair data processing. The main principles of legality, necessity, proportionality and transparency entail that processing must be reduced to the minimum extent possible and involve only data relevant to its scope, and preceded by an information notice to the data subjects.

To lawfully process personal data, consent of the data subjects is not required in specific cases, such as when processing is necessary to comply with legal or contractual obligations, or to exercise a right. Nor is consent necessary when the processing is based on a data controller’s legitimate interest. Consent of the data subjects is instead normally necessary when direct marketing for profiling is envisaged, except, obviously, for cases in which profiling is required by law (for example, pursuant to the MiFID Directive or anti-money laundering legislation).

Limitations and conditions apply to the agreements with outsourcers (including cloud-based service providers) who must be appointed as data processor through a specific agreement pursuant to Art. 28 GDPR.

In addition, the Italian Data Protection authority issued Guidelines for the Banking Sector providing, *inter alia*, for strict regulation of credit-score databases, modalities and time limits for the collection and preservation of log files regarding banking transactions.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

GDPR applies to the processing activities by a controller or processor not established in the EU, where the processing activities are related to:

- (a) the offering of goods or services to data subjects in the EU; or
- (b) the monitoring of their behaviour as far as their behaviour takes place within the EU.

Sharing data outside the EU is subject to, alternatively: a) certification by a US company to the EU-US Privacy Shield, if the entity receiving the data is US-based; b) adoption of model clauses for the data transfer in a non-EU country, approved by the EU Commission; c) adoption of Binding Corporate Rules; d) consent of the data subjects; e) performance of contractual obligations; f) important reasons of public interest; g) the establishment, exercise or defence of legal claims; and h) the protection of vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent. Sharing data outside the EU is also allowed when the transfer is made from a register legally intended to provide information to the public and open to consultation. The data controller’s legitimate interest may be a basis for transfer of data outside the EEA only if the transfer is not repetitive, concerns only a limited number of data subjects and the data controller informs the Italian DPA.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

The Italian DPA may issue blocking orders of non-compliant personal data processing (and therefore prevent further use of the data), injunctions to comply with any aspect of data processing laws (including to satisfy data subjects’ legitimate requests) and administrative fines, as provided by GDPR (and thus fines up to EUR 20 million, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher).

Criminal sanctions (imprisonment for up to six years in the most severe cases) apply in different cases, most of which require that there is gain or intent to cause harm. Other hypotheses regard: a false declaration to the DPA; the infringement of dispositions regarding the processing of particular categories of data; and the infringement of dispositions regarding employees’ monitoring.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

Legislative Decree No. 65/2018 (implementing EU Directive No. 2016/1148 – so-called “NIS Directive”) sets forth certain specific cybersecurity requirements and obligations which could be applicable to banks, financial intermediaries and payment institutions in general (e.g. technical and organisational measures for network and information system security, and notification of cybersecurity incidents to the authorities under certain circumstances).

Moreover, GDPR and DPC impose the implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risk of data processing.

The Italian criminal code also sets forth specific computer crimes, such as computer fraud or unlawful access to a third-party IT platform.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

A fintech business requires authorisation from the competent national authorities if its activity falls within the scope of a reserved activity (e.g., banking, payment services or financial services). Carrying out a reserved activity without the relevant authorisation is a criminal offence and may result in the application of criminal sanctions.

As mentioned above, Legislative Decree No. 90 of 25 May 2017 introduced a definition of “cryptocurrency” and “cryptocurrency providers” (i.e., those who provide currency exchange services between virtual currencies and legal currencies). Thus, from an AML regulation perspective, cryptocurrency providers must now enrol in a specific register and comply with AML duties, including know-your-customer duties, suspicious transaction reporting and transactions record keeping. Failure to comply with relevant AML regulation may result in an administrative or criminal sanction (depending on the offence committed).

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

We have addressed all regimes from a regulatory, IP, privacy, labour and tax perspective in other sections of this chapter.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

To hire employees in Italy, the employer must register with the National Institutes of Social Insurance (INPS) and Accident Insurance (INAIL) and inform them and the competent Labour Office of the execution of each employment contract before starting. Employees are divided into four categories: blue-collar; white-collar; high-ranking white-collar; and executives, and can be hired under open-ended or fixed-term contracts (max. 24 months). The

employment is regulated by law, national collective bargaining agreements (NCBAs – if applied) and individual contracts. To dismiss an open-ended employee, the employer must:

- (i) fulfil specific formal requirements; and
- (ii) find grounds for dismissal for specific reasons (misconduct and gross negligence, breach of contract, economic reasons). If the dismissal is fair, the employee is entitled to a notice period (not due for “just cause” dismissals). Only in exceptional cases (discriminatory dismissal or total absence of the breaches), the unfair dismissal leads to the employee’s reinstatement in the workplace. In all other cases, the employee could be entitled to an indemnity, up to 36 monthly salaries (depending on the employee’s hiring date and other factors).

5.2 What, if any, mandatory employment benefits must be provided to staff?

Terms and conditions of employment are in principle left to the parties’ negotiation. However, individual employment contracts cannot derogate from the mandatory provisions provided by law (and by the NCBA, if applied). The law provides mandatory rules for various subjects, e.g. changes to the employee’s tasks and place of work, minimum period of holidays and paid/unpaid leave, sickness leave during which the employer cannot dismiss the employee, maximum daily, weekly and annual working hours, length of notice period in case of dismissal, protection in case of unlawful dismissal, etc.). An NCBA regulates almost all aspects of the employment relationship, and its provisions are, generally speaking, more favourable to employees than provisions under law (providing, for example, longer holidays and additional health insurance). For this reason, applying an NCBA results in increased costs for the employer. Nevertheless, NCBAs are actually applied by companies on a voluntary basis (since it makes the management of the employment contracts more comfortable).

In any case, the employer must grant at least the minimum wage set by the NCBA (even if not applied). The remuneration is subject to social security contributions due to INPS, amounting to approximately 38% of the employee’s income (approximately 29% of which is borne by the employer and 9% by the employee), in order to accrue pension treatments. Italian law also provides a mandatory end-of-service allowance (TFR) payable to the employee on termination (for whatever reason) of the employment, which corresponds to 7.4% of the total remuneration earned, and must be accrued year-by-year by the employer.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

Foreign employees can be seconded to an Italian entity or directly employed by it. Employees who work in Italy, in accordance with the principle of territoriality, must pay social contributions to INPS (with exceptions provided by European law under certain requirements). No visa or work permits are required for EU citizens. With reference to the financial sector, companies must comply also with European laws concerning the remunerations of the financial sector’s managers (implemented by the Bank of Italy) which provide specific requirements.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Legislative Decree No. 30 of 10 February 2005 (“Industrial Property Code” or “IPC”) and Law No. 633 of 22 April 1941 (“Copyright Law”, as subsequently amended) set forth rules for protecting, defending and enhancing intellectual property rights. In particular, innovations and inventions are protected by:

- (i) Patents, under the common requirements (novelty, inventive step and industrial applicability) for 20 years from the filing date. Innovative software programs, which are likely to flourish in the fintech industry, can be patented only if technical effects can be demonstrated according to the EPO’s guidelines on software patentability; otherwise, software programs are eligible for protection under copyright law, which only covers the code and not the logic behind them. Standard essential patents (SEPs), which frequently regard communications and transactions based on digital technologies, can be enforced only if a licence under Fair, Reasonable and Non-Discriminatory (FRAND) terms was refused by the alleged infringer.
- (ii) Trade secrets, either of a technical or commercial nature, if the information is secret in that: (1) it is not generally well-known or easily accessible by experts in the field; (2) it has an economic value because it is secret; and (3) it is subject to reasonable measures to keep it secret. Trade secret protection provides for the same remedies and sanctions as IP. Directive EU 2016/943 on the protection of undisclosed know-how and business information, which will likely lead to a detailed regulation of specific aspects but will not change the main legal framework, is going to be implemented in Italy.

Italian law also provides for measures against unfair competition, such as slavish imitation, passing off, disparagement, boycotting, employee raiding, misleading advertising and abuse of privileged information.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Ownership of IP rights is generally obtained through a registration process. As to patents, three effective patent protection schemes are

available in Italy: national patents; European patents (classical and with unitary effects as soon as the UPC agreement enters into force); and international patents under the Patent Cooperation Treaty (PCT). Trademarks have a similar registration process. Trade secrets and copyright are, on the contrary, not subject to registration and ownership results from the creation of the work or innovation.

Ownership of IP rights is vested in whomever has funded and commissioned the creation of the intangibles. Therefore, IP rights are owned by the employer (not the employees) or the client (not the provider or contractor) unless otherwise provided by the parties.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

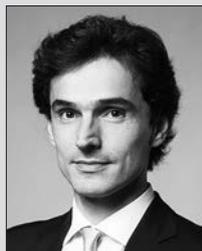
Ownership of local rights are required to protect or enforce IP rights, although there are EU rights or international registrations, patents and designs which can be protected also in the Italian territory, as long as Italy was designated in the application. Creative works, including software, published outside Italy are eligible for copyright protection depending on the country where the work was first published (provided that this country grants equivalent protection to the works of Italian authors, and within the limits of such equivalence). Italy is also a party to the Berne Convention.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

IP rights (except for trademarks) can be exploited through direct use, which makes the turnover incidental to those IP rights eligible for tax benefits under the Patent Box regime, or licensing, which generates a royalty flow equally eligible for the Patent Box regime’s fiscal benefits.

Big data sets can be exploited through data analytics to create predictive models, which can then be used or sold, provided that certain requirements under data protection law are met.

Security interests over IP rights can be created as a guarantee in the framework of financial operations.



Federico Vezzani

BonelliErede
Via Michele Barozzi
1-20122 Milan
Italy

Tel: +39 0277 1131
Email: federico.vezzani@belex.com
URL: www.belex.com

Federico (partner since 2015) advises both financial institutions (banks, financial intermediaries, insurance companies and asset managers) and non-regulated firms on the Italian and EU financial regulatory aspects of a broad range of matters and projects, including:

- innovation in the fintech sector;
- new capital issuances;
- complex funding structures;
- transactional structuring to achieve regulatory capital efficiencies;
- asset management;
- payment services;
- securities laws; and
- market conduct issues.

Federico has considerable experience in equity and debt capital market transactions, as well as in the asset management sector.



Tommaso Faelli

BonelliErede
Via Michele Barozzi
1-20122 Milan
Italy

Tel: +39 0277 1131
Email: tommaso.faelli@belex.com
URL: www.belex.com

Tommaso (partner since 2012) was admitted to the Italian Bar in 2002 and is also admitted to practise before the Italian Supreme Court.

Tommaso assists both Italian and multinational companies in contentious and non-contentious matters relating to IP, unfair competition and IT (specifically, licence and software development agreements, application management and outsourcing), e-commerce, data protection and privacy, with a specific emphasis on profiling issues and data management in technology partnerships and joint ventures based on the Internet of Things and big data, in addition to direct marketing, data transfer abroad and internal auditing.

Since 2005, Mr. Faelli has been an adjunct professor of IP law at the Faculty of Law at the University of Como.

In 2007, he obtained a Ph.D. in commercial law – IP and competition from the University of Parma.

Tommaso is a lecturer for a Master's course in IP and cyberrisk.

BonelliErede

BonelliErede is one of the largest independent law firms in Italy, with offices in Milan, Rome, Genoa, Brussels, London, Cairo (in cooperation with Bahaa-Eldin Law Office), Addis Ababa (in cooperation with Tameru Wondm Agegnehu Law Office), Dubai, Frankfurt (in cooperation with Hengeler Mueller) and Beirut (as part of the integration of the law firm Tribonian Law Advisors).

It offers a full range of commercial legal services, combining business acumen with academic excellence. BonelliErede is not only a leading law firm in Italy, but also a successful independent international law firm; an essential part of its international strategy is to forge relationships with a wide number of other distinguished independent law firms in Europe and worldwide.

BonelliErede comprises 73 partners, five local partners, 15 of counsel and more than 380 associates supported by about 190 staff employees. Among its lawyers, it boasts 15 university professors.

Japan

Ken Kawai



Kei Sasaki



Anderson Mōri & Tomotsune

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

In Japan, cryptocurrency-based businesses, cashless payment or mobile payment services, financial account aggregation services, robo-advisors and crowd funding are relatively active. Meanwhile, innovation of peer-to-peer lending and insurtech has yet to come.

What was notable in 2018 was that an increasing number of companies entered into or expanded their businesses in the mobile payment market. It is often stated that the Japanese highly prefer cash and that the ratio of cashless payment is much lower than in other major countries. According to the report “Cashless Vision and API Guidelines for Utilization of Credit Card Data” released by the Ministry of Economy, Trade and Industry (the “METI”) in April 2018, the ratio of cashless payment in Japan was less than 20% in 2015. However, in 2018, quite a few companies launched QR code payment services and they are currently facing great competition. Fintech ventures such as Origami and PAY and IT platforms such as Rakuten, Line, Yahoo and NTT Docomo have already launched QR Code payment services. It is also reported that traditional banks, including “Mega Banks”, are in preparation to standardise the use of QR Codes, and will launch “BankPay” in 2019.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

There are, at present, no prohibitions or restrictions that are specific to fintech businesses in Japan. Certain types of cryptocurrency-based business are regulated (*see* question 3.2), but these businesses can be carried out in compliance with applicable regulations.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

The methods of funding for new companies would vary depending upon the stages they are in: (i) seed stage; (ii) start-up stage; (iii)

early growth stage; and (iv) sustained growth stage. In seed or start-up stage, the founder’s own savings and borrowings and/or capital injection by the founder’s family and friends are commonly utilised. Funding through bank loans tends to be difficult in these stages. The Japan Finance Corporation and municipalities provide certain lending systems to support start-ups up to a certain maximum amount. Angel investors also provide equity capital. In early growth stage to sustained growth stage, funding by bank loans or venture capital will more likely be available. Crowd funding is also available in every stage. Meanwhile, initial coin offerings (“ICOs”) are not popular among fintech companies in Japan because an issuer must first be registered with the Financial Services Agency (the “FSA”) before it can conduct an ICO.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

- The Japanese tax system provides angel investors with the following tax incentives: (i) reduction of income tax (the amount invested in a target company, which has not made a profit in three years from its establishment, will be deducted from the gross income); or (ii) reduction of the capital gains from the transfer of shares in the target company (the amount invested in a target company which is less than 10 years old will be deducted from the capital gains).
- The research and development tax incentive system has been adopted and is often revised with the aim of maintaining and strengthening initiatives, which supports Japan’s global competitiveness.
- Unlike some European countries, the patent box scheme (which allows companies to apply a lower rate of corporate tax to profits earned from patented inventions) has not been adopted by the tax system, though the adoption has been continuously proposed by Japanese industries.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

Tokyo Stock Exchange (“TSE”) operates five equity markets: (i) the First Section; (ii) the Second Section; (iii) Mothers; (iv) JASDAQ; and (v) Tokyo PRO Market. There are two types of requirements (“Listing Requirements”): “Formal Requirements”; and “Eligibility Requirements”. The Formal Requirements include: (i) the number of shareholders as of the listing day; (ii) the number of tradable shares; (iii) the market capitalisation of tradable shares; (iv) the ratio of

tradable shares to listed shares; (v) public offering; (vi) market capitalisation of listed shares; and (vii) number of consecutive years of business operation, among others. The Eligibility Requirements include: (i) appropriateness of the disclosure of corporate information, risk information, etc.; (ii) soundness of corporate management; (iii) effectiveness of corporate governance and internal management system of an enterprise; (iv) reasonableness of the business plan; and (v) other matters deemed necessary by TSE from the viewpoint of the public interest or the protection of investors.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

In June 2018, Mercari Inc, the online marketplace or “flea market app” provider, raised approximately 1.2 billion dollars with its IPO. Its shares are listed in TSE’s Mothers market. The company was founded in 2013 and quickly became the country’s default online marketplace for selling and buying used goods. The company has a subsidiary named Merpay, which provides mobile payment apps that can be used for settlement not only in Mercari’s marketplace but also in various shops nationwide.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

Apart from the regulations applicable to cryptocurrency exchange services and electronic payment intermediate services, there is no specific regulatory framework for fintech businesses. If the services provided by the fintech companies are subject to existing financial regulations, they are required to comply with these regulations, which include obtaining applicable authorisation (licence or registration). A firm (including an overseas firm) that wishes to undertake regulated activities in Japan is required to obtain applicable authorisation from Japanese financial regulators, the FSA or one of the Local Financial Bureaus that the FSA has delegated a part of its authority to. Please note that if an entity conducts solicitation in Japan for using its services, even if this is done from abroad, such act is basically considered as an undertaking of activities in Japan.

Money transfer services are regulated under the Banking Act and acts applicable to other depository institutions, which require those who wish to enter into this business to obtain the relevant licence from the FSA. However, the service of a money transfer of not more than JPY 1 million can be provided if a firm obtains registration as a “Funds Transfer Service Provider” under the Payment Services Act (“PSA”).

For e-money, the issuer of e-money must comply with applicable rules under the PSA. If e-money can be used only for the payments to the issuer for its goods or services, the PSA does not require the issuer to obtain registration, provided that they comply with some reporting obligations. Meanwhile, if e-money can be used not only for the payments to the issuer for its goods or services but also for payments to other entities designated by the issuer, then the issuer is required to obtain registration as an “Issuer of Prepaid Payment Instruments” under the PSA.

Please note that an online payment instrument can be considered either as a “Funds Transfer” system, a “Prepaid Payment Instrument”, a “Virtual Currency” or something else. As the bounds of each definition are not easy to distinguish, a consultation of specialists is recommended if an entity wishes to undertake business related to online payments in Japan.

On June 1, 2018, the amendment to the Banking Law came into force to regulate Electronic Payment Intermediate Service Providers and facilitate open API. Electronic Payment Intermediate Service Providers are defined broadly enough to include intermediaries between financial institutions and customers, such as entities using IT to communicate payment instructions to banks based on entrustment from customers, or entities using IT to provide customers with information about their financial accounts held by banks. Entities providing financial account aggregation services are also categorised as Electronic Payment Intermediate Service Providers. They are required to register with the FSA in order to provide these services.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

Regulations on cryptocurrency came into force on April 1, 2017. The PSA was amended to introduce registration requirements for “Virtual Currency Exchange Service Providers”. For purposes of the PSA, “Virtual Currency” is defined as:

- (i) proprietary value that may be used to pay an unspecified person the price of any goods purchased or borrowed or any services provided, where such proprietary value may be (a) sold to or purchased from an unspecified person, provided such sale and purchase is recorded on electronic or other devices through electronic means, and (b) transferred through an electronic data processing system; or
- (ii) proprietary value that may be exchanged reciprocally for such proprietary value specified in the preceding item with an unspecified person, where such proprietary value may be transferred through an electronic data processing system.

Most of the so-called payment tokens and utility tokens would fall within the definition of Virtual Currency.

Virtual Currency Exchange Services have been defined to include any of the following acts carried out as a business:

- (i) the sale/purchase of Virtual Currency or exchanges for other Virtual Currency;
- (ii) intermediary, agency or delegation services for the acts listed in (i) above; or
- (iii) the management of users’ money or Virtual Currency in connection with the acts listed in (i) and (ii).

As a consequence of this definition, not only typical cryptocurrency (Virtual Currency) exchanges, but also so-called OTC brokers, are regulated as Virtual Currency Exchange Service Providers under the PSA. Moreover, most ICOs or token sales fall within the definition of Virtual Currency Exchange Services. As a result, a token issuer must, as a general rule, be registered as a Virtual Currency Exchange Services Provider if the token sale (i.e. the ICO) is targeted to residents in Japan. Notwithstanding the foregoing, it has been argued that a token issuer does not need to undergo registration as a Virtual Currency Exchange Service Provider if the issuer has completely outsourced its token issuance to a reliable ICO platform provider that is registered as a Virtual Currency Exchange Services Provider.

With regard to so-called security tokens, a different rule would be applicable. Where distributions are paid to token holders on the profits of the business conducted by the token issuer, and calculated based on the ratio of the holder’s token ownership, the token involved may constitute equity interest in an investment fund (i.e. a collective investment scheme) and subject the token issuer to the provisions of the Financial Instruments and Exchange Act (the “FIEA”), which primarily regulates securities. In short, a security token issuer is required to comply with the same regulations applicable to a traditional investment fund.

It should be noted that the legal framework regulating cryptocurrencies or cryptoassets will likely change significantly in 2019 and 2020. In December 2018, the FSA Study Group on Virtual Currency Exchange Services published a comprehensive report which made recommendations of introducing new rules on cryptocurrencies or cryptoassets. The report mainly discussed: (i) enhancing requirements for Virtual Currency Exchange Service Providers; (ii) new regulations on unfair trading of Virtual Currencies; (iii) introducing registration requirements on Virtual Currency custody business; (iv) introducing regulations on Virtual Currency derivatives transactions; and (v) introducing new regulations on security token offerings and utility token offerings. The report also indicated that the defined legal term should be changed from “Virtual Currency” to “Cryptoasset” in light of the fact that the term “Cryptoasset” has gained popularity in recent international discussions, and that the term “Virtual Currency” may be likely to cause a misconception that it is legal tender. At the time of writing, the bill to amend the PSA and the FIEA to introduce such new regulations has yet to be published, but the bill may be submitted to the Diet in Q1 2019, and pass the Diet in Q2 2019.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

Yes. Financial regulators and policy-makers in Japan are receptive to fintech innovation and technology-driven new entrants in the regulated financial services markets. Please note, however, that the FSA is taking a more conservative approach than before to cryptocurrency-based businesses. Meanwhile, the METI has been supporting the blockchain industry. For instance, it hosted the Blockchain Hackathon in February 2019 to embark on the social implementation of blockchain technologies.

In June 2018, the Headquarters for Japan’s Economic Revitalization, under the Cabinet Secretariat, opened a cross-governmental one-stop desk for the regulatory sandbox in Japan (the “Regulatory Sandbox”) within the Japan Economic Revitalization Bureau. The Regulatory Sandbox can be used by Japanese as well as overseas companies, and it enables companies that apply and receive approval for projects not yet covered by present laws and regulations to carry out a demonstration under certain conditions without the need for legal amendment. There is no limitation of the area of business which can apply for the sandbox, though in its basic policy, AI, IoT, big data and blockchain projects are explicitly mentioned as the most prospective and suitable areas.

The FSA established a “Fintech Experiment Hub” in September 2017. The Hub gives support to fintech companies and financial institutions when they conduct unprecedented PoC. Please note that certain regulations are not suspended during the PoC, but the Hub aims to eliminate companies’ concerns of violating applicable regulations during the PoC by the giving of legal and other advice.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

If an overseas fintech company wishes to perform regulated activities in Japan, it is required to obtain the same authorisation or registration as Japanese companies. It is important to note that a

fintech business only based overseas which deals with customers in Japan is likely to be viewed as carrying out activities in Japan. In some cases, a fintech business established in another jurisdiction that wishes to provide its service to residents in Japan will be required to establish a branch office or a subsidiary in Japan to obtain such authorisation.

Considering the above, it is important for an overseas fintech company wishing to enter the Japanese market to consult with its Japanese legal advisor on whether the authorisation or registration is required under Japanese law.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

Yes, the Act on the Protection of Personal Information (the “APPI”) is a principle-based regime for the processing and protection of personal data in Japan. The APPI generally follows the eight basic principles of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The Act is applicable to all private businesses including fintech businesses. In September 2015, the amendment to the APPI was promulgated and was fully implemented on May 30, 2017. The key amendments include: (i) the revision of the definition of “Personal Information” and introduction of the definition of “Sensitive Personal Information”; (ii) setting rules for the utilisation of de-identified information; (iii) the establishment of the Personal Information Protection Commission (the “PPC”); and (iv) setting restrictions on transferring personal data to foreign jurisdictions.

Under the APPI, the PPC and other government ministries are to issue administrative guidelines that are applicable to specific industry sectors under their supervision. Fintech businesses should comply with the “Guidelines on Personal Information Protection in the Financial Industry” issued by the FSA.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

Prior to the amendment, the APPI was applicable to any act involving personal information that was performed in Japan. In this sense, it was widely considered that the APPI did not have extraterritorial reach. However, the amended APPI is applicable to certain acts that are performed in a foreign country. More specifically, many of the provisions of the amended APPI are applicable to the owner of personal information regardless of the owner’s location, if the owner uses or processes personal information of an individual in Japan that is acquired in connection with the provision of goods or services to the individual. Before the implementation of the amendment, the APPI did not restrict the international transfer of data. Under the amended APPI, however, personal data may not be transferred to any third party in a foreign country, in principle, without the consent of the person concerned. This restriction does not apply if a receiving third party is located in a foreign country that has personal data protection systems comparable to those in Japan, or if the receiving third party takes necessary measures to protect personal data comparable to the measures that should be taken by an entity under the APPI.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

Criminal sanctions may be applicable for failing to comply with the APPI. Criminal sanctions include imprisonment or a criminal fine. If a breach is committed by an officer or an employee of a judicial entity, the entity itself may also be subject to a criminal fine.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

In November 2014, the Basic Cybersecurity Act was enacted, which is a basic framework law for cybersecurity. Under this Act, the Japanese government must take measures for the implementation of cybersecurity policies including legislative, financial or taxation measures. Currently, there are several laws and regulations in Japan that can be used to tackle cyber-crimes, including, among others, the Unfair Competition Prevention Act, the Unauthorised Computer Access Prevention Act, the APPI and the Penal Code.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

The Act on Prevention of Transfer of Criminal Proceeds is the key anti-money laundering legislation in Japan (the “APTCP”). The APTCP requires financial institutions and other business entities specified in the Act (“Specified Business Entities”) to adequately verify the identity of its customer upon commencement of certain types of transactions (“Specified Transactions”). If a fintech business is included in the scope of the Specified Business Entities, it must perform such verification. Most financial institutions including Funds Transfer Service Providers and Virtual Currency Exchange Service Providers are specified as Specified Business Entities under the APTCP, while Issuers of Prepaid Payment Instruments are not. The Specified Transactions vary depending on the Specified Business Entities. If a transaction falls within certain high-risk categories, the APTCP requires the Specified Business Entities to conduct enhanced customer due diligence.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

There is no other legislation in Japan which specifically covers the fintech sector. Any additional relevant regulations would likely be specific to the sector in which a particular fintech business operates.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

In regards to either hiring or dismissal, it should be noted that, under Japanese law, employers are prohibited from discriminating against employees with regard to wages, working hours and any other terms of employment because of nationality, creed and social status. With respect to hiring, there are two types of employment contracts in Japan – (i) those with a definite term, and (ii) those with an indefinite

one. As a general rule, the term of a definite term employment contract shall not exceed three years. There are exceptions to this rule, such as those that apply to employees that have special knowledge or expertise that the company is particularly looking for. Please note that, unless there is an objectively justifiable cause for non-renewal, and such non-renewal is socially acceptable, a definite term employment contract will be, upon the employee’s request made on or prior to the expiration date thereof, deemed renewed as an employment contract with an indefinite term under the same terms and conditions of employment if a certain condition is met. Please also note that a definite term contract employee whose contract periods total over five years by renewal may convert the employment contract to an indefinite term employment contract by making such request to the employer.

With respect to unilateral dismissal, where an employer terminates the employment contract unilaterally against the employee’s will, the employer must give the employee at least 30 days’ prior notice to be dismissed, or alternatively, make payment of the average wage *in lieu* of the notice. Generally speaking, it is considerably difficult for any employer in Japan to unilaterally dismiss an employee. The employer must abide by the rule that a dismissal shall, where the dismissal lacks objectively reasonable grounds and is not considered to be appropriate in general societal terms, be treated as a misuse of that right and is thus invalid. Please also note that, in case of dismissal as a means of employment adjustment (i.e. collective redundancies), the following four requirements shall all be satisfied: (i) necessity of reduction; (ii) effort to avoid dismissal; (iii) rationality in selection of target employees; and (iv) procedural appropriateness. Given the difficulty of dismissal, employers find it more practical to sometimes offer certain monetary packages to induce employees to voluntarily resign.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Employers are required to pay at least the minimum wages stipulated by the law. As general rules: (i) the wage must be paid at least monthly on a particular date; (ii) the payment must be in cash, in Japanese Yen; (iii) no amount can be deducted from the wage; and (iv) the wage must not be paid to anyone other than the employee.

Employees are entitled to take at least one statutory holiday a week. The maximum working hours cannot exceed eight hours a day or 40 hours a week. An employer must give all employees that have worked 80% or more of the designated workdays in the preceding year a certain number of days of annual leave. In order to have employees work overtime or work during holidays, the employer is required to: (i) execute an employee-employer agreement in writing on such overtime work with the labour union which represents a majority of employees or, if such union does not exist, with an employee who represents a majority of employees; and (ii) refer to the possibility of overtime work and work on statutory holidays in the Rules of Employment in advance. An employer is, in general, required to have the following two types of insurance for its employees: (i) Labour Insurance (Workers’ Compensation Insurance and Unemployment Insurance); and (ii) Social Insurance (Health Insurance and Welfare Pension Insurance).

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

For foreign workers to visit and work in Japan, a highly skilled professional visa or working visa is necessary. Under the Japanese

points-based system, foreign nationals recognised as “highly-skilled foreign professionals” will be given preferential immigration treatment. There are three categories of activities of highly-skilled foreign professionals: (i) advanced academic research activities (activities of engaging in research, research guidance or education based on a contract entered into with a public or private organisation in Japan); (ii) advanced specialised/technical activities (activities of engaging in work requiring specialised knowledge or skills in the field of natural sciences or humanities based on a contract entered into with a public or private organisation in Japan); and (iii) advanced business management activities (activities of engaging in the operation or management of a public or private organisation in Japan). The preferential treatment includes (i) permission for multiple purposes of activities, and (ii) a grant of a five-year period of stay, and so forth.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Fintech, or technology related to finance, may be protected by a patent or copyright. A patent is granted for inventions that are “highly advanced creations of technical ideas utilising the laws of nature” and that are industrially applicable. For instance, a patent may be granted for computer software as either an invention of a product or an invention of a process, provided that it involves hardware control or process-using hardware. The mathematical algorithm itself is not patentable. Business methods themselves are not patentable; however, a patent may be granted for business methods which are combined with computer systems or other devices. Productions in which thoughts or ideas are expressed in creative ways (and which fall within the literary, scientific, artistic or musical domain) are protected by copyright as “works”. Databases which constitute creations by means of selection or systematic construction of information contained therein are protected as independent works. Computer programs may be protected as works if the way in which the instructions to the computer are expressed constitute creations.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Under Japanese patent law, a patent for an invention is owned by the inventor. Only a natural person can be the inventor originally entitled to filing a patent for the invention. For an invention created by an employee, the right to obtain a patent may be assigned to an employer in accordance with the rules established by the employer, and said employer may file the patent application as the applicant to

the extent that the employer reasonably compensates its employee. The process for determining “reasonable value” may often be clarified in an agreement or Rules of Employment. In the case where the amount to be paid in accordance with the provision on “reasonable value” is found to be unreasonable, or where no provision setting forth the method for calculation exists, the amount of the “reasonable value” shall be determined by the court in light of the amount of profit to be received by the employer from the patent, the employer’s burden and contribution to the invention, its treatment of the employee and any other circumstances relating to the invention. The authorship of a work which is created by an employee during the performance of their duties for their employer is attributed to the employer. An author fundamentally obtains the moral rights of author as well as the copyright. The moral rights of the author include the right to make the work public, the right to determine the indication of the author’s name and the right to maintain integrity. The moral rights of the author are personal and exclusive.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

IP rights are territorial rights in principle. On the other hand, Japan has adopted the Paris Convention for the Protection of Industrial Property, the Patent Cooperation Treaty, the Patent Law Treaty and the WIPO Copyright Treaty. In accordance with these treaties, foreign IP rights may be protected in Japan.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

IP may be exploited or monetised through: (i) assignment; (ii) grant of security interest; or (iii) licence. Depending upon the IP right involved, the formalities of these transactions are different. Rights in registered patents can be assigned to any party upon registration of the assignment. Copyright and neighbouring rights can be assigned through an agreement, without registration; however, registration is necessary to perfect the assignment. Rights in registered patents can be pledged for the benefit of any party upon registration, which is required in order for the pledge to be valid and enforceable. Copyright and neighbouring rights can be pledged for the benefit of any party by an agreement without registration, although the pledge can still be registered in order to perfect the agreement. Exclusive and non-exclusive licences to intellectual property rights are effective upon the creation of an agreement between the right holder and a licensee.

**Ken Kawai**

Anderson Mōri & Tomotsune
Otemachi Park Building, 1-1-1 Otemachi
Chiyoda-ku
Tokyo 100-8136
Japan

Tel: +81 3 6775 1205
Email: ken.kawai@amt-law.com
URL: www.amt-law.com/en

Ken Kawai has extensive experience advising financial institutions, fintech startups, investors and corporate clients on complex finance and financial regulatory matters. Ken focuses primarily on the fintech industry and regularly advises fintech companies, financial institutions, international organisations and industry organisations on legal issues surrounding fintech, including the complex legal framework governing cryptocurrencies, initial coin offerings and blockchain.

Ken also specialises in derivatives and has counselled global banks, broker-dealers and investors on regulatory matters and best practices with respect to derivatives and related products. Ken's deep and practical knowledge in this area is rooted in his 17-year career at MUFG Bank, Ltd. (formerly known as the Bank of Tokyo-Mitsubishi and, prior to that, the Bank of Tokyo Ltd.), where he was involved in derivatives trading and marketing.

**Kei Sasaki**

Anderson Mōri & Tomotsune
Otemachi Park Building, 1-1-1 Otemachi
Chiyoda-ku
Tokyo 100-8136
Japan

Tel: +81 3 6775 1140
Email: kei.sasaki@amt-law.com
URL: www.amt-law.com/en

Kei Sasaki offers a wide range of legal services, including: (i) international and domestic tax advice; (ii) advice on financial transactions such as banking, structured finance and project finance; (iii) financial regulations; and (iv) energy and resources. Kei's practice area is expanding to fintech business advice, including structuring and registration in relation to prepaid payment instruments and cryptoasset matters such as ICOs or Virtual Currency Exchanges Business in Japan.

ANDERSON MŌRI & TOMOTSUNE

Anderson Mōri & Tomotsune is among the largest and most diversified law firms in Japan offering full corporate services. Our flexible operational structure enables us to provide our corporate clients with effective and time-sensitive solutions to legal issues of any kind. We are pleased to serve Japanese companies as well as foreign companies doing business in Japan. In response to the increasingly complex and varied legal needs of our clients, we have grown significantly, augmenting both the breadth and depth of expertise of our practice. Our principal areas of practice consist of Corporate, M&A, Capital Market, Finance and Financial Institutions, Fintech, Real Estate, Labour and Employment, Intellectual Property/Life Sciences/TMT, Competition/Antitrust, Tax, Energy and Natural Resources, Litigation/Arbitration/Dispute Resolution, Bankruptcy and Insolvency/Restructuring, International Trade and International Practice (China, India, Asia, US, EU and others).

Kenya

Sonal Sejpal



Anjarwalla & Khanna

Dominic Rebelo



1 The Fintech Landscape

- 1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).**

Kenya continues to experience a surge in investments in fintech businesses driven mainly by the penetration of mobile telephony and the receptiveness to innovations in the technological arena. The MPESA mobile money transfer platform, first piloted by Vodafone through Safaricom in Kenya in 2007, has enabled significant financial inclusion and acted as a stimulus for the establishment of other fintech businesses. These fintech businesses include: mobile banking; mobile lending and savings; fundraising platforms; mobile payment systems; and insurance.

Other notable fintech businesses which have developed include peer-to-peer lending and payment platforms, business-to-business lending and payments platforms, online payment systems, online trading, aggregation and international remittance businesses, online foreign exchange platforms, online procurement, online betting and blockchain applications.

Mobile lending has continued to grow on an upward trajectory in Kenya with a shift from traditional lending from banks since the introduction of the interest rate cap on commercial bank lending, which was introduced in 2016. Mobile lending platforms such as Tala, Branch International and Fuliza, which target individuals and small enterprises that require instant, short-term loans, are making loans cumulatively in billions of shillings. For example, Fuliza, launched by Safaricom in January 2019, is a novel overdraft product which allows M-PESA customers to complete their M-PESA transactions when they have insufficient funds in their e-wallet, with an instant overdraft facility equivalent to the amount of shortfall in the e-wallet for the transactions that cannot otherwise be concluded. Fuliza lent up to KES 6.2 billion (approximately USD 62 million) in its first month of inception.

- 1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?**

There are currently no blanket prohibitions on fintech businesses in the country and the financial sector regulator, the Central Bank of

Kenya (CBK), is generally receptive to fintech innovations. For instance, in 2007, the CBK gave a letter of no objection to Safaricom Limited, the mobile operator which sought to operate MPESA, at a time when there was no regulatory framework in place. Since then, the National Payment Systems Act, No. 39 of 2011 (the NPS Act) has been enacted, which governs payment service providers in Kenya.

2 Funding For Fintech

- 2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?**

Growing businesses may be financed through debt, equity or a combination of both. Equity financing is generally preferred as it avoids front loading often associated with debt financing. Early-stage fintech is often financed by convertible debt or the issuance of preference shares to investors.

With the boom in the fintech sector, there have been an increasing number of private and foreign investors providing equity financing to the new businesses. For example, in 2018, The Rise Fund, a global impact fund managed by growth equity platform TPG Growth, invested approximately USD 47.5 million in Cellulant, a leading digital payments provider that reaches 40 million people across 11 African countries. This is one of the largest investments for a solely Africa-focused venture-funded company.

- 2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?**

To the extent that a fintech company's business involves money transfer services, such service would be exempt from VAT which would normally be imposed on taxable supplies made by a registered person in Kenya. The Value Added Tax Act, Cap 476, laws of Kenya, lists financial services that are exempt from VAT including "*the issue, transfer, receipt or any other dealing with money, including money transfer services*", "*the making of any advances or the granting of any credit*" and "*the provision of the above financial services on behalf of another on a commission basis*" (emphasis ours).

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

Listings of shares on the Nairobi Stock Exchange (NSE) must be approved by the Capital Markets Authority (CMA) based on the satisfaction of various listing requirements. These requirements include the need to ensure that the companies' memorandum and articles of association conform to the guidelines on corporate governance for listed companies and the rules regarding immobilised securities. The company proposing to list must have at least three non-executive directors, and the chairperson of the board must not hold a chair position in more than two listed companies. The company must also meet the capital requirements depending on the investment segment on which it proposes to list: Main Investment Market Segment – KES 50 million; Alternative Investment Market Segment – KES 20 million; and Growth Enterprise Investment Segment (GEMS) – KES 10 million.

The company must appoint a transaction adviser to ensure that listing requirements are satisfied. For a company listing on the GEMS, a nominated adviser must be appointed. There are increased disclosure requirements for the company in relation to its shareholders, directors, management and financial reports which must be prepared in accordance with the International Financial Reporting Standards.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

Most founders of fintech businesses have retained an equity stake while ceding part of their businesses through sale or issuance of shares. This is generally as a result of the fintech businesses being at a nascent stage, and hence their true value is yet to be realised. Investments in the businesses are still early stage to fund the operations and growth of the company as opposed to divestures.

Approval from the relevant regulator will be required for transfer of shares above certain thresholds where the fintech company is licensed as a money remittance operator, payment systems service provider, Communications Authority (CA) licensee or an IRA licensee.

Where the transfer of shares/business is deemed a merger under the Competition Act, No. 12 of 2011 and results in a change of control, the Competition Authority of Kenya approval will be required.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

The CBK is the main regulator of the financial sector which extends to fintech businesses that fall within its realm. The regulatory framework is founded on the Central Bank of Kenya Act (Chapter 491, Laws of Kenya) (CBK Act), the Banking Act (Chapter 488, Laws of Kenya), the NPS Act and the Money Remittance Regulations, 2013. The CBK Act empowers the CBK to regulate financial services in the country while the Banking Act provides for the regulation of banks. The NPS Act provides for the licensing of payment service providers.

As fintech businesses generally involve a technological aspect, licensing under the Kenya Information and Communications Act (Chapter 411A of the Laws of Kenya) may be applicable if the

implementation of the innovation requires the fintech business to establish its own telecommunications infrastructure or results in content generation. In this instance, an approval, letter-of-no-objection or a licence issued by the CA may be required. One important issue to note is that where the CA determines that a communications licence is required, the licensee would be required to ensure that at the end of the third year from the date of issuance of the licence and thereafter for the duration of the licence term, Kenyan citizens own and control no less than 20% of the shareholding in the licensee.

Public issuance of shares is regulated by the Capital Markets Act, Cap 485 (A) of the laws of Kenya. Companies selling shares through public placements or offers to the public will be required to seek approval from the CMA, the primary regulator in this sector. New regulations (which are currently in draft form) will make it compulsory for non-listed firms with smaller public offers to inform the CMA of their offers, rather than having to procure a full approval. Where the fintech product involves the insurance industry, the provisions of the Insurance Act will be applicable and the regulatory authority is the Insurance Regulatory Authority (the IRA).

It should be noted that there is a controversial draft Financial Markets Conduct Bill, 2018 (the FMCB) which seeks to regulate, amongst others, the making of non-cash payments other than by the physical delivery of Kenyan currency in the form of notes or coins. The FMCB also proposes the establishment of new regulators (in addition to the CBK) called the Financial Markets Conduct Authority, the Financial Sector Ombudsman and the Financial Sector Tribunal. Fintech companies have been pushing for the establishment of their own independent regulatory body other than the CBK, arguing that this would further bolster innovation within the sector.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

There are no laws or regulations in Kenya specifically directed at cryptocurrencies or cryptoassets.

The CBK has, however, declined to recognise virtual currencies such as bitcoins and has issued a public notice cautioning the public against dealing with virtual currencies. Though not expressly prohibited or regulated, the CBK reiterated its position in the CBK Annual Report for the year ending 2017 (the CBK Annual Report) that it does not recognise cryptocurrencies as legal tender. The CBK cautioned that cryptocurrencies are associated with anonymity, and commonly used by criminals. It has stated that in its opinion, despite the ubiquitous positive influence of technology, there lies a potential of great risk in the event that the technology fails or is misused by unscrupulous individuals.

Despite the CBK declining to grant licences to deal with virtual currencies, fintech businesses continue to deal with virtual currencies in the country. It remains unclear how the CBK will deal with such businesses as they are currently unregulated and we are not aware of any proposed regulations on virtual currencies.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

The various regulators have shown that they are receptive to the development of fintech businesses that deepen financial penetration in the country. The classic example in this respect is the CBK allowing the implementation of MPESA while the country did not have

legislation governing this innovation. This was a critical decision that enabled the development of financial services in the country and served as the basis for the growth of fintech business innovations. Other examples of the CBK being open to approving non-regulated financial services are set out in the CBK's Annual Report. These included: (i) blockchain-based storage systems; (ii) chatbots for customer service delivery; (iii) video teller machines; and (iv) psychometric credit scores proposed by a credit reference bureau. It is unclear whether these approvals were received.

That said, however, and as mentioned above, the CBK remains sceptical of virtual currencies and has issued a public notice to discourage against the use of virtual currencies such as bitcoins, which are not considered legal tender.

The CMA has prioritised efforts to create a "safe space" (or Regulatory Sandbox) in which businesses can test innovative fintech products, services, business models and delivery mechanisms for the capital markets in a live environment, without immediately incurring all the normal regulatory consequences of engaging in the fintech activity in question.

The law generally follows technology with policy makers generally seeking to catch up with technological developments. This generally provides a space for fintech companies to innovate prior to being regulated.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

Depending on its operations, a fintech company may need to be licensed by the relevant authorities in order to access customers in Kenya. The financial sector is a core of the country's economy and, as such, applications for licensing can be more stringent in comparison to other sectors. The evaluation mainly relates to the competence and capacity of the investors and employees depending on the circumstances. The regulations generally seek to protect the populace against fraud. Therefore, businesses offering fintech products and services should ensure that they have obtained the relevant clearance, licences and approvals from the CBK, CMA, CA and/or IRA depending on the type of business that they wish to carry on before accessing customers in Kenya. Due to the novel nature of fintech products, entrepreneurs may be required to hold meetings with the relevant regulators to explain how the product works. Lack of proper understanding by the regulators may lead to onerous conditions being imposed and/or delays in obtaining approvals. In general, provided that the innovator can demonstrate how it intends to mitigate the risks to the public and the risk of its innovation being used for money laundering or the financing of illicit activities, the regulators will allow the innovation to proceed to market.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

Currently, Kenya does not have any statute specifically for the dealing and handling of personal data. There is, however, a draft

Data Protection Bill (the **DP Bill**) that has been pending before Parliament for the last six years. The DP Bill seeks to provide for protection of personal information and thereby give effect to the constitutional right of a person not to have information relating to their family or private affairs unnecessarily required or revealed.

The Constitution of Kenya provides for broad protections in that it states that every person has a right to privacy, which also includes the right to not have information relating to their family and private affairs unnecessarily revealed. There is no prohibition on the collection, use and transmission of personal data, provided that the collection is undertaken in a lawful manner and the person to whom the data relates has been informed of the reasons their data has been collected and their consent to disclose such data has been obtained. The disclosure of this data without the owner's consent may be considered an infringement on a person's right to privacy, under the Constitution.

The Access to Information Act, No. 31 of 2016 provides that every citizen has the right of access to information held by the State or any other person where the information is required for the exercise or protection of any right or fundamental freedom.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

There are no restrictions on the transfer of data outside the country provided that the transfer does not infringe on the individual's right to privacy. Consent of the owner of the information must be sought before the transfer or the storage of data outside the country is undertaken.

Firms are required to be mindful of the right to privacy of the owner when handling personal data. However, the enforcement of this right against companies operating outside the country may prove challenging, especially if they do not have any legal presence within the country to which action can be brought against, should an infringement take place.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

The applicable data privacy laws in Kenya relate to the right to privacy that is enshrined within the Constitution. The remedies available for a breach or infringement of this right could either be: a declaration of the right to privacy; restriction of the conduct that is infringing on that right; or an order for compensation.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

The Cybercrimes Act provides for the monitoring, control and curbing of cybercrimes which have been on the rise in Kenya and around the world. The Cybercrimes Act criminalises cyber offences such as computer fraud, phishing, cyber stalking, child pornography, unauthorised access or interference or interception to computerised systems and identity theft, among others.

However, provisions relating to unauthorised access or interference or interception to computerised systems have been suspended, pursuant to a High Court order issued on 30 May 2018 in the matter of *The Bloggers Association Kenya vs the Honourable Attorney General and 5 others (Petition No 206 of 2018)*, and would therefore not be applicable for enforcement purposes.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

The Proceeds of Crime and Anti-Money Laundering Act No. 9 of 2009 is the primary statute on money laundering in Kenya and sets out on-going reporting requirements for financial institutions. The Proceeds of Crime and Anti-Money Laundering Regulations, 2013 also regulate money laundering activities in Kenya. Financial institutions are required to (i) monitor complex and unusual transactions, (ii) report any transaction exceeding USD 10,000 to the Financial Reporting Centre, and (iii) verify customer identities. The law imposes stiff penalties on those found culpable in addition to identification, tracing, freezing, seizure and confiscation of the proceeds of crime. In September, 2018, the CBK penalised five Kenyan banks that were used by persons suspected of transacting illegally with the National Youth Service (NYS).

The National Payment System (Anti-Money Laundering Guidelines for the provisions of Mobile Payment Services) Guidelines 2013 applies to mobile payment service providers.

The Anti-Corruption and Economic Crimes Act, No. 3 of 2003 provides for the prevention, investigation and punishment of corruption, economic crime and related offences.

The Prevention of Terrorism Act, No. 30 of 2012 provides for measures for the detection and prevention of terrorist activities and requires financial services providers to monitor their products and services for possible use in aiding and facilitating terrorist activities. Kenya is especially sensitive on this issue, having borne the brunt of several terrorist attacks. Following the latest terror attack in Kenya, a bank manager at one of the commercial banks was charged with failure to report suspicious activity regarding proceeds of crime and anti-money laundering, aiding and abetting the commission of a terrorism act, as well as failure to report a suspicious transaction.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

Fintech businesses should adhere to general laws, regulations, rules and guidelines that apply to all businesses generally. The laws that govern the financial sector and the telecommunications sector would in turn also apply to fintech businesses. There are other regimes that may also be applicable, including consumer protection law, anchored in the Consumer Protection Act, No. 46 of 2012 and the Competition Act, No. 12 of 2011.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

The Employment Act, 2007 sets out the parameters of the employee-employer relationship. Employees are required to be provided with an employment contract which may be either written or oral, with the written contract containing the information that is mandatorily required by statute.

Employees are required to be paid in Kenyan shillings.

Kenyan law does not provide for “at will” termination of employment. An employee may be terminated from employment on account of

redundancy, by summary dismissal without notice on certain grounds or on notice for fair reason. In general, the employment courts are considered employee-friendly.

5.2 What, if any, mandatory employment benefits must be provided to staff?

The mandatory employment benefits are:

1. medical insurance cover through the National Health Insurance Fund;
2. pension scheme contributions through the National Social Security Funds;
3. reasonable housing or sufficient allocation of salary to afford reasonable housing;
4. wholesome water;
5. sufficient medicine during illness and medical attention for serious illness. General practice is for employers to put in place medical insurance cover with respect to their employees;
6. annual leave of at least 21 days, maternity leave of at least three months and paternity leave of at least two weeks with full pay; and
7. overtime payment subject to the limits prescribed by the law.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

The Kenya Citizenship and Immigration Act, 2011 (KCIA) requires all foreigners who wish to work within Kenya to obtain a valid work visa and a work permit. There are no specific benefits or special routes for expatriate employees who wish to work for fintech companies. An employer is required to procure work permits for its non-Kenyan citizen employees. The employer is required to demonstrate that there is a Kenyan citizen being trained to take on the job. It is an offence under the KICA to employ a person who requires a work permit and does not have one.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Innovations and inventions are protected under the intellectual property legal regime. This regime includes the following statutes:

1. patents, industrial designs and utility models receive protection under the Industrial Property Act;
2. trade marks receive protection under the Trade Marks Act;
3. copyrights receive protection under the Copyrights Act;
4. plant breeders' rights receive protection under the Seeds and Plant Varieties Act; and
5. trade secrets receive protection under the Paris Convention and the TRIPs Agreement.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

To gain protection for registerable intellectual property, such as trademarks, patents and designs, the owner must register the invention

or innovation. The registered legal owner of the intellectual property rights is considered to be the *prima facie* owner of those rights. Copyright exists from when the literary or artistic works are prepared and need not be registered; however, registration will help to establish a first right. An IP holder has the right to alienate, assign or license the IP rights held in respect of an innovation or invention, and these rights only apply in the country.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

In Kenya, the owner of a globally recognised IP right does not need to own local/national registrations so as to be able to enforce their IP rights in Kenya. Multi-jurisdictional rights in respect of patents, utility models and industrial designs apply by virtue of Kenya being a state party to the African Regional Intellectual Property Organisation's (ARIPO) Harare Protocol on Patents and Industrial Designs. Kenya is also a party to the Protocol Relating to the

Madrid Agreement Concerning the International Registration of Marks (the **Madrid Protocol**) and, as such, subject to the national approval process, an international trade mark registration under the Madrid Protocol may also be enforced in Kenya where Kenya has been designated under it.

Kenya is also a party to the Patent Co-operation Treaty (**PCT**) which provides for an international filing mechanism for patent applications, but the rights that are yielded at the end of a patent process initiated through the PCT are actually national rights.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

Intellectual property rights may be monetised by use, assignment or licensing. There are no particular rules or restrictions regarding such exploitation or monetisation – these would be governed by the agreements made between the relevant parties.



Sonal Sejpal

Anjarwalla & Khanna
The Oval, 3rd Floor
Junction of Ring Rd. Parklands & Jalaram Rd.
Westlands, Sarit Centre
P.O. Box 200-00606, Nairobi
Kenya

Tel: +254 20 364 0000 / +254 20 364 0000
Email: ss@africalegalnetwork.com
URL: www.africalegalnetwork.com/kenya

Sonal Sejpal has been a Director with A&K for over 20 years. She co-heads the firm's fintech practice. Sonal also provides support to ATZ Law Chambers, A&K's affiliate firm in Tanzania. She has considerable experience in banking and finance, including advising local and international banks, financial services firms and Fintech companies in areas such as financial services regulation, bank regulatory, transactional and compliance matters. She also advises on project finance, company commercial matters, employment, restructuring and insolvency. Sonal is a regular speaker at seminars on various aspects of banking and commercial law, including seminars organised by the UK-based Loan Market Association. She has until very recently sat on the Board of Directors of both Liberty Life Insurance and Heritage Insurance, and is the Vice Chairperson of the British Chamber of Commerce.

Sonal is ranked as a leading lawyer in Kenya in *Chambers Global*, *IFLR 1000*, *The Legal 500* and other publications.



Dominic Rebelo

Anjarwalla & Khanna
The Oval, 3rd Floor
Junction of Ring Rd. Parklands & Jalaram Rd.
Westlands, Sarit Centre
P.O. Box 200-00606, Nairobi
Kenya

Tel: +254 20 364 0000 / +254 70 303 2000
Email: djr@africalegalnetwork.com
URL: www.africalegalnetwork.com/kenya

Dominic Rebelo is a Partner in A&K's Corporate department and co-heads the firm's Fintech practice. He has wide-ranging experience in advising local, regional, and international fintech clients on various matters, including regulatory, corporate and compliance issues and providing assistance on government policy and business concerns. Dominic has extensive experience in financial services regulations, crowdfunding, online payments and mobile banking, Peer-to-Peer (P2P) lending and charity platforms, technologically innovative payment structures, instruments and systems. He has previously collaborated with FSD Africa on examining the regulatory and public landscape that governs crowdfunding in Kenya.

Dominic also has wide-ranging experience in corporate mergers and acquisitions, private equity, and capital markets. He has advised domestic, regional and international private and publicly listed companies on a variety of commercial transactions, including share acquisitions, privatisations, public listings and cross listings. Dominic is ranked as a leading lawyer in Kenya by *Chambers Global* and *IFLR 1000*.



Anjarwalla & Khanna (A&K) is considered the leading full-service corporate law firm in Kenya, and with over 100 lawyers is currently the largest law firm in Sub-Saharan Africa outside of South Africa. Our client base is made up of both local and international clients. A&K's longstanding experience advising clients in the financial and technology media and telecommunications sectors has naturally placed it as a leading advisor to fintech businesses starting up and operating in East Africa, including advising on various regulatory and compliance issues together with providing assistance on government policy and business concerns. A&K has received the African Law Firm of the Year Award four times since the launch of the awards in 2013, Law Firm Innovation (2017) and M&A Team of the Year (2018) awards, all presented by the African Legal Awards as well as the Best Legal Advisor Award (2018) at the EAVCA Industry Awards.

Learn more about A&K here: www.africalegalnetwork.com/kenya.

Korea

Jung Min Lee



Kim & Chang

Samuel Yim



1 The Fintech Landscape

- 1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).**

Korea has a wide array of fintech businesses from payment services, peer-to-peer (P2P) lending and investment, and blockchain applications. The most notable fintech innovation trends are electronic payment services led by major Korean IT companies and financial institutions. These new electronic payment services, such as KakaoPay and NaverPay, are tailored to Korean consumers and are generally well accepted in Korea. New internet-only banking platforms, such as K-Bank and Kakao Bank, have flourished in Korea. These internet-only banks were developed by major Korean IT companies and financial institutions, or through a consortium of major IT companies and financial institutions. These internet-only banks launched their operations in 2017, and secured a sizeable market share of customers by marketing loans with low interest rates or bank deposits with favourable interest rates.

In addition, due to the sharp increase in P2P lending in Korea, the Korean financial regulatory authorities published the “P2P Loan Guidelines” in February 2017. Subsequently, the P2P Loan Guidelines were amended in 2018 and 2019 to provide stronger protections to investors. The latest version of the P2P Loan Guidelines became effective on January 1, 2019 and will remain effective until the end of 2019. However, the P2P Loan Guidelines are not legally binding. Thus, the Financial Services Commission (FSC) recently announced that they will recommend a comprehensive bill regulating P2P loans to the National Assembly.

Finally, the Foreign Exchange Transaction Act regulates foreign exchange businesses and covers the issuance or dealing of foreign exchange and payment, collection and receipt between Korea and a foreign country. The Foreign Exchange Transaction Rule (FX Rule) is a subordinate regulation of the Foreign Exchange Transaction Act, which was recently amended and became effective on January 1, 2019, (i) increased the annual limit for overseas remittance by institutions registered as small-amount remittance operators from USD 20,000 to USD 30,000, and (ii) allowed securities companies and credit card companies to remit funds overseas without filing an FX report with a designated FX bank if the amount does not exceed USD 3,000 per remittance and USD 30,000 per year. In addition, electronic currencies (e.g., vouchers where a monetary value is

stored electronically, such as “K-CASH”) and prepaid electronic payment means (e.g., T-money, Tossmoney or Kakaomoney) issued in Korea may now be used in foreign jurisdictions to pay for goods or services or be exchanged directly for foreign currencies.

- 1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?**

Currently, there are no prohibitions or restrictions for certain types of fintech businesses in Korea. However, fintech businesses providing certain financial services are required to obtain a licence under the relevant Korean financial laws and regulations. (For details of the licensing requirements, please refer to our answer in question 3.1 below.) Furthermore, there are no laws or regulations that directly regulate blockchain or cryptocurrency businesses in Korea (see question 3.2).

In 2017, Korea experienced a dramatic increase in the volume of cryptocurrency trading where the trading volume for a 24-hour period in the Korean cryptocurrency exchanges averaged up to KRW 8 trillion. Due to the high volume of cryptocurrency trading in Korea, in September 2017, the Korean government formed an intergovernmental task force to create and implement cryptocurrency regulations. The government agencies that participated in this task force were the Ministry of Strategy and Finance, the Ministry of Justice, the FSC and other relevant regulatory authorities. The FSC also issued a press release prohibiting initial coin offerings (ICOs) in Korea, but no laws or regulations have yet to be enacted to enforce this prohibition. Further, in January 30, 2018, the Korean Financial Intelligence Unit (KOFIU) announced the “Anti-Money Laundering Guidelines for Cryptocurrencies” (AMLC Guideline) for financial institutions that transact with cryptocurrency companies. The AMLC Guideline covers, among others, real-name verification, due diligence on cryptocurrency exchanges, and reporting suspicious transactions. On June 27, 2018, the AMLC Guideline was amended to additionally require financial institutions to share the list of foreign cryptocurrency exchanges among financial institutions (see question 4.5).

On January 31, 2019, the Korean government announced the result of its review of overseas ICOs by Korean companies and its proposed approach in regulating ICOs. In this announcement, the Korean government stated that they identified companies bypassing the government’s prohibition on ICOs by performing ICOs through paper companies in foreign jurisdictions (such as Singapore) while raising funds from domestic investors. The Korean government declared that such practice, in substance, is a domestic ICO even though the ICO originated overseas. Moreover, the Korean government stated that

domestic investors were at significant risk due to such practice because the companies conducting the ICOs did not disclose material information for investors to make an informed investment decision.

In addition, the Korean government also indicated that some of the previous ICO projects may violate the Financial Investment Services and Capital Markets Act (FSCMA). The Korean government specifically cited ICO projects that involved: (i) issuance and transaction of P2P collateralised loan tokens; (ii) sale of cryptocurrencies investment funds; or (iii) operation of unauthorised financial investment businesses by providing investment services with ICO tokens.

Since ICOs can be high-risk investments, and without any clear regulatory framework, the Korean government announced that it will take a conservative approach in legalising ICOs. Also, the Korean government has yet to decide on whether it will publish an ICO guideline, stating that an official issuance of an ICO guideline may give the market a wrong impression that the Korean government approved domestic ICOs.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

Korea has debt and equity capital markets that are accessible to new and growing businesses, such as fintech start-up companies. The early rounds of fundraising for fintech start-up companies in Korea are similar to that of other types of start-up companies that rely on angel investors and founders. Recently, start-up companies in Korea have also been taking advantage of other methods of funding, such as crowdfunding, accelerators, and government funding programmes.

Equity

Equity-based crowdfunding, which involves funding a project or venture by raising monetary contributions from a large number of people through an investment in equity or securities, was introduced in Korea through an amendment to the FSCMA that came into effect on January 25, 2016. There are, however, certain restrictions in the issuance of equity for crowdfunding under the FSCMA. Namely, a single company can raise funds up to KRW 1.5 billion per year through crowdfunding. To raise funds that exceed KRW 1.5 billion, conventional means of financing should be utilised. Moreover, under the FSCMA, the issuance of equity for crowdfunding is permitted for non-listed small/medium-sized companies with less than seven years of business operations.

In April 2018, the Enforcement Decree of the FSCMA was amended to increase the limit for an ordinary investor to invest in crowdfunding from KRW 5 million to KRW 10 million per year with an issuer of equity. In addition, the amended Enforcement Decree of the FSCMA allowed “social enterprises”, which are companies certified by the Ministry of Employment and Labor that seek to improve financial, social and environmental well-being through commercial activities (e.g., providing employment opportunities to disadvantaged groups or making contributions to the local society), to raise funds through crowdfunding.

Debt

New and growing businesses may borrow through P2P lending in Korea. The P2P lending industry in Korea has grown significantly in recent years. Due to the sharp increase in P2P borrowing in Korea, the FSC introduced the P2P Loan Guidelines in February 2017 to regulate the P2P loan industry, mainly to protect investors.

The total amount of loans in the P2P lending industry in 2017 has increased approximately 8–10% per month since the publication of the P2P Loan Guidelines.

The 2019 P2P Loan Guidelines became effective on January 1, 2019 and will remain effective until the end of 2019. For individual P2P lenders, the P2P Loan Guidelines set a lending limit between KRW 10–40 million, which varies depending on the income of the individual P2P lender. However, the limit for investment in P2P real estate loan products (e.g., project finance) is KRW 20 million. In contrast, the P2P Loan Guidelines do not set a monetary limit for investors who are either corporate investors or accredited individual investors (i.e., professional investors). However, there is no P2P loan amount borrowing limit for borrowers under the P2P Loan Guidelines.

The 2019 P2P Loan Guidelines also expanded the scope of disclosure for P2P lenders. In particular, the 2019 P2P Loan Guidelines recommend P2P lenders to disclose a “third party expert’s review” of key features of project finance P2P loans (e.g., loans for construction of new buildings). In addition, the offer of any real estate P2P loans, including project finance P2P loans, should be disclosed on the P2P lender’s website at least two days prior to the sale of these P2P loans.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

The Korean government offers special incentive schemes mainly in the form of tax incentives for tech/fintech businesses or small/medium-sized businesses in Korea.

- Small/medium-sized businesses established in certain areas of Korea that are not located in highly populated cities in Korea can receive 50% corporate tax relief for up to five years on their business income.
- Those companies identified as a “venture business” by the Korean government, by which many fintech companies may qualify, may receive 50% corporate tax relief even if they are located in highly populated cities in Korea.
- Research and development (R&D) tax deduction may be available for certain R&D costs (including labour costs and material costs).

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

The conditions for a business to IPO in Korea depend on the type of listing and the securities market where the shares will be listed. The Korea Exchange (KRX) is the sole stock exchange in Korea. The KRX has three securities markets: (i) the KOSPI (for stocks issued by companies with equity capital of KRW 30 billion or more); (ii) the KOSDAQ (for stocks issued by companies with equity capital of KRW 1 billion or more); and (iii) the KONEX (for stocks issued by companies with equity capital less than KRW 1 billion).

The KONEX market was introduced to provide IPO opportunities to small/medium-sized companies as an alternative to the KOSPI or KOSDAQ market. When compared to the KOSPI and KOSDAQ, the KRX does not apply the rigorous financial requirements for a KONEX market listing so that start-up companies, in the early stages of a business, can also list in the Korean securities market. As a result, the KONEX market has opened IPO opportunities for start-up fintech and small/medium-sized companies in the Korean securities market.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

There have not been any notable exits by the founders of fintech businesses in Korea.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

The Electronic Financial Transaction Act (EFTA) regulates electronic financial transactions in Korea. The EFTA covers the: (i) rights and obligations of the parties to an electronic financial transaction; (ii) provisions to ensure the safety of electronic financial transactions and protection of users; and (iii) authorisation, registration and specific scope of activities of electronic financial businesses.

The following activities are listed as “electronic financial business” under the EFTA: (a) issuance and management of electronic currency; (b) electronic funds transfer services; (c) issuance and management of electronic debit payment services; (d) issuance and management of electronic prepayment services; (e) electronic payment settlement agency services; (f) depository service for settlement of transactions; and (g) intermediary electronic collection and payment services between payors and payees. Other than the issuance and management of electronic currency, which needs to be licensed by the FSC, the above types of electronic financial businesses must be registered with the FSC and are supervised by the FSC and the Financial Supervisory Service (FSS).

Further, fintech businesses that do not engage in electronic financial business activities under the EFTA but which intend to undertake regulated activities in Korea, such as banking or credit card businesses, should review whether it is required to obtain appropriate authorisation (licence or registration) from the relevant Korean regulatory authorities such as the FSC or the FSS.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

There is no existing regulatory regime or statute that specifically regulates cryptocurrency. However, the Korean regulators are likely to apply and/or enforce the existing Korean laws and regulations for cryptocurrencies.

For example, in an ICO, if tokens are classified as “securities” under Korean law, the tokens will then be subject to the offering restrictions in Korea under the FSCMA. Or, even if tokens are not classified as securities, if the marketing of the tokens in an ICO raises funds from the public with a promise to return the original investment amount, or an amount exceeding such investment in the future, the ICO could be regulated by the Act on the Regulation of Conducting Fundraising Business without Permission.

Currently, there are several cryptocurrency bills proposed at the National Assembly. These bills generally cover, among others, licensing requirements for cryptocurrency businesses, anti-money laundering requirements, consumer protection, cybersecurity requirements for cryptocurrency exchanges, and damage compensation for consumer losses. It is unclear when or if these pending bills, in their current form, will be enacted into law in Korea.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

Financial regulators and policy-makers in Korea are generally receptive to fintech innovations and technology-driven new entrants to regulated financial services markets in Korea. The Korean government identified fintech as one of its 24 key areas to support innovation as a means to spur growth in the Korean financial industry. For example, the Korean government established the Fintech Support Centre that provides guidance on fintech-related projects and an opportunity for fintech start-ups to present their services to financial institutions. The FSC has announced 18 key projects for “financial innovation” to be implemented as part of their 2018 business plan, and support for the fintech industry is one of the FSC’s key initiatives.

The Special Act on Support of Innovation of Finance, which will introduce the regulatory sandbox system in Korea, was passed by the National Assembly in December 2018 and will be effective on April 1, 2019. The new law introduces the following two measures:

- Expedited confirmation on regulation: A financial company that plans to start a new type of financial business may deem that no regulation on the new business exists if the company does not receive a response from the FSC within 30 days after filing an inquiry to the FSC as to the existence of a regulation on the new business. The FSC may forward the inquiry to other relevant government agencies, if deemed necessary, but in any case the FSC must provide a response within 30 days.
- Designation of innovative financial service: A financial service that is designated as an “innovative financial service” by the government may operate without regulatory oversight during the designated period (less than two years and may be renewed once for less than two years). Financial service providers whose service can be clearly distinguished from pre-existing services, in terms of contents and methods, may apply to the government to designate such service as an innovative financial service. Upon receiving such application, the Innovative Financial Services Examination Committee, which consists of public officials from the FSC and other relevant government agencies and private experts, will assess various factors, such as: (i) whether the proposed innovative financial services are provided in Korea; (ii) whether the proposed financial services are truly innovative; and (iii) whether the proposed financial service will likely increase the customers’ interests. In addition, if a designated innovative financial service is being operated under a licence required by other financial laws and regulations, such designated innovative financial service shall be afforded an exclusive right of operation for two years after designation as an innovative financial service. This means that during the two-year period granted by the Korean government, no other service provider may provide the same type of financial service in Korea.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

Where a fintech business established out of Korea wishes to access new customers in Korea, it will need to consider whether it requires authorisation from a Korean regulatory authority. A fintech business established outside of Korea may be subject to Korean laws and

regulations if it carries out regulated activities in Korea. Where an overseas fintech business performs regulated activities in Korea, it will need to obtain authorisation from the relevant Korean financial regulatory authority (as discussed in our answer to question 3.1 above). Generally, the standard to determine the applicability of Korean laws to foreign fintech businesses is whether the foreign fintech businesses targets Korean customers (e.g., Korean websites) or allows payment in Korean won.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

In Korea, the protection and regulation of personal data is primarily governed by the Personal Information Protection Act (PIPA). The PIPA is the overarching personal data protection law in Korea that may apply to fintech businesses operating in Korea. The PIPA prescribes detailed measures for each of the stages involved in the processing of personal data such as collection and use, provision to a third party, outsourcing and destruction. The PIPA must be followed by all personal information processing entities, which are defined as all persons, organisations, corporations and governmental agencies that process personal data for business purposes. Under the PIPA, data subjects must be informed of, and provide their consent to, the following matters before their personal data is collected or used: (i) the purpose of the collection and use; (ii) the items of personal information that will be collected; (iii) the duration of the possession and use of the personal information; and (iv) disclosure that the data subject has a right to refuse to give consent and the negative consequences or disadvantages that may result due to such refusal.

In addition, there are various sector-specific privacy laws such as the Act on the Promotion of IT Network Use and Information Protection (Network Act) and the Use and Protection of Credit Information Act (Credit Information Act) that complements the PIPA. The Network Act regulates the processing of personal information in the context of services provided by online service providers (e.g., personal information collected through a website). The Credit Information Act regulates and protects financial transaction information and credit information of individuals and entities. Both the Network Act and the Credit Information Act can apply to fintech businesses operating in Korea.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

Yes, to both questions.

- The PIPA applies to all personal information processing entities regardless of whether they are located overseas. In addition, sector-specific privacy laws such as the Network Act would apply to overseas online service providers collecting personal information in Korea. Further, the Credit Information Act would also apply to overseas entities handling financial transaction information and credit information of individuals or entities in Korea. Although the PIPA, the Credit Information Act, and the Network Act do not specifically address their jurisdictional scope for overseas entities, the Korean regulatory authorities have measures to ensure compliance by overseas entities with these laws.

- The PIPA and the Network Act requires users to be informed of and provide their consent to the following before their personal data is transferred to a third party overseas: (i) name of the third party; (ii) the third party's purpose of use of the personal information; (iii) items of personal information; (iv) the third party's period of retention and use; and (v) the user's right to refuse to give consent and consequence of any such refusal. Further, under the Network Act, if a user's personal data is transferred to an overseas entity, online service providers must disclose and obtain the user's consent with respect to the following: (a) specific information to be transferred overseas; (b) the destination country; (c) the date, time and method of transmission; (d) the name of the third party and the contact information of the person in charge; and (e) the third party's purpose of use of the personal information and the period of retention and usage. Although the Credit Information Act is silent on international transfers of credit information, the PIPA requirements would likely apply for overseas data transfers of credit information of individuals and entities in Korea.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

The Ministry of the Interior and Safety (MOIS) is responsible for enforcing the PIPA. The Korean Communications Commission (KCC) and the Ministry of Science and ICT (MSIT) are responsible for enforcing the Network Act. The FSC and the FSS are responsible for enforcing the Credit Information Act. Each of these regulatory agencies can make requests for information and conduct inspections at the premises of data controllers to ensure they are compliant with the respective privacy laws. In addition, once a violation of a relevant privacy law is confirmed, each of these respective regulatory agencies can impose administrative penalties, such as corrective orders and fines, and, as necessary, refer the case for criminal prosecution. Criminal sanctions can be imposed following an investigation by the police or prosecutors' office either on its own initiative or upon a referral by the relevant regulatory authority.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

The main statutes in the context of cyber security that apply to fintech businesses are the PIPA and the Network Act. The PIPA and the Network Act prescribe detailed technical security and administrative requirements for cyber security, such as: (i) the establishment and implementation of an internal management plan for the secure processing of personal information; (ii) installation and operation of an access restriction system for preventing illegal access to and leakage of personal information; and (iii) the application of encryption technology to enable secure storage and transfer of personal information.

Further, the EFTA criminalises certain types of cyber activities that may apply to fintech businesses operating in Korea. The EFTA criminalises cyber activities that: (a) intrude on electronic financial infrastructures without proper access rights or by surpassing the scope of permitted access rights or altering, destroying, concealing or leaking data that is saved in such infrastructures; and (b) destroy data, or deploy a computer virus, logic bomb or program such as an email bomb for the purpose of disrupting the safe operation of electronic financial infrastructures.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

The anti-money laundering and other financial crime requirements in Korea are governed by the Act on Reporting and Using Specified Financial Transaction Information (also known as Financial Transaction Reporting Act or FTRA) and the Act on Regulation and Punishment of Criminal Proceeds Concealment (also known as the Proceeds of Crime Act or POCA).

The FTRA regulates money-laundering activities through financial transactions by establishing a reporting mechanism to review certain financial transaction information. The FTRA specifically provides for the submission of Suspicious Transaction Reports (STRs) and Currency Transaction Reports (CTRs) from financial institutions, and the analysis and dissemination of STRs to relevant law enforcement agencies for further action. The FTRA, however, only applies to licensed financial institutions in Korea, therefore fintech businesses that are licensed under Korean financial regulations would be subject to these requirements.

The POCA criminalises money-laundering activities and imposes criminal penalties and seizure of assets relating to money-laundering activities. Under the POCA, fintech businesses that are licensed financial institutions are required to report transactions to law enforcement agencies if, among other situations, they became aware that transacted assets are criminal proceeds or that the counterparty is engaged in the crime of concealment of criminal proceeds.

From January 2018, financial institutions doing business with companies that handle cryptocurrencies must comply with the AMLC Guideline issued by the KOFIU. Notable requirements are as follows:

- Real-name verification required for payment and receipt to cryptocurrency companies:
 - Users are only allowed to make payment to and receive payment from a cryptocurrency company's bank account using their own real-name verified account that has been opened under the same bank as the cryptocurrency company.
 - Financial institutions may decline transactions with cryptocurrency companies that make payments to or receive payments from its users that do not use real-name verified bank accounts.
- Customer due diligence:
 - Financial institutions must put in place a process to check whether a customer is a cryptocurrency company.
 - Financial institutions must verify, through on-site due diligence, certain additional information pertaining to cryptocurrency companies (including whether the cryptocurrency company is maintaining separate transaction records for each customer) at least every six months.
- Suspicious activity reports:
 - Financial institutions must appoint dedicated staff for monitoring suspicious transactions of cryptocurrency companies and their users.
 - Financial institutions must establish stronger transaction monitoring rules for suspicious activities of cryptocurrency companies.

In April 2018, the FSC conducted a compliance review of the AMLC Guideline by financial institutions. Based on this review, the FSC amended the AMLC Guideline in June 2018 and will remain effective until July 2019. The key requirements of the amended AMLC Guideline are as follows:

- Financial institutions are now also required to monitor the corporate accounts of the cryptocurrency companies (e.g.,

cryptocurrency exchanges), when previously they were required to only monitor the client accounts in order to be able to conduct enhanced customer due diligence in case they identified a suspicious transaction.

- Financial institutions must share the customer list of foreign cryptocurrency companies with other financial institutions.
- Financial institutions must decline a transaction, without delay, if they identified a suspicious transaction of the cryptocurrency company or they are unable to conduct due diligence on the cryptocurrency company due to the suspension/termination of business of the cryptocurrency company.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

Other sector-specific laws that may apply to fintech businesses include:

- The Foreign Exchange Transaction Act, which regulates foreign exchange businesses, including the issuance or dealing of foreign exchange and payment, collection and receipt between Korea and a foreign country.
- The Act on Consumer Protection in e-Commerce, which regulates online retailers, including persons engaged in the business of selling goods or services by providing information relating to such goods or services and soliciting offers to purchase from customers by means of mail or telecommunications networks.
- The Use and Protection of Location Information Act, which regulates companies that collect, use and share location information of a living individual or movable things.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

Korea is a "just cause" and not an "at will" employment jurisdiction. Companies employing five or more employees are subject to a "just cause" standard for termination under the Labour Standards Act (LSA). What constitutes just cause is not clearly defined in the LSA, but, as a matter of practice, it is a high standard for an employer to meet and it is generally not easy to terminate employees in Korea. Based on the Korean case precedent, when determining the existence of just cause for termination, the courts/labour authorities will take into account the totality of the circumstances and give weight to factors, including, without limitation, the: (i) frequency and degree of the reason for termination (e.g., poor performance, misconduct, etc.); (ii) impact on the company; and (iii) whether the company gave the employee an opportunity to redeem himself/herself. In sum, the authorities will determine whether the sanction (i.e., termination) is commensurate with the reason for the sanction.

Just cause to terminate an employee may be based generally on one of three grounds: (a) acts of serious (or repeated) misconduct or wrongdoing; (b) poor performance; or (c) business reasons (e.g., winding down of a company). However, in each case, unilateral termination would require that the company meets these high standards. For example, termination for poor performance may require that the company establish a record of continued poor performance over a relatively long period of time, while having given the employee a sufficient opportunity to redeem his or her performance issues.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Employers must pay all employees at least the specified national minimum wage of KRW 8,350 per hour (about USD 8.00 per hour) as of 2018, under the Minimum Wage Act. Also, employers are required to subscribe to the four main statutory insurance programmes of the National Health Insurance, National Pension, Unemployment Insurance, and Workers Compensation Insurance so that employees can receive coverage and benefits. The National Health Insurance, National Pension, and Unemployment Insurance each involve employer and employee contributions, while the Workers Compensation Insurance only involves employer contributions.

An employee who has been with the employer for one year or more is entitled to a statutory severance payment of at least 30 days of average wages per year of service from the employer upon termination of employment (regardless of the cause of termination). If the employer has adopted a defined benefit or defined contribution plan in accordance with the Employee Retirement Benefits Security Act, the employer can satisfy this statutory severance requirement through the pension plan.

An employee who records at least 80% attendance during one full year is entitled to 15 days of paid annual leave. If an employee has worked for less than one year or has recorded less than 80% attendance during a full year, he/she is entitled to one day of paid leave for each completed month of service. An employee who has worked for three consecutive years or more is entitled to an additional day of annual paid leave for every two consecutive years of service thereafter, with the total number of days of leave capped at 25 days. An employer must compensate for any unused days of annual leave at the rate of 100% of ordinary wage, unless the employer implemented measures to “encourage” the use of annual leave pursuant to the LSA.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

All non-Korean citizens must have a proper visa to work in Korea. The Immigration Control Act (ICA) is the main immigration regulation in Korea and applies to all companies, and there are no special rules/exemptions for fintech businesses. The ICA prescribes the restrictions for the employment of foreigners and the applicable regulations vary depending on factors such as: (i) where the foreigner resides (whether the foreigner stays in Korea or abroad); (ii) the form of employment (whether the company hires the foreigner as a professional or a labourer); and/or (iii) the nationality of the foreigner. Currently, there are over 30 types of entry visas for entering Korea and the appropriate visa will depend on, among others, the nature of the assignment/employment, type of entity located in Korea, and qualifications of the expatriate. The most commonly applied visas by foreigners to work in Korea are the D-8, D-7, and E-7 for long-term visas and C-3-4 for short-term visas.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

In Korea, innovations and inventions can be protected by IP rights such as patents, utility models, designs, copyrights, and trade

secrets. Korean law explicitly provides for the protection of patents under the Patent Act, utility models under the Utility Model Act, designs under the Design Protection Act, copyrights including copyrights in computer software under the Copyright Act, and trade secrets under the Unfair Competition Prevention Act (UCPA).

Under the Patent Act, fintech inventions relating to software or business methods are generally patentable if they meet the statutory requirements such as subject matter, novelty, and inventiveness. If an invention is not sufficiently creative or inventive to meet the standards of patentability, protection may be available under the Utility Model Act. The basic difference between a utility model and a patent is that a utility model requires a lower technical content. However, fintech inventions that are mainly software or business methods may not be eligible for utility models.

Graphical user interfaces of fintech software may be protected by design registrations under the Design Protection Act. For example, images represented on a display portion of a product such as a display panel can be registered and protected as a design. Copyright protection is also possible upon creation of an original computer program without any formality. Although a copyright registration is not a prerequisite for copyright protection or enforcement, it provides certain advantageous statutory presumptions in enforcing the copyright. The source code of fintech software may be protected as a trade secret under the UCPA. The UCPA defines a “trade secret” to mean information of a technical or managerial nature that: (i) is useful for business activities; (ii) is generally unknown to the public; (iii) possesses independent economic value; and (iv) whose secrecy is maintained through reasonable effort.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Ownership of IP rights such as patents, utility models, and designs initially belong to the person who created such rights. Such person may transfer his or her IP ownership right to another party through an agreement. However, transfer of an IP right, other than through inheritance or other general succession, is not effective in Korea against third parties unless it is recorded at the Korean Intellectual Property Office.

In the context of an employer-employee relationship, there are two ways for the employer to obtain ownership rights to in-service inventions of its employees. First, the employer may enter into a pre-invention assignment agreement with an employee with a provision that the employee agrees to assign any and all future in-service inventions to the employer. Second, the employer may adopt an employment rule such as an invention remuneration policy that expressly provides for employee-inventors to assign any and all future in-service inventions to the employer and the employer to provide remuneration to such employee-inventors. In either case, if the employer chooses to acquire the ownership right to an in-service invention pursuant to the agreement or employment rule, the employee is entitled to “reasonable compensation” from the employer.

Ownership of copyright initially belongs to the actual author or authors of a given work. In the context of an employer-employee or work-for-hire relationship, however, an employing legal entity, organisation, or person may be deemed to be the “author” of a work with ownership of copyright in the work. Under the Copyright Act, such employer is deemed to have copyright ownership of a work if: (i) the work is created by an employee within the scope of employment and made public (computer program works do not need to be made public), subject to the employer’s supervision; and (ii) there is no separate or particular contract or employment regulation providing that the status of the author of, or ownership of copyright in, the work-for-hire should belong to the employee.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

For IP rights such as patents, utility models, and designs, the party enforcing an IP right should own the registered rights in Korea. For copyrights, works by foreigners, such as source code of fintech software, are entitled to protection under treaties to which Korea has acceded. However, the Copyright Act provides exceptions to favourable treatment of foreigners' copyrights under such treaties. In particular, the Copyright Act provides that even if the copyright protection period for foreigners' copyrights may be in force and entitled to protection under the Copyright Act, if the copyright protection period granted in the country of their origin has already expired, Korea will not recognise the copyright protection period.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

IP rights including patents, utility models, and designs are a type of property right and thus, owners of IP rights may exploit or monetise

them for their benefit. For example, an IP owner may assign or sell his or her IP right to another person or entity and receive payment in return. An IP right may also be pledged as collateral for a loan or investment from another person or entity. Further, an IP right may be licensed through an exclusive or non-exclusive agreement for royalties or may be licensed to another party in a cross-licence agreement. If an IP right is jointly owned, a joint owner may license the IP right only with the consent of all the other joint owners, but each owner may still freely practise the jointly-owned IP.

IP-related licences may be subject to governmental review under certain circumstances. For example, under the Fair Trade Law, the Fair Trade Commission has released the Guidelines on the Unfair Exercise of IP Rights (IP Guidelines), for examining licence agreements. If a provision of a licence agreement violates one of the standards set forth in the IP Guidelines, a court may find such provision to be null and void as being contrary to Korean public policy. As for licence terms, there are no statutory or regulatory restrictions on a maximum royalty rate or payment terms. Further, Korean courts have not issued a ruling on a maximum royalty rate. Thus, the parties may agree on royalty rates and payment terms based on the facts in individual cases.



Jung Min Lee

Kim & Chang
39, Sajik-ro 8-gil, Jongno-Gu
Seoul 03170
Korea

Tel: +82 2 3703 1671
Email: jungmin.lee@kimchang.com
URL: www.kimchang.com

Jung Min Lee is a senior attorney at Kim & Chang who specialises in finance. He primarily provides legal advice on cryptocurrency, blockchains, P2P lending, banking regulations, finance IT, electronic banking and personal/financial information protection. Mr. Lee's clients include Korean and global financial companies, Korean and global portal/platform service providers, e-commerce and payment service providers and IT service providers.

Since joining the firm in 2008, Mr. Lee has advised clients on various legal, administrative, and technical regulations related to electronic banking and on the management and protection of financial transaction information. Mr. Lee is also licensed to practise as a public accountant and registered as a CPA.



Samuel Yim

Kim & Chang
39, Sajik-ro 8-gil, Jongno-Gu
Seoul 03170
Korea

Tel: +82 2 3703 1543
Email: samuel.yim@kimchang.com
URL: www.kimchang.com

Samuel Yim is a senior foreign attorney at Kim & Chang. His practice primarily focuses on general regulatory compliance for financial institutions and high-tech/internet companies, and he advises clients on legal and regulatory matters pertaining to cryptocurrency, blockchain, privacy and data protection. Prior to joining Kim & Chang, Mr. Yim worked at Allen & Overy LLP in its New York and Hong Kong offices and served in the U.S. Army with the rank of Captain.

Mr. Yim received a B.S. from the United States Military Academy in 1997 and a J.D./M.A. from Georgetown University Law Center and the Paul H. Nitze School of Advanced International Studies, Johns Hopkins University in 2008. He was also a recipient of the Fulbright Fellowship in 2005 and was a Term Member on the Council on Foreign Relations from 2010–2015. He is admitted to the New York Bar.

KIM & CHANG

Kim & Chang is Korea's premier law firm and one of Asia's largest law firms. Our successful track record of "first-of-its-kind" and groundbreaking solutions to some of the largest and most complex transactions in Korea and around the world have set us apart since our founding in 1973. We are the market leader in all major practice areas and industries. Today, more than 1,400 professionals – both attorneys and other subject matter and industry experts – work collaboratively, in teams, to craft innovative solutions to our clients' most difficult challenges.

Liechtenstein

Dr. Helene Rebholz



König Rebholz Zechberger Attorneys at Law

MMag. Degenhard Angerer



1 The Fintech Landscape

- 1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).**

The fintech business area in Liechtenstein is still in a relatively early stage of development. Until now, only a few players which have been established are considerably active in the field of fintech, which are, however, quite successful all over Europe. For example, one Liechtenstein fintech company is offering Finetrading, which represents a bank-independent financing alternative for SMEs. Another business is providing services with regard to electronic money-related mobile payments and wallet solutions with a focus on the European market.

Liechtenstein is open to and very interested in fintech solutions, and also strives to become a major player in the fintech industry with, at the moment, a focus on blockchain-related projects in particular. There are many factors which indicate that the fintech business field is intended to become a thriving sector of the Liechtenstein economy: on the one hand, the Liechtenstein financial markets regulator, the Financial Market Authority (“FMA”), acts in a very cooperative and constructive manner with regard to the realisation of blockchain-related projects. On the other hand, the Liechtenstein Government is currently in the middle of the legislative process of passing the so-called “Blockchain Act” (“Act on the regulation of trust-worthy technologies”). A first draft of this law has already been published and it is intended to enter into force in 2020. Liechtenstein would therefore be within the worlds’ first jurisdictions to pass such an act. As a result, this would provide enhanced legal certainty for blockchain-related projects, thus increasing the attractiveness of the Liechtenstein fintech market. For about two years now, Liechtenstein has been experiencing a sharp growth in blockchain-based undertakings.

- 1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?**

We are not aware of any prohibited or restricted fintech business areas in Liechtenstein.

2 Funding For Fintech

- 2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?**

Liechtenstein law knows and allows a broad range of funding possibilities: investment-based (selling shares of the company, bonds); lending-based (loans, credits); invoice trading (company sells open claims); reward-based (investors fund a project/company and receive discounts in return when buying products or services); and donation-based and hybrid models of funding.

There is no specific regulation or legislation with regard to crowd-funding; funding through ICOs (Initial Coin Offerings) or STOs (Security Token Offerings) against crypto-currency is, however, acknowledged and possible within the framework of existing financial market regulation (e.g. on the basis of a Securities Prospectus, if so required).

- 2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?**

There are no special incentive schemes for small/medium-sized businesses or tech/fintech businesses in particular available. However, Liechtenstein provides in general a business-friendly environment, as taxes are very low, especially in comparison to other jurisdictions. Furthermore, the establishment of businesses in Liechtenstein can be achieved easily and swiftly. In addition, the Liechtenstein jurisdiction provides a broad range of legal forms and general flexibility to (legally) structure the business to best meet the company’s requirements.

- 2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?**

Liechtenstein has not yet implemented any regulated market (exchange); therefore, it is actually not possible to initiate a “regular” IPO in Liechtenstein.

It is, however, of course possible under Liechtenstein law (as Liechtenstein has implemented the EC Securities Prospectus Directive and will implement the Liechtenstein Securities Prospectus Ordinance) to publicly offer securities, which may then be traded bilaterally or may also be listed on foreign exchanges, MTFs or OTFs.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

We are not aware of any notable exits in Liechtenstein.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

Liechtenstein is as a member of the European Economic Area (EEA); therefore, Liechtenstein law is overall in line with the European regulatory framework. Liechtenstein has therefore implemented all regulatory legal acts passed by the EC legislator, such as, e.g., MiFID II (the domestic Banking Act (“BankG”) and the Asset Management Act (“VVG”) were adapted accordingly), the Prospectus Directive (as of July 2019, the Prospectus Directive will become directly applicable in Liechtenstein), PSD (influenced the domestic Act on Payment Services (“ZDG”)), UCITS and AIFM legislation, etc.

Liechtenstein has, however, not enacted a specific law on crowd-funding or fintech in specific. Such projects and activities therefore have to be analysed as to whether they have to be considered regulated or not. It has to be evaluated on a case-by-case basis if, e.g., a fintech business case may trigger any licensing requirement.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

As mentioned in question 1.1, due to the great potential of the blockchain technology *per se*, the Liechtenstein Government has decided not only to review current applications of, in particular, crypto-currencies or initial coin offerings on the basis of the existing legal framework, but rather to provide a legal basis for a broad and secure application of the “token economy”. Therefore, the Liechtenstein legislator intends to pass the so-called *Blockchain Act*. The Government issued in November 2018 a so-called “*Vernehmlassungsbericht*”, which is a formal legislative act disclosed to the public with an invitation to various interest groups or individuals to comment on the proposed draft.

With the Blockchain Act, the Liechtenstein Government intends to clarify open legal questions with respect the blockchain technology and its application in order to create legal certainty for both users and service providers. The main purpose of this Act is to protect users on blockchain systems as well as to ensure confidence in blockchain systems. The Blockchain Act intends to regulate the registration and supervision as well as the rights and obligations of service providers who perform activities on blockchain systems.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

As mentioned in question 3.2, the Liechtenstein Government shows great interest in establishing Liechtenstein as a fintech-friendly jurisdiction, and intends to offer fintech projects a great deal of legal certainty whereby the domestic financial markets regulator, the

Liechtenstein Finanzmarktaufsicht (FMA), plays an essential role. In general, the FMA is well-known for its cooperative and constructive approach with regard to realising fintech, particularly blockchain-based projects. For example: entrepreneurs planning to launch a fintech-related project in Liechtenstein may address informal requests to the FMA, which generally will be answered swiftly and competently. The FMA also offers personal meetings where projects can be presented to the FMA at an early stage in order to discuss the most suitable approach – from a regulatory perspective – and to address concerns in this context with the FMA.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

This strongly depends on which products or services are marketed or offered in Liechtenstein and where the business has its registered seat, i.e., if the company is established in an EEA or non-EEA country. If fintech services which qualify as financial services in the meaning of MiFID II are or are intended to be provided, the following does apply:

EEA Countries

If a company registered and licensed in an EEA country intends to market fintech products or services in Liechtenstein which qualify as financial services according to MiFID II (as implemented in Liechtenstein), the company which intends to market or offer financial services to Liechtenstein-based prospects requires a prior notification of the regulator of the home Member State to the FMA. On receipt of the notification, the company may begin to provide the services in question. This notification must contain the following:

- information concerning the planned activities (programme of operations);
- an attestation that the transmitting authority has licensed and supervises the company;
- an attestation that the planned activities are covered by the licence issued by the competent authorities of the home Member State; and
- the names and addresses of tied agents to be appointed, if any, who are domiciled in the home Member State.

Non-EEA Countries

If a company with a registered office or residence in a non-EEA state (third country state) wishes to offer fintech services, which qualify as financial services in the meaning of MiFID II, in or into Liechtenstein, it will need to apply for a licence, which regularly requires the establishment of a subsidiary or branch in Liechtenstein.

There are, however, some exemptions from such licensing requirement, e.g. on the basis of tolerated market practice or reverse solicitation.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

Since July 2018, the EU Data Protection Regulation (Reg. (EU) 2016/679; “GDPR”) has been applicable in Liechtenstein. The GDPR and the domestic Data Protection Act (*Datenschutzgesetz*;

“DSG”) jointly govern and regulate all relevant aspects with respect to processing and protecting personal data. Any information relating to an identified or identifiable natural person (“data subject”) is considered to be personal data. Processing means – according to Art. 4 para. 2 GDPR – any operation or set of operations which is performed with regard to personal data or sets of personal data, such as collection, recording, storage, adaptation or alteration, retrieval, use, disclosure by transmission, dissemination or otherwise making available, erasure or destruction. As a result, the data protection rules are applicable as soon as personal data is processed, regardless of the underlying business or the reasons for its processing.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

The GDPR generally applies to the processing of personal data of all data subjects who are in the EEA. If that is the case, it is irrelevant whether (i) the processor is not established in the EEA, or (ii) the processor is established in the EEA but the processing is carried out outside the Union.

The international transfer of data is restricted, as any transfer of personal data which is subject to processing or which is intended for processing after transfer to a third country is allowed only if certain conditions are met by both the controller and the processor. For example, a transfer of personal data to a third (non-EEA) country may take place if the European Commission has decided that the third country or a territory or one or more specified sectors within such third country ensures an adequate level of data protection, or if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

Infringements of provisions of the GDPR are subject to administrative fines of up to 22 million CHF or, in the case of an undertaking, up to 4% of the total worldwide annual turnover. Furthermore, culprits can be subject to imprisonment of up to six months.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

Liechtenstein has not yet passed any law or ordinance governing the particular aspects of cyber security. However, the DSG stipulates that personal data must be processed in a manner that ensures adequate security. This also includes protection against unauthorised or unlawful processing, accidental loss, destruction or damage by appropriate technical and organisational measures. In this regard the FMA has issued a guidance paper (FMA Wegleitung 2018/3). The FMA in general stipulated that, in accordance with the NIST standard (National Institute of Standards and Technology), security levels must be appropriate to the threat level and that an appropriate emergency management system must be in place in order to resume normal business operations as quickly as possible after an attack.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

Liechtenstein has implemented the EU AML Directives in the Liechtenstein Due Diligence Act (*Sorgfaltspflichtgesetz*; “SPG”)

and Due Diligence Ordinance (*Sorgfaltspflichtverordnung*; “SPV”). The purpose of these legal acts is to combat money laundering, organised crime, and terrorist financing, laying down the requirements to be adhered to when providing certain (financial) services, e.g.:

- a. identification and verification of the identity of the contracting party and the beneficial owner;
- b. establishing a business profile with specified content;
- c. risk-based supervision of business relationships at a level that is commensurate with the risk;
- d. record-keeping requirements and internal organisation; and
- e. requirements for the appointment of auditors, audit companies and audit offices subject to special legislation.

Whether and to what extent the above provisions do apply depends on the underlying business of a provider. It must be evaluated on a case-by-case basis if a fintech business is subject to such due diligence requirements, as those provisions only apply to persons or entities such as, e.g.:

- a. banks and investment firms licensed under the Banking Act;
- b. e-money institutions licensed under the E-Money Act;
- c. undertakings for collective investment that market their unit certificates or units (UCITS and AIFM);
- d. insurance undertakings licensed under the Insurance Supervision Act, insofar as they offer direct life assurance;
- e. payment service providers with a licence under the Payment Service Act;
- f. asset management companies licensed under the Asset Management Act;
- g. real estate agents, insofar as their activities cover the purchase or sale of real estate; and
- h. persons trading in goods, insofar as payment is made in cash and the amount involved is 10,000 CHF or more, irrespective of whether the transaction is executed in a single operation or in several operations which appear connected.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

As already stated above, each business case of a fintech will need to be analysed in detail in order to verify whether the services provided qualify as services subject to, e.g., financial market regulation, and thus require a licence.

Apart from that, each entity pursuing commercial activities within Liechtenstein will need to notify such activities to the *Amt für Volkswirtschaft* in order to obtain a commercial licence (*Gewerbebewilligung*). This is, however, more or less a formality, though certain basic requirements (e.g. holding of offices, appointment of managing directors, etc.) of course need to be complied with.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

Liechtenstein is very restrictive with providing residence permits. Only 56 permits are issued each year. Twenty-eight of those residence permits are awarded within the framework of a lottery procedure and another 28 are awarded by the Liechtenstein

Government, whereby the financial resources and working position of the applicant are the most important factors.

If an entity intends to hire staff not already resident in Liechtenstein, according to the Freedom of Movement of Persons Act (*Personenfreizügigkeitsgesetz*; “PFZG”) and the Foreigners Act (*Ausländergesetz*; “AUG”) a cross-border commuter permit is required. Such permits are issued to employed or self-employed persons (with differences with regard to EEA and non-EEA citizens) who have their place of work and employer in Liechtenstein and return daily to their place of residence outside Liechtenstein. Such permits are regularly issued if certain basic documentation (such as, specifically, an employment agreement) is filed.

As residence permits are hard to obtain, it is quite common in Liechtenstein for companies to hire staff who are resident or plan to become resident in one of the neighbouring countries of Liechtenstein (mostly Austria or Switzerland) and then commute to their place of work on a daily basis.

5.2 What, if any, mandatory employment benefits must be provided to staff?

If the staff is employed by an entity established in Liechtenstein, the provisions of the domestic labour law and in most cases Liechtenstein laws on social security are applicable.

Maximum weekly working hours in Liechtenstein are in general 48 hours, with “normal” working hours of an employee between 40 and 42 hours per week. The employer must grant the employee at least four weeks’ holiday and is obliged to pay – in addition to the monthly salary – 154 CHF (2019) per month as the employers’ contribution to health insurance, and in total 7.0875% (2019) of the employees’ monthly gross salary as the employers’ social security contributions.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

There is no special route for obtaining working permits for individuals in the fintech business sector. For further details, please see the answer to question 5.1.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

The Liechtenstein jurisdiction offers comprehensive protection for intellectual property rights (marks, patents, designs, copy and associated rights), as Liechtenstein has passed a wide range of domestic IP right acts and ordinances (e.g. Trademark Protection Act and Ordinance, Design Act and Ordinance, Copyright and Associated Proprietary Rights Act and Ordinance, etc.) and is, *inter alia*, a member of the European Patent Convention, the Paris Convention for the Protection of Industrial Property, the Madrid Agreement Concerning the International Registration of Marks, the Hague Agreement Concerning the International Deposit of Industrial Designs and the Universal Copyright Convention. Therefore, Liechtenstein is able to provide the basis for locally registered IP rights to obtain international registrations with regards to marks, designs and patents.

With regards to copyrights in Liechtenstein, one local specific has to be mentioned: if an employee creates a copyrighted work while performing their official duties and in fulfilment of their contractual obligations, the rights to this work pass to the employer unless otherwise agreed.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Trademarks & trademark protection

Applications to register a trademark or to amend existing trademarks must be submitted to the Office of Economic Affairs. A trademark is considered to be deposited (registered) as from the date when all statutory preconditions have been fulfilled. The trademark is then recorded in the Liechtenstein trademark register. The protection period for a trademark is 10 years and can be repeatedly extended for a further 10 years. With Liechtenstein as registration basis, it is easily feasible to register a trademark internationally (EUIPO, WIPO).

Designs & design protection

The design of a product can be protected by registration carried out by the Office of Economic Affairs. The design must be new and unique and must not be unlawful or offensive. The Office of Economic Affairs does, however, not examine whether a design indeed is new and sufficiently different from existing designs. Third parties, however, can contest the novelty of a design at any time in court. The protective period of a design amounts to 25 years. The Liechtenstein registration can act as a basis to register the design internationally (EUIPO, WIPO).

Patents

On the basis of a patent protection treaty between Liechtenstein and Switzerland, the competent public authority to issue patents is the Swiss Federal Institute of Intellectual Property (IGE) in Berne. The IGE handles all associated administrative matters and offers information about questions relating to patent law, such as, e.g., whether a desired protection is even covered by a patent protection. The protection generally expires 20 years after the day of application of the patent.

Copyright & associated proprietary rights

The rights of authors and their works in the fields of literature, painting, music etc. are known as copyrights. This protection also encompasses computer programs. Copyrights, however – in contrast to trademarks, designs or patents – are not recorded in a register. A work is protected by copyright from the moment of its creation, and does not have to be recorded on a medium. The protection expires 70 years after the death of the originator.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

In general, with regard to patents, designs and trademarks, the Liechtenstein Court has jurisdiction if the defendant’s domicile or the place where an act infringing such rights was committed is in Liechtenstein. However, it is necessary that patents, designs and trademarks have been registered in Liechtenstein either via a local or an international registration (WIPO).

As Liechtenstein is a member of the Universal Copyright Convention, Liechtenstein authorities grant every (international) copyright the same level of protection, regardless of whether the product was created in Liechtenstein or not.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

IP rights can be exploited and monetised on the basis of licensing agreements, but can of course also be sold.

In general, IP rights can be transferred as any other right, as a whole or in part. Usually, the transmission agreement must be in a written form to be valid. However, with regards to *bona fide* third parties, the transfer shall not be effective until it has been entered into the register (if any).

Copyrights are also transferable and inheritable, whereby no written agreement is required.



Dr. Helene Rebholz

König Rebholz Zechberger Attorneys at Law
Landstrasse 36
9495 Triesen
Liechtenstein

Tel: +423 399 10 83
Email: rebholz@akrz-law.com
URL: www.akrz-law.com

Helene Rebholz is a founding partner of *König Rebholz Zechberger Attorneys at Law*. She holds a law degree from the University of Innsbruck (Austria) and a MAS/LL.M. in European Law. She further qualified as a CAS Fund Business Expert in 2011. Helene Rebholz is admitted to the bar in Liechtenstein and Austria.

Helene Rebholz started practising law in Liechtenstein in 2001. In 2003, she joined the former law firm Batliner Gasser where she soon became Managing Partner. She headed the M&A, Banking, Insurance and Investment Funds Practice Group. In 2015, she founded *König Rebholz Zechberger Attorneys at Law* together with MMag. Benedikt König and Mag. Florian Zechberger.



MMag. Degenhard Angerer

König Rebholz Zechberger Attorneys at Law
Landstrasse 36
9495 Triesen
Liechtenstein

Tel: +423 399 10 85
Email: angerer@akrz-law.com
URL: www.akrz-law.com

Degenhard Angerer has been working as a legal associate ("*Rechtsanwaltsanwärter*") at *König Rebholz Zechberger Attorneys at Law* since 2017. He holds diplomas in law, commercial law and economics from the University of Innsbruck.

Degenhard Angerer started practising law in the framework of a legal internship at the district and regional court in Austria in 2017. Shortly thereafter (August 2017) he joined *König Rebholz Zechberger Attorneys at Law*.



König Rebholz Zechberger Attorneys at Law was established in January 2015.

König Rebholz Zechberger Attorneys at Law specialises in private client litigation (Liechtenstein foundations, trusts, establishments), advice and representation in the field of "financial services" in the widest sense (Banking Law, Investment Funds, "MiFID", Insurance Law) including fintech and crypto/blockchain-related business and M&A transactions. In addition, the law firm has a "generalistic" approach and offers legal advice and represents clients in a broad number of areas of the law.

All partners are experienced practitioners and have been practising law in Liechtenstein and Austria for many years, frequently dealing with complex international cases.

Dr. Helene Rebholz, LL.M. is specialised in the field of Financial Market Law and is a well-renowned expert in Liechtenstein in this regard. In the past years, Dr. Rebholz has developed a particular focus on fintech, particularly blockchain-based projects.

MMag. Degenhard Angerer BSc is working as an associate at *König Rebholz Zechberger Attorneys at Law* and supports Dr. Rebholz in all legal matters in the Financial Market Law area in particular.

Luxembourg

Bonn Steichen & Partners

Pierre-Alexandre Degehet



1 The Fintech Landscape

- 1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).**

Like in most European countries, laws and regulations have significantly increased over the last year, leading to an increasing number of obligations to be complied with by financial actors, including those in Luxembourg. Consequently, the regtech sector – which was intended to release the burden of companies active in the funds industry and professionals in the financial sector – has evolved importantly.

Similarly, considering the leading position of Luxembourg in the insurance sector, insurtech companies have been very active and increasing in the past year, as well as payment services businesses.

Finally, we have noted a considerable increase from clients or potential clients for the implementation of cryptocurrency-related businesses and particularly those related to cryptocurrency exchange platforms, and a constantly growing interest in initial coin offerings and initial coin offerings-related businesses.

- 1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?**

Luxembourg has not prohibited any fintech business *per se*. The legal framework is mainly constituted by existing laws and rules, such as the law of November 10th 2009 on payment services, as amended (**Law 2009**), the law of April 5th 1993 on the financial sector, as amended (**Law 1993**) and the regulations or circulars issued by the Luxembourg financial supervisory authority (*Commission de surveillance du secteur financier, CSSF*) related thereto. The CSSF strives to fit new fintech businesses (such as cryptocurrency businesses) into those existing rules.

Regarding cryptocurrencies and ICOs, the CSSF has, for the time being, been very cautious not to take any position, by issuing warning statements aimed at warning investors against the risks associated with cryptocurrencies and ICOs, based on European Securities and the Market Authority's statements. Even though cryptocurrencies are not *per se* regulated under Luxembourg law, the CSSF will monitor any ICO or cryptocurrency initiative on a case-by-case basis. In addition, it should be specified that in any

case, and with any company, cryptocurrency businesses and ICOs remain subject to rules regarding, for example, anti-money laundering.

In conclusion, although there is no prohibition *per se*, there is uncertainty on the final position of the CSSF hereto, which is likely to evolve over time.

2 Funding For Fintech

- 2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?**

As one of the top countries in Europe as regards the financial sector, Luxembourg is dedicated to creating a favourable environment for fintech start-ups. As a matter of consequence, various options exist regarding both public and private funding.

First of all, the Ministry of the Economy of Luxembourg has set up, in partnership with private entities, the Digital Tech Fund which invests, in particular, in the fields of cybersecurity, fintech, big data, digital health, the media and next-generation communication networks, digital learning, the internet of things or telecommunications and satellite services. The Digital Tech Fund is managed by Expon Capital.

Furthermore, the European Investment Fund (**EIF**) and the *Société Nationale de Crédit et d'Investissement (SNCI)* also created a fund called the Luxembourg Future Fund, investing in innovative sectors, which is designed as an incentive for existing innovative companies from other countries to set up their business in Luxembourg. Moreover, LuxInnovation, which is a public entity promoting Luxembourg as a country in particular regarding innovative technologies, offers packages designed for start-ups at different stages of their development.

- 2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?**

From a mere tax perspective, investments in tech/fintech businesses are treated similarly to other investments in “regular” companies. Moreover, to the best of our knowledge, there are no specific incentive schemes for investors in tech/fintech.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

Depending on the choice of the targeted market (i.e., regulated or non-regulated, such as Euro MTF in Luxembourg), different sets of rules and various requirements will apply. Admission to listing and trading of shares on Euro MTF is less cumbersome than on the regulated market operated by the Luxembourg Stock Exchange (LSE). In such case, the rules and regulations of the LSE (R&R LSE) and the Regulation (EU) No 596/2014 of the European Parliament and of the Council of April 16th 2014 on market abuse (MAR) will apply. Trading and listing on the regulated market of the LSE assumes compliance (among others) with (i) the R&R LSE, (ii) the Luxembourg law of July 10th 2005 on prospectuses for securities (the **Prospectus Law**), and (iii) the Luxembourg law of January 11th 2008 on transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market (the **Transparency Law**).

In order to be admitted to trading and listing on the Luxembourg regulated market, an issuer shall respect the following requirements:

- Corporate form: public limited liability company (*société anonyme*) or partnership limited by shares (*société en commandite par actions*).
- Existence: at least three financial years.
- Capital: foreseeable stock market capitalisation of the shares or, if this cannot be assessed, the capital, including the results from the last financial year, which must amount to at least EUR 1 million (or equivalent in any other currency).

Requirements relating to the shares:

- Free negotiability: no transfer restrictions.
- Fungibility: same features within the same class.
- Capability to trade in a fair, orderly and efficient manner:
 - clear and unambiguous terms;
 - a reliable and publicly available price;
 - correlation between the price of the shares and the price of the underlying assets;
 - transparent value; and
 - adequate settlement and delivery procedures (in case of settlement in kind).
- Distribution to public: the shares must represent at least 25% of the subscribed capital of the issuer.
- Application must cover all shares of the same category already issued.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

To the best of our knowledge, we are not aware of any such sale of business or IPO by the founders of fintech businesses in Luxembourg for the time being.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

As a general rule, as mentioned above, fintech businesses in Luxembourg are likely to fall into the scope of Law 2009 or Law

1993 whether they operate in payment services, electronic money, disruptive financial services or the cryptocurrency sector.

Most fintech businesses will be considered by the CSSF as falling within the scope of application of existing laws or regulations; therefore, it is very unlikely that some fintech businesses would be considered to be operating unregulated fintech activities.

Indeed, the CSSF clearly and repeatedly stated that even though an innovative financial activity may seem unregulated at first sight, it would actually be covered by existing legal provisions (i.e., likely Law 2009 or Law 1993). Therefore, all fintech businesses should proceed to a thorough analysis of the contemplated activity from a legal standpoint and contact the CSSF prior to starting any activity in Luxembourg.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

As in other EU Member States, Luxembourg does not yet provide for specific regulation regarding cryptocurrencies. However, this situation is likely to evolve rapidly. In this context, a recent new law dated March 1st 2019 adopted by the Luxembourg legislator aims to extend the scope of the 2001 law on the circulation of securities, in order to allow account holders to hold securities accounts and to register securities by means of secure electronic recording devices (DLTs), including registers or distributed electronic databases of the blockchain type. This new law operates a legal fiction essential for its proper functioning by recognising that successive registrations of securities in a blockchain have the same effects as those resulting from transfers between securities accounts. For the sake of legal certainty, it expressly confirms that the maintenance of securities accounts within DLTs or the recording of securities in securities accounts through such DLTs does not affect the fungibility of the securities concerned.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

Luxembourg aims to develop a genuine start-up ecosystem. Considering its past and present reputation as a leading financial centre, the country has focused its efforts on the development of fintech start-ups by creating subsidies programmes, launching public-private initiatives (e.g., the Luxembourg House of Financial Technology) and encouraging the major financial and banking actors to develop their own initiatives.

As a result, Luxembourg now has a full ecosystem dedicated to start-ups, but more precisely to fintech start-ups with numerous incubators, awards and both public and private initiatives. However, there is no regulatory sandbox option as of yet in Luxembourg.

Major companies from the banking and financial sectors are increasingly investing in fintech technologies and supporting the newly created ecosystem.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

If the company is established in an EU Member State and has a licence for regulated fintech businesses, it can apply to obtain the European passport for such regulated services before the CSSF.

Once the passport has been obtained, the said company (acting through a Luxembourg subsidiary) may provide such fintech business regulated services in Luxembourg. On the contrary, should the company be established outside the EU and would like to provide fintech business regulated services in Luxembourg, it should incorporate a company that will apply for a specific licence before the CSSF in order to validly operate in Luxembourg. In both cases, the said companies will be subject to all other applicable laws and regulations in Luxembourg. Application for an EU passport is less cumbersome to obtain in comparison with the entire process regarding the obtaining of the licence.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

Like all other EU Member States, Luxembourg is subject to the application of the EU Charter of fundamental rights which states that all EU citizens have a right to the protection of their personal data. Personal data has been a widely discussed subject over the last few years, in particular due to the increase of all new innovative technologies that have an impact on companies and customers. Thus, the legal framework of personal data protection has been moving over the past years.

Today, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (**GDPR**) has applied since May 25th 2018. Additionally, the law dated May 30th 2005 applies concerning the specific provisions for protection of the individual in respect of the processing of personal data in the electronic communications sector (the **E-Privacy Law**).

The GDPR will apply to the processing by an individual, company or an organisation of personal data relating to individuals in the EU. Considering that data has become increasingly valuable for companies in general, it necessarily impacts fintech companies to which the collection and processing of customers' data is of tremendous importance.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

The GDPR, as a regulation, has applied since May 25th 2018 in all EU countries and thus supersedes any national legislation on the matter. As a matter of principle, the GDPR forbids any transfer of personal data outside the EU. That being said, it contains numerous exceptions such as (i) the transfer of data to non-EU countries considered as having an adequate level of protection of personal data, and (ii) the EU-US privacy shield and derogations (i.e. consent, legitimate interest, public interest, public register, vital interest, judicial proceedings, and contract).

The GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or processor in the EU, regardless of whether the processing takes place in the Union or not. The GDPR applies as well to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the EU, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a

payment of the data subject is required, to such data subjects in the EU; or (b) the monitoring of their behaviour as far as their behaviour takes place within the EU. The GDPR applies to the processing of personal data by a controller not established in the EU, but in a place where Member State law applies by virtue of public international law.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

Under the GDPR, sanctions are particularly severe, with administrative pecuniary sanctions up to EUR 20 million or 4% of the annual turnover of the previous financial year.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

The E-Privacy Law contains requirements regarding security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

The main law regarding AML in Luxembourg is the law dated November 12th 2004 regarding the fight against money laundering and terrorist financing, as amended from time to time (the **AML Law**) and supplemented by regulations and various CSSF circulars. The AML Law fully applies to fintech businesses. Furthermore, payment services/electronic money institutions within the meaning of the 2009 Law, in particular, are subject to the strict control of the fulfilment of their AML/KYC obligations from the CSSF at both the application stage and in the course of their business.

In connection with Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (the **AML 4th Directive**), and Directive (EU) 2018/843 of the European Parliament and of the Council of May 30th 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (the **AML 5th Directive**), Luxembourg implemented on January 13th 2019 a law aiming at setting up a register of beneficial owners. This law creates a register of beneficial owners, which aims to preserve and make available information on the beneficial owners of the specific registered entities.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

This is not applicable.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

All employees employed in Luxembourg, whether they are residents,

border residents, European nationals or third-country nationals, are subject to the provisions of the Luxembourg labour law, which sets the standards aimed at governing both individual and collective labour relations. Due to its overall presence in everyday life, the Luxembourg labour law consists of a series of laws, Grand-Duchy regulations and ministerial decrees, making the entire process difficult to facilitate. To this end, the Ministry of Labour and Employment edited a labour code, the first version of which entered into force on September 2016.

There are two main categories of employment agreement. As a matter of fact, it is strongly recommended to evidence the labour relationship by the conclusion of a written employment agreement. A fixed-term contract can only be concluded in exceptional cases and must be in writing, otherwise it will be deemed as an indefinite employment agreement. As a general comment, labour law rules in Luxembourg offer a certain degree of protection to the employees.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Remuneration as global compensation includes cash remuneration and any other benefits or accessory compensations (lunch voucher, transportation, etc.). There are no legal obligations for an employer to grant bonuses to its employees, which remains at the employer's sole discretion and are considered as a goodwill gesture. There are about 10 statutory public holiday days a year which are in addition to the minimum holiday entitlement. The legislation provides all employees with an annual paid vacation of at least 25 working days, which can occur after three months of uninterrupted work with the same employer.

The social security code makes it mandatory for all employees to be insured with the Social Security Services (Accident Insurance, Pension National Insurance, Health National Insurance).

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

The hiring possibilities regarding European citizens (including European Economic Space Member State citizens and Switzerland) or third-country nationals are different.

European citizens can reside, move and work freely in the European Union, while third-country nationals may enter Luxembourg for less than three months with a valid passport and a visa, if it is required. If a third-country national wishes to stay and work for more than three months in Luxembourg, he or she must apply to the Immigration Directorate of the Ministry of Foreign and European Affairs of Luxembourg for a (temporary) authorisation to stay (including an authorisation to work), prior to entering Luxembourg.

Notwithstanding the above, the Minister may grant a residence permit to a national qualified from a third country who proposes to work in a sector or profession characterised by recruitment problems. When the job requires a high degree of competence, a residence permit for a "highly qualified worker" may be granted under certain conditions.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Luxembourg law provides for a standard protection of innovations

and inventions mainly constituted by patent protection and design protection on one side, and copyright and related rights on the other side.

Registering a patent allows its holder to prevent others from using an invention for 20 years in exchange for the disclosure of the said invention. To be eligible for the registration of a patent, such invention shall be new, involve an inventive step and have an industrial application.

Design protection allows for the protection of a two-dimensional representation (i.e., design) or three-dimensional representation (i.e., model) related to a product's visual appearance. The protection lasts for a maximum of 25 years.

Copyright mainly protects works of literature, music or art but also, e.g., software, designs, maps, graphic elements, and plans, and as such contributes to the innovation protection legal framework in Luxembourg. The only two conditions are (i) originality, and (ii) taken form. Therefore, ideas are not protected by copyright (or by any other IP rights). That being said, ideas may be deposited within the i-DEPOT system which may prove very useful, as evidence, when the ideas turn into inventions or other innovations and may then be protected as such. The i-DEPOT shall be used at an early stage to secure as much as possible for the future invention or innovation which is still at the idea stage.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Please see question 6.1 above. Ownership of IP rights is proved by the deposit of the contemplated IP rights with the Benelux Office of Intellectual Property.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

As mentioned above in question 6.1, patent as well as design protection and copyright require a registration at national level in Luxembourg. That being said, an applicant may also file a European patent application which may cover up to 40 countries, or an international patent application under the Patent Cooperation Treaty, which has been signed by more than 130 countries around the world including Luxembourg. In both cases, with a single application, a patent may be requested in all Member States/signatory countries.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

IP rights may be exploited directly by the owner of the said IP rights or by third parties, when the owner of such IP right has agreed to authorise its use by third parties. Such use is generally determined and limited by a contractual agreement to be signed between the owner of the IP right and the user, under certain terms and conditions, for a specific consideration (price payment determined by the parties). There are no particular restrictions under Luxembourg law for the exploitation or monetisation of IP rights, which are often set up through contractual agreements, except in case of non-respect of Luxembourg public order rules.

**Pierre-Alexandre Degehet**

Bonn Steichen & Partners
2 rue Peternelchen – Immeuble C2
L-2370 Howald
Luxembourg

Tel: +352 260 251
Email: padegehet@bsp.lu
URL: www.bsp.lu

Pierre-Alexandre is a Partner and a member of the Corporate M&A, Private Equity, Capital Markets, Banking & Financial Services practices. He created and developed the Startup & Fintech practice and he is Head of the French desk. In addition to general corporate law, he specialises in M&A, capital markets, stock exchange regulations and corporate governance involving listed and private companies. Pierre-Alexandre has participated in numerous stock exchanges transactions, hostile and friendly takeovers, equity investments in listed companies, contribution or demerger transactions, capital increases, public and private placements of equity and debt securities.

Additionally, Pierre-Alexandre has been involved in a number of capital markets transactions advising international and Luxembourg financial institutions and companies. He handles equity offering and listing matters.

In relation to the Startup & Fintech practice, Pierre-Alexandre handles matters related to fintech, blockchain and cryptocurrency assets, and financial regulatory issues relating to electronic money or payment services and banking.



Bonn Steichen & Partners (**BSP**) is a full-service law firm committed to providing the highest quality legal services to domestic and international clients in Luxembourg.

With a partner-led service as a hallmark, our attorneys have developed specific expertise in banking & finance, capital markets, corporate, dispute resolution, fintech & start-ups, investment management, M&A, labour law and tax.

Our crucial ability to adapt to new laws and regulations enables us to provide our clients with timely and integrated legal assistance.

Our client base includes domestic and foreign clients from all business sectors, including some of Luxembourg's largest corporations and some of the world's leading international groups.

BSP is independent and non-affiliated to any other local or international law firms allowing us to work with the world's leading law firms in multi-jurisdictional transactions in the best interest of our clients.

Please visit our website www.bsp.lu for more information.

Malaysia

Timothy Siaw



Christina Kow



Shearn Delamore & Co.

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Developments in 2018 in terms of sectors were:

- Payments: Telenor Microfinance Bank, in partnership with Valyou Malaysia, has introduced a blockchain-based cross border remittance service, developed by Alipay. It is expected that the blockchain technology will boost efficiency of remittances from Malaysia to Pakistan.
- Banks: locally licensed banks continue to adopt, and/or support, fintech in their business. PayNet Malaysia launched a DuitNow function which was adopted by locally licensed banks. DuitNow enables consumers to make bank transfers only using a mobile number, without having to remember unwieldy bank account numbers.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

The Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019 issued by the Securities Commission Malaysia (SC) came into force on 15 January 2019.

Cryptocurrency exchanges are temporarily prohibited from accepting new investors and will only be allowed to facilitate the withdrawal or transfer of client assets with the written instruction of the investor, until the regulatory requirements are published.

The SC also announced that no person can conduct initial coin offerings without its authorisation.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

More than 97% of Malaysian businesses are small or medium-sized businesses (SMEs). Governmental action and support for SMEs

have been available through policies (including the SME Masterplan 2012–2020) co-ordinated by SME Corporation Malaysia, and implemented by specified agencies of the government and the banking sector. Malaysia has both conventional and Islamic financial and capital markets providing debt and equity financing.

Financial institutions like banks and development financial institutions (which have specified sector objectives like the Small Medium Enterprise Development Bank Malaysia Berhad) provide debt financing. An established debt capital market also exists, in both conventional and *Shari'ah* compliant issues.

Equity financing can be raised by listing on the stock exchange of Bursa Malaysia Securities Berhad, which is further discussed in question 2.3 below, venture capital investment, or utilising an equity crowdfunding platform approved by the SCM under the equity crowdfunding framework.

Specific examples of funding sources include:

- Peer-to-peer (**P2P**) financing under the SCM guidelines.
- Malaysia Debt Ventures Berhad, Malaysia's leading technology financier, has various schemes, including an Intellectual Property Financing Scheme of RM 200 million, to enable companies with IP rights (**IPRs**) to use their IPRs as additional collateral to obtain financing.
- In addition, one programme under the SME Masterplan is the SME Investment Partner, which provides early-stage financing through the establishment of investment companies to invest in potential SMEs, not limited to fintech businesses. Various governmental and government established entities provide loans, grants and guarantee services to SMEs, disbursed directly or through the banking system.

Entities that focus specifically on financing to the technology sector include:

- Cradle Fund Sdn Bhd. (**Cradle**), owned by the Ministry of Finance. Cradle focusses on pre-seed, early, seed and start-up financing, and provides non-financial assistance to local tech start-ups. Its CIP 300 programme provides debt seed financing, and its Direct Equity 800 (**DEQ800**) programme launched in 2017 to early-stage start-ups that meet the applicable criteria.
- The Malaysian Digital Economy Corporation Sdn Bhd. (**MDEC**), wholly owned by the government, which focusses on building a sustainable digital ecosystem.
- The Malaysia Venture Capital Management Berhad (**MAVCAP**).
- The Malaysian Technology Development Corporation (**MTDC**).

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

SME Corporation Malaysia is the Central Coordinating Agency under the Ministry of International Trade and Industry (MITI) in Malaysia that formulates overall policies and strategies for SMEs, and coordinates the implementation of SME development programmes across all related government ministries and agencies.

SMEs in Malaysia are given preferential tax rates as well as a wide range of tax incentives for businesses in the manufacturing, services and agriculture sectors. Fiscal incentives are pioneer status, investment tax allowance, reinvestment allowance, accelerated capital allowance and industrial building allowance – for example:

- The angel tax incentive granted to angel investors in technology based start-ups administered by Cradle.
- Pioneer status with income tax exemption of various percentages by the Malaysian Industrial Development Authority (MIDA).
- Partial corporate tax exemption for entities in the Malaysian Digital Hub under the MDEC.
- Malaysia Tech Entrepreneur Programme under the MDEC to attract individuals and help them set up and develop their start-ups in Malaysia, subject to specified conditions.
- The Multimedia Super Corridor (MSC) Malaysia status recognition by the MDEC for ICT and ICT-facilitated businesses that meet specified criteria available to local and foreign companies. The MSC is located in cybercities and cybercentres which comply with a set of minimum standards administered by the MDEC. Specific incentives are granted to MSC Malaysia Status entities, including the MSC Malaysia Bill of Guarantees, 100% exemption from taxable statutory income, 100% investment tax allowance, eligibility for R&D grants, and the freedom to source capital and borrow funds under specific waivers from the foreign exchange administration requirements of Malaysia.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

The conditions for a business to IPO in Malaysia would depend on the market it intends to list on. Bursa Malaysia Securities Berhad has three securities markets: (i) the Main Market; (ii) the ACE Market; and (iii) the LEAP Market.

The LEAP Market was introduced to provide SMEs and other companies, from all industries including fintech, with greater fundraising access and visibility. Only sophisticated investors (comprising entities set out in Part 1 of Schedules 6 and 7 to the Capital Markets and Services Act 2007 (CMSA) may invest in the LEAP Market. The LEAP Market provides opportunities for start-up fintech companies, which may generally find it difficult to meet the Main Market or ACE Market listing requirements.

To list on the LEAP Market, an applicant must:

- be a public company incorporated in Malaysia;
- not be: (i) a subsidiary or holding company of a corporation currently listed on the Main Market or ACE Market of the Exchange, and the listing of such applicant will result in the existing listed corporation within the group ceasing to have a separate autonomous business of its own and not be capable of sustaining its listing in the future; (ii) an investment holding corporation with no immediate or prospective business operations within its group; or (iii) an incubator, including a technology incubator;

- engage an adviser, approved by Bursa Malaysia Securities Berhad, to carry out both the initial listing activities and post-listing activities, to assess the suitability for listing and submit the application for admission to the LEAP Market; and
- achieve a minimum shareholding spread of 10% of its ordinary shares upon admission to the LEAP Market.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

There were no notable exits in 2018.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

Other than the order issued by the SC referred to in question 3.2 below, there is no specific regulatory framework for fintech businesses in Malaysia, apart from the incentives and functions of governmental or government-owned entities referred to under sections 1 and 2 above. Where a fintech business falls within any business, or includes an activity that is regulated or licensed in Malaysia, the regulatory and legal requirements to conduct such business or activity must be complied with in accordance with the applicable Malaysian laws.

Fintech activities which involve banking, investment banking, insurance or *takaful*, money changing, remittance, operating a payment system or issuing payment instruments business will come under the purview of the Central Bank of Malaysia, Bank Negara Malaysia (BNM). The Financial Services Act 2013 (FSA) is the statute that regulates and provides supervision of conventional financial institutions, payment systems and operators thereof and the oversight of the money market and foreign exchange market. BNM also regulates the Islamic financial sector, largely under the Islamic Financial Services Act 2013.

In 2016:

- BNM launched the Financial Technology Regulatory Sandbox Framework (the **BNM Framework**) to provide a regulatory environment that is conducive for the deployment of fintech innovations. This includes reviewing and adapting regulatory requirements that may unintentionally inhibit innovation or render them non-viable. The BNM Framework provides for innovation by fintech companies to be deployed and tested in a live environment, within specified parameters and timeframes, and whether to allow the product, service or solution to be introduced to the market on a wider scale. If allowed, the participating fintech companies intending to carry out regulated businesses will be assessed based on applicable licensing, approval and registration criteria under the applicable laws.
- BNM has also established the Financial Technology Enabler Group (FTEG) to support innovations that will improve the quality, efficiency and accessibility of financial services in Malaysia.

The SC, which regulates the Malaysian capital markets, has adopted a Digital Markets Strategy intended to enhance access to financing, increase investor participation, augment the institutional market and develop synergistic ecosystems for the capital markets in Malaysia. Stockbroking, provision of investment advice, financial planning, dealing in derivatives and advising on corporate finance are among the activities regulated by the SC under the CMSA.

In 2015:

- the SC launched the “Alliance of FinTech Community” (aFINity@SC), an initiative to catalyse greater interest towards the development of emerging technology-driven innovations in financial services, whether existing or prospectively developing in Malaysia. In December 2017, the SC invited parties interested in establishing and operating an Alternative Trading System (ATS) in Malaysia to participate in its regulatory sandbox sessions.
- Malaysia became the first country in ASEAN to have a regulatory framework for equity crowdfunding for the purpose of early-stage financing for start-ups and entrepreneurs.
- Since 2015, there has existed a regulatory sandbox set up by the SC for fintech providers on whom regulation is imposed on a graduated scale, in line with the growth of the market and complexity of the product.

In 2016, the SC introduced the regulatory framework for P2P lending, allowing SMEs access to this avenue for debt funding.

In May 2017, the SC introduced the Digital Investment Management framework, setting out licensing and conduct requirements for the offering of automated discretionary portfolio management services to investors.

In January 2019, the SC announced the issuance of a Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019 to prescribe certain digital currency and digital tokens as securities for the purposes of securities law.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

Yes, the Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019 came into force on 15 January 2019. The order prescribes digital currency and digital tokens, each as defined therein, as securities and thus falling within the purview of the SC under the CMSA.

All the provisions of the CMSA applicable to securities will apply to each such digital currency save for Division 3 of Part VI of the CMSA. The SC is expected to issue guidelines for initial coin offerings by the end of the first quarter of 2019.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

Malaysia is very receptive to fintech innovation and technology. Specific agencies and incentives are in place to facilitate the development of the digital economy. MDEC is an agency under the Ministry of Communications and Multimedia Malaysia which has been entrusted to develop, coordinate, and promote Malaysia’s digital economy, information and communications technology industry, and the adoption of digital technology amongst Malaysians. Its Malaysia Digital Hub has been set up to attract technology investments, support local technology innovation and create a sustainable digital ecosystem in Malaysia.

Both BNM and the SC have policies encouraging fintech by the initiatives referred to above, and offer regulatory flexibility to entities approved in their respective sandboxes.

The SC announced, in December 2018, a successful completion of its pilot project, Project Castor. Project Castor is a project whereby the

SC sought to explore the technical implementation and feasibility of using distributed ledger technology as the underlying market infrastructure for unlisted and over-the-counter (OTC) markets. A blueprint entitled Capital Market Architecture Blueprint in a Decentralised World has been issued, and it outlines the regulator’s vision for “a future multi-tiered market environment” which contains both centralised and decentralised markets, with the latter underpinned by distributed ledger technology. According to the blueprint, the regulator used equity crowdfunding and Ethereum-based tokens to represent equity and monies. It also used smart contracts to codify the rules of offerings and distribute the appropriate tokens and assets once offerings were closed, as well as for KYC/AML requirements.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

A fintech business, or financial services business established outside Malaysia offering fintech products and services, must comply with the Malaysian laws applicable to the service or product offered. Malaysian licensing laws apply to financial services and the regulated activities set out in the CMSA, unless any waiver or exemption specifically applies by law or is granted by the regulator.

BNM’s regulatory sandbox is open to all fintech companies including those without any presence in Malaysia, but fintech companies with potential to contribute to the creation of high value-added jobs in Malaysia will be viewed more favourably by BNM. Most of the financial services businesses regulated by BNM and the regulated activities supervised by the SC have to be conducted by a locally incorporated entity, so any foreign entity will have to establish a local company to apply for the relevant licence or approval.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

Yes. The Personal Data Protection Act 2010 (PDPA) came into force in 2013 and regulates the collection, use, processing and disclosure of personal data in Malaysia in respect of commercial transactions. The legal basis for the PDPA is to ensure information security, network reliability and integrity through the regulation of processing of personal data by a data user in any commercial transaction and protection of personal data. “Commercial transactions” by definition includes any transaction of a commercial nature, whether by way of a contract or not, including any matter relating to the supply or exchange of goods or services, agencies, investment, finance, banking and insurance, but does not include a credit reporting business under the Credit Reporting Agencies Act 2010. As such, the PDPA would be applicable to fintech businesses who are in operation within Malaysia. “Personal data” has been defined widely as any information in respect of commercial transactions, which:

- (a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;
- (b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject; but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

The PDPA applies to all data users in Malaysia. Moreover, the PDPA applies to data users not established in Malaysia, but which use equipment in Malaysia to process personal data other than for the purposes of transit through Malaysia.

In general, the transfer of data out of Malaysia is not allowed unless the transfer is to a place specified by the Minister and notified by Gazette, namely to such countries that have in place substantially similar data protection laws as the PDPA, or an equivalent adequate level of protection. There is currently no gazette notification of any permitted country released by the Minister to date.

The PDPA provides that a data user may transfer personal data outside of Malaysia under the following conditions:

- (a) the data subject has given their consent for the transfer;
- (b) the transfer is necessary for the performance of a contract between the data subject and the data user;
- (c) the transfer is necessary for the conclusion or performance of a contract between the data user and a third party, which:
 - (i) is entered into at the request of the data subject; or
 - (ii) is in the interests of the data subject;
- (d) the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights;
- (e) the data user has reasonable grounds for believing that in all circumstances of the case:
 - (i) the transfer is for the avoidance or mitigation of adverse action against the data subject;
 - (ii) it is not practicable to obtain the consent in writing of the data subject to that transfer; and
 - (iii) if it was practicable to obtain such consent, the data subject would have given his consent;
- (f) the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner which, if that place is Malaysia, would be a contravention of the PDPA; and
- (g) the transfer is necessary in order to protect the vital interests of the data subject; or the transfer is necessary as it is in the public interest in circumstances as determined by the Minister.

On 4 April 2017, the Personal Data Protection Commission issued the Personal Data Protection (Transfer of Personal Data To Places Outside Malaysia) Order 2017, a public consultation setting out jurisdictions which it is considering recommending to be approved as places to which personal data may be transferred outside Malaysia. Among the criteria considered by the Commissioner in preparing a list of those places are:

- (i) places that have comprehensive data protection law (which can be from a single piece of comprehensive personal data protection legislation, or otherwise a combination of several laws and regulations in that place);

- (ii) places that have no comprehensive data protection law but are subject to binding commitments (multilateral/bilateral agreements and others); and
- (iii) places that have no data protection law but have a code of practice or national co-regulatory mechanisms.

The Personal Data Protection (Transfer of Personal Data To Places Outside Malaysia) Order 2017 has not been finalised to date.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

Failure to comply with the PDPA will result in the imposition of a fine between RM 10,000 to RM 500,000 and/or imprisonment of up to three years, depending on which section/rule has been breached. Pursuant to Section 133 of the PDPA, where a body corporate commits an offence under the PDPA, any person who at the time of the commission of the offence was:

- (a) a director, chief executive officer, chief operating officer, manager, secretary;
- (b) other similar officer of the body corporate;
- (c) was purporting to act in such capacity; or
- (d) was responsible for the management of any of the affairs of the body corporate,

may also be charged severally or jointly and be deemed to have committed that offence in the event the body corporate is found liable.

The said person may escape liability if he proves that the offence was committed without his knowledge, consent or connivance and that he had taken all reasonable precautions and exercised due diligence to prevent the commission of the offence.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

Yes. The following cyber security laws or regulations have general application in Malaysia:

- (a) Communications and Multimedia Act 1998;
- (b) Communications and Multimedia Commission Act 1998;
- (c) Computer Crimes Act 1997;
- (d) Copyright Act 1987;
- (e) Consumer Protection Act 1999;
- (f) Consumer Protection (Electronic Trade Transactions) Regulations 2012;
- (g) Digital Signature Act 1997;
- (h) Electronic Commerce Act 2006;
- (i) Malaysian Communications and Multimedia Content Code (Version 6, published in 2012);
- (j) Penal Code;
- (k) Personal Data Protection Act 2010;
- (l) Personal Data Protection Regulations 2013;
- (m) Personal Data Protection Standard 2015; and
- (n) Strategic Trade Act 2010.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

Malaysia is a member of the Financial Action Task Force (FATF) and the Asia/Pacific Group on Money Laundering. The Anti-Money

Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (**AMLA**) reflects the FATF recommendations on money-laundering and anti-terrorism financing. The main offence of money laundering is engaging in a transaction that involves, acquires, receives, possesses, disguises, transfers, converts, exchanges, carries, disposes of or uses, removes from, or brings into, Malaysia, proceeds of an unlawful activity or instrumentalities of an offence. Further, the Minister of Home Affairs may declare an entity known to have committed, participated in or facilitated, or known to have attempted to commit, participate in or facilitate, a terrorist act to be a specified entity. These include United Nations Security Council Resolutions (**UNSCR**) 1267 and 1988 (and the Al-Qaida Sanction List) as well as a Malaysian list in line with UNSCR 1373. No citizen or entity incorporated in Malaysia may knowingly provide or collect any property for use by a specified entity.

Entities providing financial services, and licensed stockbrokers, derivatives dealers and fund managers under the CMSA are reporting institutions under the AMLA. Entities designated as reporting institutions have to conduct customer due diligence, report suspicious transactions to BNM and maintain specific records in accordance with the provisions of the Act and the requirements of BNM. Certain obligations are prescriptive, while others are risk-based (for example, enhanced due diligence has to be conducted where aspects of a transaction are classified as high-risk). Specific anti-money laundering requirements apply to reporting institutions that exchange digital currency for fiat money, exchange money for digital currency, or exchange one digital currency for another digital currency in Malaysia.

The Malaysian Anti-Corruption Commission (**MACC**) enforces the Malaysian Anti-Corruption Commission Act 2009 (the **MAC Act**). The main offences under the MAC Act relate to giving or receiving gratification. Gratification is widely defined in the MAC Act, and includes:

- any gift, reward, property or interest in property, financial benefit, or any other similar advantage;
- any office, dignity, employment, contract of services, and agreement to give employment or render services in any capacity;
- any payment, release, discharge, discount, deduction or liquidation of any liability;
- any valuable consideration of any kind;
- any forbearance to demand any money or money's worth or valuable thing;
- any other service or favour of any description, including protection from any penalty or disability incurred or apprehended or from any action or proceedings of a disciplinary, civil or criminal nature, whether or not already instituted, and including the exercise or the forbearance from the exercise of any right or any official power or duty; and
- any offer, undertaking or promise, whether conditional or unconditional, of any gratification within the meaning of any of the preceding items.

In proceedings relating to any of the offences described above, any gratification received or solicited, given, offered or promised, by or to an accused is presumed to have been done so corruptly, unless the contrary is proved. The MAC Act imposes an obligation on persons to report bribery transactions to the MACC or the police. Failure to do so will result in a fine or imprisonment or to both on conviction of the offence. The MAC Act applies to the commission of offences whether within or outside Malaysia.

The MACC maintains a database of offenders found guilty of corruption.

The **Malaysian Penal Code** also prohibits the commission of the criminal offences of bribery and corruption, such as taking a gratification in order to, by corrupt or illegal means, influence a public servant, and criminal breach of trust. Whoever commits criminal breach of trust shall be punished with imprisonment for a term of up to 10 years and with whipping, and shall also be liable to a fine. A criminal breach of trust is committed where a person dishonestly misappropriates, or converts to his own use, any property that he is entrusted with or where the person has dominion over such property, or the person dishonestly uses or disposes of that property in violation of any direction of law or of any legal contract.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

There is no law specifically applicable to fintech businesses only in Malaysia. A fintech business operating in Malaysia must comply with the Malaysian laws and regulations relevant to its activities, location and legal structure. The provisions of the Electronic Commerce Act 2006 govern the validity of electronic communications and transactions.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

The following legislation is applicable in relation to employment in Malaysia:

- (a) Employment Act 1966 (**EA**);
- (b) Children and Young Persons (Employment) Act 1966;
- (c) Industrial Relations Act 1967;
- (d) Employment (Restriction) Act 1968;
- (e) Occupational Safety and Health Act 1994;
- (f) Factories and Machinery Act 1967;
- (g) Minimum Wages Order 2016;
- (h) Minimum Retirement Age Act 2012; and
- (i) Workman's Compensation Act 1952.

The EA applies to all employees with a monthly wage of MYR 2,000 or below. The minimum notice period should be as prescribed in the employment contract or the EA, whichever is longer. The minimum notice period prescribed under the EA is as follows:

- (a) four weeks' notice (for employment of less than two years);
- (b) six weeks' notice (for employment of two years or more but less than five years); and
- (c) eight weeks' notice (for employment of five years or more).

5.2 What, if any, mandatory employment benefits must be provided to staff?

Under the EA, employees in Malaysia are entitled to paid annual leave and sick leave (depending on the number of years of service), payment for overtime work, maternity leave of 60 days, and paid holiday of at least the 11 gazetted public holidays including National Day and Labour Day.

The Employees Provident Fund Act 1991 requires employees and their employers to contribute towards their retirement savings, and

allows the employees to withdraw these savings at retirement or for specified purposes before then.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

The Employment (Restriction) Act 1968 requires non-Malaysian citizens to obtain a valid work permit before they can be employed.

Fintech companies may be eligible to apply for MSC Status from the MDEC. Companies with MSC Status are eligible to apply for special employment passes and exemptions to employ foreign knowledge workers.

Under the Malaysia Tech Entrepreneur Programme provided by MDEC, a tech founder with no track record of established business may apply for a one-year pass, and an individual who is an established entrepreneur may obtain a five-year pass to stay in Malaysia, subject to meeting specified application requirements as set out in <https://www.mtep.my/>.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Innovations and inventions are protectable under the patent, copyright and industrial design laws as well as confidential information under the common law in Malaysia. This would include the Patents Act 1983, the Copyright Act 1987 and the Industrial Designs Act 1996.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Copyright

Under the Copyright Act 1987, copyright shall initially vest in the author of the copyrighted work. The Copyright Act 1987 provides for presumptions in cases of commissioned work or work made in the course of employment. As such:

- (a) where the work is commissioned by a person who is not the author's employer, copyright is deemed to be transferred to the person who commissions the work; or
- (b) where the work is made in the course of the author's employment, the copyright is deemed to be transferred to the author's employers.

However, this is subject to any contrary agreement.

Where the work is made by or under the direction or control of the government, government organisation or international body, the copyright shall initially vest in the government, government organisation or international body.

Trade Marks

Under the Trade Marks Act 1976, any person claiming to be the proprietor of a trade mark used or proposed to be used by him may apply to the Registrar for the registration of that mark. While the proprietor of a registered trade mark is the person whose name appears on the Register as the owner, the concept of proprietorship for the purposes of an application for registration depends on who is entitled to the exclusive use of the trade mark, i.e. the first person to

use the mark in the course of trade and to develop business goodwill in relation to that mark.

Patents

Under the Patents Act 1983, the right to a patent belongs to the inventor unless the invention is made by an employee (including government employees, and employees of a government organisation or enterprise) or pursuant to a commission, in which case the right to the invention will be deemed to accrue to the employer or the person who commissioned the work, subject to any contrary agreement.

Industrial Designs

Under the Industrial Designs Act 1996, the author of the industrial design is entitled to make an application for registration, except for:

- (a) industrial designs created pursuant to a commission or money or money's worth – the person who commissioned the work is the original owner;
- (b) industrial designs created by an employee in the course of employment – the employer is the original owner; and
- (c) industrial designs subject to any contrary agreement.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

Except for copyright where registration is voluntary and there are common law rights such as passing off, one must have a patent, trade mark or industrial design registration in Malaysia to enjoy protection of these rights in Malaysia.

Malaysia is a member of the following Intellectual Property international treaties/conventions/agreements:

- (a) Paris Convention for the Protection of Industrial Property 1883.
- (b) Agreement on Trade-Related Aspects of Intellectual Property Rights.
- (c) Nice Agreement Concerning the International Classification of Goods and Services for the Purposes of the Registration of Marks.
- (d) Vienna Agreement Establishing an International Classification of the Figurative Elements of Marks.
- (e) Madrid Protocol.
- (f) Patent Cooperation Treaty.
- (g) Berne Convention for the Protection of Literary and Artistic Works 1886, as revised by the Paris Act of 1971.
- (h) World Intellectual Property Organisation (WIPO) Copyright Treaty.
- (i) WIPO Performances and Phonograms Treaty.

Malaysia is in the process of implementing the Madrid Protocol (the Protocol Relating to the Madrid Agreement Concerning the International Registration of Marks) in the near future. The Madrid Protocol is an international treaty administered by the International Bureau of the WIPO and provides for a multinational system for trade mark owners to obtain trademark registrations in various countries with a single application.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

There are currently no specific rules or restrictions on monetisation or exploitation of IP in Malaysia. IP in Malaysia is generally exploited either by way of creating licences for the use of IP or co-development

of new inventions/products, or selling the IP rights for a value. There has been significant progress in the development and the implementation of IP monetisation mechanisms. Essentially, the aim was to harness the value of locally-nurtured IP as revenue-generating streams. As such, the MDEC developed the IP valuation Module which was launched on 7 March 2013. This was used to assist SMEs in evaluating their IP.

The Industrial Designs (Amendment) Act 2013 came into force on 1 July 2014 and provides for the amendments that allow for a registered industrial design to be the subject of a security interest in the same way as other personal or movable property. This interest has to be recorded in the Register of Industrial Designs.

Additionally, the IP Financing Scheme (**IPFS**) was introduced specifically for SMEs to provide them with easier access to credit through their IP assets instead of movable assets. The sum of RM19 million was allocated for training programmes for local IP

evaluators conducted by the Intellectual Property Corporation of Malaysia (**MyIPO**), as well as to create an IP right market platform. The IP right market platform is vital to enable SMEs to fully utilise the opportunities to set up their IPR for sale and licensing. The MyIPO has recently begun implementation of an integrated online system to facilitate the registration and verification of intellectual property, which is expected to be finalised in 2019.

Furthermore, the Malaysian Competition Commission (**MyCC**) recently published a draft guideline on intellectual property rights and competition law in 2018, which laid out guidelines on any competition issues under the Competition Act 2010 relating to intellectual property rights. The draft guideline provides for situations in which certain acts in relation to intellectual property rights are deemed anti-competitive and may attract liability under the Competition Act 2010.



Timothy Siaw

Shearn Delamore & Co.
Level 7, Wisma Hamzah-Kwong Hing, No. 1
Leboh Ampang
50100 Kuala Lumpur
Malaysia

Tel: +603 2027 2660
Email: timothy@sheandelamore.com
URL: www.sheandelamore.com

Timothy graduated with a B.Sc. and LL.B. from Monash University, Australia. He has been admitted as a Barrister & Solicitor of the Supreme Court of Victoria, Australia (non-practising) and was admitted to practice in the High Court of Malaya in 1991. Timothy has extensive experience in all areas of Intellectual Property and his practice extends to the new and emerging areas of Technology & Communications.



Christina Kow

Shearn Delamore & Co.
Level 7, Wisma Hamzah-Kwong Hing, No. 1
Leboh Ampang
50100 Kuala Lumpur
Malaysia

Tel: +603 2027 2786
Email: christina@sheandelamore.com
URL: www.sheandelamore.com

Christina was admitted to practise in the High Court of Malaya in 1986. She holds an LL.B. and B.Com. from the University of Melbourne, Victoria, Australia. She is the head of the financial services practice in Shearn Delamore & Co. and regularly advises multi-national banks and other financial institutions and capital market intermediaries on regulatory matters. Her areas of advice cover foreign exchange administration, the regulation of financial institutions, payment systems, securities (including collective investment schemes, securities borrowing and lending, licensing of regulated activities) and derivatives.

She also has extensive experience in financing transactions, having acted for borrowers as well as lenders in different transactions, including onshore and offshore financing transactions under conventional as well as *Shari'ah* compliant facilities.

Shearn Delamore & Co.

Shearn Delamore & Co. is one of the largest award-winning full service law firms in Malaysia with more than 100 lawyers and 290 support staff. The firm has the resources to manage complex cross-border transactions, projects and matters.

The firm's clients include multinationals, private equity firms, government agencies and individuals. It is regularly instructed by and works with international law firms. The firm's global reach and network include member firms of the World Law Group, the World Services Group, the Employment Law Alliance and other international organisations.

Shearn Delamore & Co.'s diverse experience and interdisciplinary collaborations enables the firm to provide its clients with a complimentary range of skills to meet their needs. The firm is consistently ranked highly by *Chambers and Partners*, *International Financial Law Review (IFLR) 1000*, *The Legal 500 Asia Pacific* and *Asialaw Profiles*.

Malta

Dr. Andrew J. Zammit



Dr. Kurt Hyzler



GVZH Advocates

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Malta provides a very attractive environment for technology-based businesses with a European marketing strategy. The island has seen significant growth in the technological sector, including an exponential rise in fintech businesses, including both start-ups and more established businesses.

The predominant type of fintech businesses currently established in Malta are payment institutions (“PI/PSPs”) and electronic money institutions (“EMIs”), both of which are classified as “financial institutions”. Rolling spot forex and binary option models are also present, albeit to a lesser extent than PSPs and EMIs.

With the introduction of the Second Payment Services Directive (“PSD2”) framework, it is expected that there will be an increase in the number of operators in the payment services space establish themselves in Malta.

After 12 months of very intense work by the Malta Financial Services Authority (“MFSA”) and a number of legal and regulatory practitioners, July 2018 saw the Maltese Parliament approve three separate laws aimed at regulating blockchain and cryptocurrency technologies, providing an environment of certainty for an industry that has been fraught with its fair share of opacity and risk.

The three laws are distinguished by their regulatory objectives, covering different aspects of these industries:

1. The Malta Digital Innovation Authority Act (“MDIA Act”) serves to establish the Malta Digital Innovation Authority (“MDIA”), a governmental agency tasked with the responsibility of promoting consistent principles for the development of visions, skills, and other qualities relating to technology innovation, and for the exercise of regulatory functions regarding innovative technology arrangements including distributed or decentralised ledger technologies (“DLT”), and related services. The MDIA has the role of granting formal recognition to innovative technology services providers or arrangements, such as smart contracts, by certifying them, giving users and service providers the necessary legal certainty regarding their use of certified DLT platforms, smart contracts and other technological arrangements.
2. The Virtual Financial Assets Act (the “VFA Act”) lays down the regulatory framework to regulate Initial Coin Offerings

(“ICOs”) or “Initial Virtual Financial Asset Offerings”, as they are referred to in the Act, and other Virtual Financial Assets (“VFAs”). In essence, the VFA Act represents the most significant of the three laws given the breadth of its scope, capturing cryptocurrencies, utility tokens and ICOs and all those operators providing services within the cryptocurrency ecosystem, such as advisors, brokers, exchanges, trading platforms and custodians.

3. The Innovative Technology Arrangements and Services Act (“ITAS Act”) provides the regulatory foundations for the development and regulation of innovative technology arrangements and innovative technology services. The ITAS Act provides that the MDIA will have regulatory responsibility for such arrangements and services. The technologies targeted by the ITAS Act are essentially DLT technologies, smart contracts, decentralised autonomous organisations and any other designated innovative technology arrangements which may be certified by the MDIA, thereby attributing higher levels of public trust.

As from 1st November 2018, all of these laws have been brought into effect, subject to specific grandfathering procedures enabling undertakings already established and operational on the effective date to comply with the new regulatory requirements.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

While no specific types of fintech businesses are prohibited in Malta, the MFSA takes a prudent and conservative approach towards reviewing any applicants looking for a Malta licence, particularly those in the online forex and binary options space. The MFSA is also very prudent in its approach towards “pay-day loan” type offerings.

Insofar as ICOs, and virtual currencies (“VCs”) are concerned, it is the specific features of each particular instrument that will determine whether or not it falls within the scope of existing legislation and would therefore be governed by existing EU legislation such as the Markets in Financial Instruments Directive (“MiFID” and “MiFID 2”), the Prospectus Directive, the Alternative Investment Fund Managers Directive (“AIFMD”), and/or the Financial Instruments Directive or possibly within the remit of Maltese national legislation, such as the Investment Services Act and the Financial Institutions Act. Those offerings falling outside the scope of existing EU and Maltese financial legislation such as, for example, tokens having features of membership or privilege cards and/or single- or multiple-use vouchers would not be prohibited by Maltese law, but could very well be caught and regulated by the VFA Act.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

Fintech businesses looking to set up in Malta would typically have equity backing originating from outside Malta, primarily in other EEA jurisdictions. Such financing usually takes the form of venture capital, loan capital or a combination of the two. Admittedly, debt financing is made available to more established business models having a track record and a significant collateral-to-debt ratio, since such models have a trading history to present to the banking institutions from which they seek to raise finance. In the case of start-ups, debt financing is a significantly more challenging route, precisely due to the absence of corporate collateral available.

Employee Share Option Programmes (“ESOPs”) are also commonly used by start-up companies seeking to engage and retain talent in the early years of their operations, whilst keeping their salary bill lower on the basis of key employees’ future equity participation. Such arrangements also enjoy a favourable 15% Malta tax rate in the hands of the employee benefitting from such a benefit, when properly structured.

To date, there have not yet been any fintech businesses that have sought to raise capital through an equity or a bond listing in Malta. However, we do expect that it is a matter of time until fintech businesses begin resorting to the Malta Stock Exchange for the listing of equity offerings.

ICO issues by Maltese companies, on the other hand, increased significantly over 2018, in keeping with international trends, although it is difficult to say how long this trend may continue. Regrettably, there is no centralised record in Malta from which any reliable statistical information may be obtained in this regard.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

Malta provides a very attractive corporate tax environment for businesses based in and operating from the island, and this has contributed significantly to the growth in the Maltese economy over the past years.

In addition to the corporate tax incentives, expat employees working in key positions with operators regulated by the MFSA may also avail themselves of a 15% personal tax rate on their employment income, provided that it exceeds an established threshold that is adjusted every year to reflect the cost of living index (€85,000 gross income for base year 2019). This Highly Qualified Person programme applies to EU and non-EU nationals alike, and was introduced by the Maltese Government in 2011 to sustain the burgeoning financial services industry with the best skill and talent available on the wider international market.

Due to the restricted size of the Maltese market, there are no venture capital financing houses based in Malta. Entrepreneurs seeking to base their businesses in Malta invariably source financing for their businesses from financial centres outside Malta.

Other incentives targeted at research, development and innovation could also be availed of by qualifying fintech undertakings. These incentive schemes are administered by the Malta Enterprise, which is the public corporation charged with attracting Foreign Direct Investment into Malta.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

The requirements for an IPO in Malta can be stated as follows:

- Minimum three-year track record.
- Appointment of a sponsoring broker.
- Issuing of a Prospectus complying with the EU Prospectus Directive.
- Shareholders’ funds and less intangible assets must be of at least €585,000.
- The company must have a fully paid-up capital of at least €235,000.
- Expected aggregate market value of the securities forming the subject of the application must not be less than €1,165,000 (not being Preference Shares).
- At least 25% of the listed class of shares shall be publicly held.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

No, there have not been any notable exits by the founders of fintech businesses in Malta over the past few years.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

The MFSA is the single regulator charged with the authority of regulating, monitoring and supervising the full spectrum of financial services in Malta. Fintech businesses are regulated by the general legal and regulatory provisions relating to credit institutions, financial institutions, investment services and insurance. All of these financial services activities have undergone tremendous changes over the past years, presenting new opportunities in the form of electronic distribution channels. As a firm we have witnessed the most significant transformation in payment-related services, partly as a result of the introduction of the PSD2.

Malta’s financial services legislation is organised under service- or activity-specific statutes which focus on the nature of the service being provided by the relevant undertaking. The Banking Act, the Financial Institutions Act, the Investment Services Act and the Insurance Business Act regulate the specific financial services activities falling within their respective regulatory scope. Therefore, fintech activities would be regulated in the same way as corresponding “non-fintech” business (i.e. brick-and-mortar operations).

However, in a recent launch of its “Vision 2021”, the MFSA announced that it will be launching a specialised fintech unit and also a “sandbox” environment, enabling operators that are fundamentally technology-driven businesses to operate within a framework of regulatory oversight without a fully-fledged licence, until the model is developed and the specific regulatory treatment is established by the regulator.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

Yes. As indicated above, in 2018 Malta introduced a comprehensive legal framework to regulate the issue and intermediation of

cryptocurrencies, and also a comprehensive test to enable operators and practitioners to classify this novel asset class correctly and objectively.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

The MFSA is very receptive to fintech innovation and technology-driven financial services operators, and takes a very pro-active approach towards new entrants, dedicating the resources to meet with the promoters of fintech businesses, even prior to commencing the application process, in order to understand their proposed model and provide valuable preliminary feedback.

This approach of open dialogue and hands-on regulation has made Malta a very popular base for fintech businesses, particularly in the PSP and EMI space.

The MFSA is currently undertaking a comprehensive analysis about the optimal approach to be taken towards sandbox environments as a test-ground for novel business models, which is expected to be rolled out in 2021.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

Fintech businesses licensed in another EEA state may freely target and access new customers in Malta as long as they have undertaken the necessary regulatory notifications to (i) provide cross-border services, or (ii) establish a branch in Malta. If a branch is physically established in Malta, there is a registration requirement for that branch and also tax registration requirements.

Where, on the other hand, the fintech business is based outside of the EEA, the applicable regulatory framework would effectively prohibit any solicitation of customers based in Malta.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

Yes – the Data Protection Act (Chapter 586 of the Laws of Malta) (“DPA”) implements the provisions of the EU’s General Data Protection Regulation (“GDPR”) and, together with the related subsidiary legislation, provides for the protection of individuals against the violation of their privacy by the processing of personal data.

The DPA and the GDPR are applicable to any fintech businesses processing personal data and operating in or from Malta.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

Yes – Maltese data protection law applies to:

- the processing of personal data in the context of the activities of an establishment of a controller or processor in Malta;
- data controllers or processors in a Maltese Embassy or High Commission outside Malta, regardless of whether the processing takes place in Malta;
- the processing of personal data of data subjects located in Malta by a controller or a processor not established in the European Union; and
- the processing of personal data by a controller not established in the European Union but in a place where the laws of Malta apply by virtue of public international law.

Further to the GDPR, the transfer of personal data to a non-EU/EEA country may only take place on the basis of an adequacy decision in favour of such country issued by the European Commission. In the absence of an adequacy decision, such transfer may take place if it is subject to one of the following appropriate safeguards:

- a legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules in accordance with Article 47 of the GDPR;
- standard data protection clauses adopted by the European Commission or by a supervisory authority and approved by the Commission; or
- an approved code of conduct.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

Penalties for non-compliance with the DPA will depend on the level of breach. The provisions of the law specify which level of sanction should apply for specific types of breach. The Information and Data Protection Commissioner may impose fines of two different categories, depending on the provision of the law which has been breached:

- up to €10 million, or 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher; or
- up to €20 million, or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

In the case of a public authority or body which has been found to be in breach of the DPA, the Information and Data Protection Commissioner may impose administrative fines of two different categories, depending on the provision of the law which has been breached:

- up to €25,000 for each violation and a daily fine penalty of €25 for each day during which such violation persists; or
- up to €50,000 for each violation and a daily fine penalty of €50 for each day during which such violation persists.

Any person who knowingly provides false information to the Commissioner or fails to comply with any lawful request pursuant to an investigation by the Commissioner is liable to a fine of between €1,250 and €50,000, or to imprisonment for six months or to both such fine and imprisonment.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

Yes. Maltese laws dealing with various aspects of cybersecurity include the following:

- the Maltese Criminal Code deals with cybercrime in a chapter entitled “Of Computer Misuse”;
- processing of Personal Data (Electronic Communications Sector) Regulations (Subsidiary Legislation 440.01); and
- the Electronic Communications Networks and Services (General) Regulations (Subsidiary Legislation 399.28).

Malta has also been a signatory to the Council of Europe Cybercrime Convention since 2001; such Convention was ratified in April 2012.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

Malta holds full EU Member status and is a signatory to the main international multilateral treaties which tackle money laundering in the world’s financial markets. Although Malta is not a member of FATF, it does play an active role in Moneyval, or the Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures.

Malta’s prevention of the money laundering regime is contained in two pieces of legislation, namely the Prevention of Money Laundering Act (“PMLA”) and the Prevention of Money Laundering and Funding of Terrorism Regulations (“PMLFTR”). The PMLA establishes the foundations for the legal framework by introducing basic legal definitions, laying down the procedures for the investigation and prosecution of money laundering offences, and establishing the Financial Intelligence Analysis Unit, whilst the regulations provide the substantive provisions relating to the offences, and clarify the systems and procedures to be adopted by subject persons in the course of their business activities.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

The Electronic Commerce Directive (Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market), which is transposed into Maltese law by virtue of the Electronic Commerce Act (Chapter 426 of the Laws of Malta), and the Electronic Commerce (General) Regulation are relevant for fintech businesses operating from Malta. These rules are relevant insofar as they define what constitutes an “Information Society Service” and provide a framework for such services to be conducted.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

Employment law draws heavily on Anglo-Saxon law and practice, providing an extremely balanced framework for employers. Whilst employees are provided with all the protection one would expect within the European Union, businesses are able to dismiss employees on the basis of just and sufficient cause or on the basis of redundancy without liability.

Social security contributions in Malta are reasonable and payroll formalities uncomplicated. Besides, the Highly Qualified Persons tax programme offers key expat fintech personnel with a competitive 15% personal income tax rate on their employment income. This programme has attracted significant and much-needed foreign talent to Malta within the fintech sector.

Unemployment in Malta is extremely low, requiring the labour market to be supplemented by EU and non-EU nationals that have moved to the island seeking various opportunities, including in the financial services industry, which is estimated to contribute an excess of 20% to Malta’s GDP. Finding experienced fintech professionals could prove to be difficult given the limited size of the labour market (Malta has a population of approximately 470,000). However, the Maltese labour force is educated, loyal and ambitious, with a university population of over 10,000 students. This provides fintech operators with the opportunity of training staff and providing them with on-the-job training.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Employees are not granted any significant mandatory benefits by Maltese law above those provided for within the framework of European law. Commercially agreed benefits are, however, becoming increasingly more commonplace.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

Any EEA citizens may freely establish themselves and work in Malta without any material formalities besides the usual tax and social security registration and a notification procedure intended for statistical purposes. Citizens of non-EEA countries (third-country nationals) are required to apply for a work permit on the basis of a formal job offer. The granting of such a work permit will depend largely on the skills of the individual concerned and the industry in which he/she is seeking to be employed.

With Malta’s shortfall of personnel having both skill and experience in the fintech sector, obtaining a work permit for a suitably qualified individual should not be difficult, although such permits can involve a waiting time of up to 90 days until approved. Efforts are being made by the authorities concerned to shorten this waiting period and make the work permit procedures more streamlined and efficient.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Any innovations and inventions that would qualify for protection can be protected locally depending on the nature of the particular innovation and invention. Indeed, the European intellectual property framework has been transposed into local law and provides ample protection for any patents, trademarks, industrial designs and copyright in the widest sense.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Maltese law provides for specific protection for all aspects of IP, and

this in the form of specific statutes regulating each individual area of IP. Accordingly, in the case of trademarks, patents and designs, protection may be sought pursuant to registration of the IP with the Maltese or European intellectual property office, whilst copyright would enjoy automatic protection in terms of the local Copyright Act without the need to pursue any formal registration in its regard. In addition to the foregoing, the Maltese Commercial Code also provides specific protection in respect of trademarks against unlawful competition.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

In addition to local/national rights, one would be able to enforce any European Union rights, registered with the competent supranational

authorities, as well as any rights that are considered to be famous and well-known in terms of Article 6bis of the Paris Convention.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

There are no restrictions on the exploitation or monetisation of IP rights, provided that such practices are in keeping with the general Maltese legal framework and Maltese mandatory public policy rules.

Acknowledgment

The authors would like to thank Dr. Yasmine Aquilina for her contribution related to data protection and privacy.



Dr. Andrew J. Zammit

GVZH Advocates
192, Old Bakery Street
Valletta
Malta

Tel: +356 2122 8888
Email: andrew.zammit@gvzh.com.mt
URL: www.gvzh.com.mt

Dr. Andrew J. Zammit is the Managing Partner of GVZH Advocates. With over 16 years' experience in the corporate and financial services field, he heads the firm's Corporate & Financial Services and TMT practices.

After reading law at the University of Malta at undergraduate level and obtaining a Doctor of Laws degree in 1999, Andrew furthered his studies at the London School of Economics and Political Sciences, where he was conferred with a Masters of Law degree in Company Law, Financial Services Law and International Trade Law. He was called to the bar in Malta in 2001 and has since been engaged in private legal practice in Malta.

Andrew is a member of the Chamber of Advocates, the International Bar Association, FinanceMalta and is also a Council Member of the Institute for Financial Services Practitioners ("IFSP") in Malta, the leading industry pressure group on the island. Andrew lectures Corporate and Business Law and regularly contributes academic articles to various publications and online information resources.



Dr. Kurt Hyzler

GVZH Advocates
192, Old Bakery Street
Valletta
Malta

Tel: +356 2122 8888
Email: kurt.hyzler@gvzh.com.mt
URL: www.gvzh.com.mt

Dr. Kurt Hyzler has accumulated extensive experience in investment funds, financial services regulation, banking and finance transactions throughout his career. Throughout his career he has successfully led several financial services licensing projects, including various types of collective investment scheme structures (UCITS, hedge funds and AIFs), investment services providers and financial institutions (Payment Services Providers and Electronic Money Institutions). He is also regularly engaged in complex corporate and financing transactions. Kurt regularly gives seminars and courses on the regulatory aspects of collective investment schemes licensed in Malta.

Kurt graduated with a Doctor of Laws from the University of Malta in 2006 after submitting a doctoral thesis entitled "The Principle of *Pari Passu* in Corporate Insolvency Law". Kurt was awarded the Chevening Scholarship in 2006 in order to further his studies at Queen Mary University London, where in 2007, he obtained a Masters of Law degree from the University of London in Banking and Finance Law after sitting four examinations in Company Law, International Finance Law, Financial Services Law and Corporate Insolvency Law.



GVZH Advocates is a modern and sophisticated legal practice composed of top-tier professionals, firmly rooted in decades of experience in the Maltese legal landscape. Built on the values of acumen, integrity and clarity, the firm is dedicated towards providing the highest levels of customer satisfaction, making sure that legal solutions are not only soundly rooted and rigorously tested, but also meticulously implemented.

At GVZH we understand that today's business environment requires legal advisors that have both skills and expertise geared towards effectively addressing specific and technical issues in the context of complex projects, transactions and disputes. It is through the contribution of these skills and expertise in an accurate and timely manner that GVZH Advocates looks to cement long-term and meaningful relationships with clients and partners.

GVZH Advocates is regularly involved in cross-border transactions, tapping into a wide network of international consultants, all experts in their respective field.

Mexico



Claudio Kurc



Arturo Portilla

Galicia Abogados, S.C.

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

According to Fintech Radar Mexico's website (<https://www.finnovista.com/actualizacion-finnovista-fintech-radar-mexico-agosto-2018/>), currently there are approximately 334 fintech startups incorporated in Mexico. The main fintech business models identified in Mexico are: (i) payments and remittances; (ii) lending; (iii) enterprise financial management; (iv) personal financial management; (v) crowdfunding; and (vi) enterprise technologies for financial institutions.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

Under the Mexican Fintech Act, Crowdfunding and E-Money Institutions' (jointly referred to as "Financial Technology Institutions" or "FTIs") activities may only be carried out by licensed entities. FTIs and Credit Institutions are only allowed to conduct transactions with crypto-currencies that have been expressly authorised by the Mexican Central Bank (the "MCB"). However, currently no crypto-currency (e.g. Bitcoin, XRP) has been authorised by the MCB as of today. No licence is required to operate with non-authorised crypto-currencies; however, such activity is deemed as vulnerable for anti-money laundering purposes.

On March 8, 2019 the MCB published the 4/2019 Regulations further regulating the crypto-currency-related activities that may be conducted by FTIs and Credit Institutions. Thereby, the MCB provided that such entities will only be entitled to use crypto-currencies for internal processes, and will have to implement specific mechanisms to avoid transferring the associated risks to final customers (crypto-currency exchange and wallet services were expressly forbidden for these entities). Also, the MCB established an ambiguous three-rule test in order to assess which will be the authorised crypto-currencies for these purposes. Authorisations will be granted on a case-by-case basis.

Broadly, some of the fintech business activities fall on one or more restricted activity categories (e.g. under banking, securities markets, mutual funds, insurance companies and other statutes regulating

activities of similar import). For instance, issuance of currency, solicitation of money deposits, public offering of securities, acting as a trading platform, rendering investment advice, fund formation, underwriting of insurance and other brokerage activities are restricted to specifically authorised entities.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

Mexico has relatively liquid capital markets. There are no restrictions or limitations to private funding through debt or equity. The securities markets statutes further provide safe harbour rules for private offerings that do not require listing. Private offerings include those limited to qualified or institutional investors, to less than 100 persons, or under employee incentive (or similar) plans. Public offerings entail listing requirements for which startups would generally not qualify. Venture capital and private equity are also available to new and growing businesses. Furthermore, under the Fintech Act, new and growing business may be funded through Debt or Equity Crowdfunding.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

Government-sponsored incentives may be obtained at both the federal and local (i.e., state or municipal) levels. The federal incentives are relatively scarce and are directed to specific programmes or industries, such as socially conscious endeavours, the film industry, energy projects and real estate developments. Federal tax credits are available for research and development investment in technology, and a federal grant is available for low-earning individuals investing in information and communication technologies. Local incentives vary widely from state to state. The export of certain communication technologies services has been incentivised through the enactment of a specific value added tax ("VAT") regime. Such activity now qualifies for the application of a 0% VAT rate provided certain requirements are fulfilled.

On January 8, 2019, a Presidential Decree was published through which fiscal incentives were granted on capital gains obtained by individuals resident in Mexico and any foreign tax residents,

provided such gains arise from share disposals made through an initial public offering in an authorised Mexican stock exchange and additional requirements are fulfilled.

The tax incentive gives the “Founding Shareholders” of a Mexican company, the option to apply a 10% income tax rate to the capital gains obtained during 2019–2021, to the extent they held the ownership of those shares before being registered in the National Securities Registry.

The following requirements should be met for the application of the incentive:

- (a) the value of the shareholders’ equity of the company corresponds to an amount of \$1 million Pesos (we understand this as a minimum reference value) and is subject to secondary provisions;
- (b) such shareholders, or a group of related persons, who directly or indirectly own at least 10% or more of the issuer’s shares or the control thereof (“Qualified Persons”), do not sell 10% or more of such equity or its control within a period of 24 months;
- (c) the share disposal must not be carried out outside the authorised stock exchange, through protected crossings or through registration operations; and
- (d) the disposal must not involve certain types of shares obtained from the exchange of shares of merged or unmerged companies.

This tax incentive might also be available to Qualified Persons, where at least 20% of the Mexican company’s shares are owned by a publicly traded venture capital trust (“FICAP”) or a similar investment vehicle, subject to the compliance of certain requirements, and the disposal is made within the context of a disinvestment process in order to initiate the public listing of the company. We are expecting that this incentive will be further regulated by means of secondary rules.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

Businesses that wish to carry out an IPO through the Mexican Stock Exchange have to meet several conditions. Pursuant to the Mexican Securities Market Law, only two types of companies in Mexico can carry out an IPO: (i) public stock companies (“SABs”); and (ii) transitional stock companies (“SAPIBs”). Requirements for SAPIBs are more lenient, given their non-permanent condition, but they must convert into SABs within a 10-year period and file a conversion programme with their IPO disclosure documents.

To carry out an IPO, the company must list its securities with the Securities National Registry, obtain authorisation from the Mexican securities regulator (“CNBV”) and obtain a favourable opinion from the exchange in which it plans to list. Applications must include audited financial statements and an offering prospectus.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

Although there have not been any fintech IPOs, according to Crunchbase, there have been several notable investment rounds on fintech businesses in the past few years: (i) Konfio, a lending platform, has raised approximately USD 102.3 million, which is currently the largest amount of funding in the Mexican fintech market; (ii) Clip, a payment processor platform, has raised approximately USD 42.3 million; (iii) Kueski, another lending platform, raised USD 38.8 million; and (iv) Kubo Financiero, a P2P lending platform, has raised approximately USD 11.3 million.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

The Mexican Fintech Act, issued on March 9, 2018, established a regulation for FTIs, which will require a licence in order to carry out their operations:

- (i) Crowdfunding Platforms for the following investment schemes: (a) debt; (b) equity; and (c) joint ownership and royalties.
- (ii) E-money Institutions, which may issue, distribute, manage, redeem and transact with e-money and/or crypto-currencies (separate authorisations may be obtained for remittances, foreign currency e-money and cash reception).

Fintech companies that do not fall under the activities described herein are not subject to the Mexican Fintech Act regulation.

Furthermore, the following novelties are also included under the Fintech Act:

- (i) Crypto-currencies (considered virtual assets under Mexican law): only licensed FTIs and Credit Institutions are able to conduct operations with crypto-currencies authorised by the MCB.
- (ii) A regulatory sandbox for both licensed and non-licensed companies.
- (iii) Open Banking: fintech institutions, clearing houses, traditional financial institutions and credit bureaus must develop application program interfaces (“APIs”) that allow connectivity and access to other APIs.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

As mentioned hereinabove, crypto-currencies are regulated under the Fintech Act and are defined as the electronically registered representation of value used among the public as means of payment for all kinds of legal acts, whose transfer can only be conducted through electronic means. Furthermore, as per the Fintech Act, crypto-currencies shall not be deemed as legal tender or currency. Additionally, FTIs and Credit Institutions may only carry out operations with crypto-currencies authorised by the MCB. Such authorisation will take into account the following: (i) the use given to the crypto-currencies as means of exchange, store of value and unit of account; (ii) the treatment given to such crypto-currencies in other jurisdictions; and (iii) the mechanisms or protocols that allow crypto-currencies to generate, identify, fractionate and control its replication.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

There are regulatory sandbox options for both licensed (traditional financial institutions and FTIs) and non-licensed companies in order to test their business model in a live, supervised and controlled environment: (i) non-licensed companies may request a temporary authorisation, for a maximum term of two years, in order to carry out operations which require a financial licence under Mexican regulation; and (ii) licensed companies will be able to request a temporary authorisation, for a maximum term of one year, in

connection with operations that are not permitted or excluded under the corresponding secondary regulation. All sandbox authorisations may be extended by an additional year.

Although the Fintech Act establishes certain requirements for the sandbox licence, the issuing of such authorisation is discretionary. Currently, no sandbox has been authorised by the financial regulators; therefore, it is unknown if financial regulators will be lenient in connection with sandbox authorisations.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

Under the Fintech Act, in order to carry out operations as an FTI, companies must first obtain a licence from the CNBV. Such licence requires, among others: (i) a company incorporated under Mexican law and with a domicile in Mexico; (ii) a minimum capital stock of approximately USD 163,265.00 to USD 228,571.00; and (iii) compliance with certain accounting and valuation mechanisms.

Furthermore, under the Fintech Act, Mexican financial regulators are authorised to block crowdfunding and e-money services offered in Mexico without a licence, in an effort to limit Mexican consumers' exposure to foreign and non-licensed fintech institutions.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

In Mexico, data protection and privacy are fundamental rights protected under the Constitution. Additionally, the data protection statutes regulate these matters at the federal level, by regulating the processing and transfer of personal data, and are applicable to anyone that collects personal data pertaining to individuals (other than credit bureaus, which are exempt from these statutes).

FTIs, as any other businesses, must provide a data subject (*i.e.*, the individual underlying the personal data) with a privacy notice, and process personal data in accordance with the principles of consent, information, data quality, due purpose, proportionality and responsibility. Data controllers must develop adequate safeguards and security measures to protect personal data against unlawful processing or transfers, give notice to data subjects whenever its privacy notice changes, and appoint an in-house data protection officer charged with overseeing compliance with the data protection statutes and ensuring data subjects' right to access, rectify, cancel or oppose the processing of data.

As regards Open Banking, the following type of data may be transmitted through APIs:

- (i) Open Financial Data: includes information regarding the financial products and services offered to the public.
- (ii) Aggregated Data: includes statistical information that does not allow identification of personal or transactional data of the client.
- (iii) Transactional Data: includes the financial and transactional information of the client and, therefore, requires the explicit consent of the data owner and may only be used for expressly authorised purposes.

At present, technical and security standards applicable to APIs have not been issued by the regulator.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

The Mexican data protection regulatory framework is applicable to organisations established outside of the Mexican jurisdiction in the following cases:

- (i) When the data controller is not established in Mexico but processes personal data through an establishment located in Mexican territory.
- (ii) The processing is carried out by a processor, regardless of its location, on behalf of a controller established in Mexico.
- (iii) Whenever an agreement or international treaty specifies that Mexican law will be applicable.
- (iv) When the data controller is not established in Mexico but processes personal data utilising means located on Mexican territory.

Regarding restrictions applicable to international transfers of data, the Mexican regulation provides that controllers shall inform data subjects, via the privacy notice, the personal data subject to transfer, the purpose of the transfer and the third party to whom the data will be disclosed. Said transfers require the data owner's consent. Such consent is not necessary when the transfer is established in a legal framework, is made to a related company or whenever such transfer is made by virtue of an agreement, in the interest of the data subject. The terms and conditions governing the transfers must be established in contractual clauses, stating that the data importer shall assume the same obligations on data protection as those imposed by law on the data exporter.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

Failure to comply with personal data protection brings about sanctions for the data collector. Such sanctions can be broadly classified as warnings, fines or imprisonment:

- Warnings can be issued by the data protection authority whenever the controller fails to comply with the data subjects' request to access, rectify, cancel or object to the processing of his personal information.
- Data collectors can be fined for failure to obtain the data owner's consent for the processing of data, and to comply with legal restrictions to transfer personal data, among other actions. Fines go up to USD 0.3 million and in case of repeated violations, the amount may be doubled.
- Imprisonment can range from three months to 10 years, depending on the way the information was used, intention and whether the information was sensitive or not.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

Under the Fintech Act, FTIs must develop continuity of business and cyber-security policies.

Cyber-attacks, hacking, virus infection and other cyber-crimes constitute punishable criminal offences. Furthermore, the National Security Program (2014–2018) includes among its objectives the creation of a regulatory framework applicable to cyber-security.

However, given the recent change of administration in the Mexican government, it is unknown if cyber-security will be an important part of the agenda of the new administration.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

The Anti-Money Laundering regulations (“AML”) apply to any person involved in lending activities or activities related to cryptocurrencies not authorised by the MCB.

Among the AML requirements that such lending and cryptocurrencies businesses have to comply with are the following:

- Know Your Customer (“KYC”) Policy.
- Identify the beneficiaries of transactions.
- Give notice of suspicious transactions.
- Have internal manuals.
- Register with the AML overseer.
- File monthly reports.

In addition, FTIs including regulatory sandbox participants are subject to specific AML provisions, such as the following:

- Have an AML Risk Focus Policy.
- Have an AML Policy, which must include KYC and internal AML procedures.
- Classify clients based on their transactional and risk profile.
- Implement mechanisms to identify suspicious activities.
- Submit Suspicious Activity Reports.
- Have a special AML committee and an AML compliance officer.
- Have an automatised AML system.
- Provide AML training to employees.
- Implement mechanisms in connection with blocked persons and politically exposed persons.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

There are a number of additional regulations applicable to fintech businesses in Mexico; for example, the General Law on Commercial Corporations and the Securities Market Law where applicable, determine the general regulatory framework and corporate structure applicable to legal entities established in Mexico. Furthermore, the Mexican Code of Commerce determines the framework applicable to commercial activities performed through electronic means, including the possibility of executing agreements or other documents through an electronic signature. Also, given that Sofomes and Sofipos are financial entities, they are regulated by the General Law on Auxiliary Credit Organizations and Related Activities and the Popular Credit and Savings Law, respectively.

Additional regulatory frameworks applicable to fintech businesses include the Financial Services Consumer Protection Law, which determines certain information that must be available to consumers, such as product information and fees. Such regulation also establishes the safeguards available to clients whenever the service provider fails to comply with the consumer protection obligations. Finally, for lending platforms, the General Law for Negotiable Instruments and Credit Operations establishes the regulatory framework applicable to credit agreements entered into by any private individual or corporation.

On September 6, 2018, a tax Bill was introduced to the Mexican Chamber of Representatives, proposing a new taxation regime for income derived from the provision of digital services, broadly those that consist of: a) the placing on a digital interface of advertising targeted at users of that interface; b) the transmission of data collected about users; and c) the provision of multi-sided digital interfaces to users very akin to the taxation rules, very similarly to the rules proposed by the European Commission in March 2018. As of today, the Bill’s discussion in the Chamber of Representatives is still pending.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

There is no *employment-at-will* in Mexico. As a general rule, employment relationships in Mexico are for an indefinite term. However, there are different hiring modalities available, subject to certain conditions. Existing hiring modalities are indefinite term, fixed term, specific project, initial training, seasonal work and probation period. Further, according to the Mexican Federal Labour Law (*Ley Federal del Trabajo*), employment contracts must be in writing and shall include, among other items, provisions regarding position and description of services to be rendered, place of work, salary, working schedule and days of rest, training and other working conditions, such as vacations, method of payment, etc.

Regarding an employee’s dismissal, the Law provides employers may terminate an employment relationship at any time so long as there are grounds for dismissal. The Mexican Federal Labour Law provides a limited list of misconducts considered as grounds for termination with cause. An employee terminated without legal cause may demand either the reinstatement of his/her job or severance pay.

Mexican labour and tax legislation have recently established burdensome rules regarding outsourcing schemes (applicable also in insourcing cases).

5.2 What, if any, mandatory employment benefits must be provided to staff?

Employee benefits mandated by the Labour Law are the following:

- Salary, which cannot be lower than the minimum wage in force at the time. Currently, minimum wage equals \$102.68 Pesos per day, except for the northern border free zone, in which minimum wage amounts \$176.72 Pesos per day.
- Working schedule, which shall not require more than 48 working hours per week and shall comprise at least one day of rest.
- Annual vacations that shall be equivalent to six days for the first year of employment and shall increase annually in proportion to the seniority of the employee.
- Vacation premium of at least 25% over the salary corresponding to the vacation period.
- Christmas bonus equivalent to 15 days of salary to be paid no later than December 20 of each year, in proportion to the time worked during the year.
- Payment of profit sharing equivalent to 10% of the employer’s pre-tax annual profits, allocated among employees.

- Enrolment with the Mexican Social Security Institute (“IMSS”), the National Housing Fund for Workers (“INFONAVIT”) and the National Pension Fund System (“SAR”), with the subsequent payment of social security dues and contributions.

The Labour Law also regulates the payments that must be made for employees’ overtime and work performed during days of rest.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

The hiring of foreign employees requires special permits from the immigration authorities to legally live and work in Mexico. No special route for obtaining permission for individuals who wish to work for fintech businesses are available. The Mexican Federal Labour Law establishes, as general rule, that employers in Mexico shall employ at least 90% Mexican nationals.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

In Mexico, most inventions are protected through the patent system, while other kinds of innovation or non-patentable inventions are protected either under trade secrecy, as copyrights (this is in the case of computer programs, databases or software), or by obtaining registration of utility models, industrial designs, trademarks and commercial ads or slogans.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Patents are protected for a non-extendable term of 20 years; industrial designs have a protection of 15 years, and utility models have a protection of 10 years. The right to obtain a patent, industrial design or utility model registration corresponds to the inventor or designer, as applicable.

Original computer programs are subject to registration as copyrights. An author’s (in this case, the developer’s) patrimonial rights over a computer program shall be protected for a term consisting of the life of the author plus 100 years after his death. Moral rights protection does not lapse and can be transmitted by death.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

Although registration is not a requirement for copyright protection or enforcement in Mexico, registration is crucial for the enforcement of any industrial property right. Additionally, most industrial property rights (save for trade secrets) are country-based rights, where Mexican authorities govern their grant, scope, enforcement and validity within Mexico.

Original works of authorship shall be protected, even absent registration or publication. Nevertheless, registration grants legal certainty and publicity to the work. Therefore, although registration in Mexico is not mandatory for enforcement of the relevant copyrighted work (and does not grant any specific procedural right), it is advisable to register any work of art or computer program susceptible to protection.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

In addition to direct exploitation, IP rights are often monetised through either technology transferral, licensing or the constitution of liens. Both, applicants and holders of IP rights may assign and transfer their IP rights, in whole or in part. All rights arising from an application, a patent or a registration may be transferred or be the subject matter of liens.

Licensing is arguably the most common manner of exploiting IP rights. Licences must be recorded.

The registered owner of a computer program may assign or license the program. The assignment of computer programs is not subject to any time limitations generally found in other copyrights.

Acknowledgments

This paper was drafted as a multidisciplinary effort in which the following lawyers also contributed: (i) Irma Ross Navarro (*Intellectual Property*); and (ii) Nadia González Elizondo (*Labour Law*).

**Claudio Kurc**

Galicia Abogados, S.C.
Blvd. Manuel Ávila Camacho #24
7° Piso, Col. Lomas de Chapultepec, 11000
Mexico City
Mexico

Tel: +52 55 5540 9243
Email: ckurc@galicia.com.mx
URL: www.galicia.com.mx

Claudio Kurc's professional practice focuses on banking and finance. He also has experience in anti-money laundering, fintech regulation, data privacy, contracts and corporate matters in general.

Prior to joining Galicia Abogados, he worked at the Banking, Securities and Savings Unit of the Ministry of Finance. He studied law at *Instituto Tecnológico Autónomo de México*.

**Arturo Portilla**

Galicia Abogados, S.C.
Blvd. Manuel Ávila Camacho #24
7° Piso, Col. Lomas de Chapultepec, 11000
Mexico City
Mexico

Tel: +52 55 5249 2019
Email: aportilla@galicia.com.mx
URL: www.galicia.com.mx

Arturo Portilla's professional practice focuses on national and international tax consulting. He also has experience in fintech regulation.

Prior to joining Galicia Abogados, he focused on tax litigation in two different consulting firms of national reach. He studied law at *Universidad Iberoamericana* and has taken post-graduate courses on taxation.

GALICIA

ABOGADOS

Galicia Abogados, S.C. is a leading law firm in Mexico with more than 23 years of experience helping its clients take better business decisions by providing specialised knowledge, and its ability to understand the clients' business needs and strategies. Galicia Abogados is a leader in five strategic sectors through a multidisciplinary approach from our specialised practices: Finance; Energy & Infrastructure; Private Equity; Real Estate; and Regulated Industries. The firm's unique way of thinking provides solid and constructive solutions to the challenges faced by its clients in light of ever more complex and demanding operations. Galicia Abogados strikes a balanced approach covering and protecting the needs and positions of its clients, while making sure the transaction reaches successful closing.

Galicia Abogados has a close relationship with the most important law firms in North and Latin America, Europe and Asia. Most of its attorneys hold graduate degrees and have worked in leading firms in the United States and Europe.

Morocco

Nihma Elgachbour



Ayoub Berdai



Hajji & Associés

1 The Fintech Landscape

- 1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).**

The fintech sector in Morocco is booming. The willingness of new industry players combined with mindful management by regulators allow the Moroccan fintech sector to offer to its customers a wide range of services, particularly in the fields of payment, insurance, scoring and, soon, crowdfunding.

Moroccan historical finance establishments are striving to switch their services and products to align them with the development of new technologies, while new fintech operators, especially start-ups and telecom operators, are competing with traditional finance players.

No official statistics on the number of fintech companies have been presented to date. However, it is estimated that since 2017 – the year in which NAPS, the first Moroccan fintech start-up providing secured payment services, was launched – the number of fintech operators has grown to exceed 20 entities, four of which were licensed by Moroccan central bank (“BAM”) in 2018.

In addition to these operators, 20 bank and insurance institutions are moving towards the adoption of fintech strategies, notably through mobile banking as well as electronic banking and insurance platforms.

Finally, it should be pointed out that at the beginning of 2018, Morocco was moving towards cryptocurrency, and mainly bitcoin, in so far as the country was ranked 36th in the world and 3rd in the MENA region as having one of the highest numbers of cryptocurrency transactions, despite the current but temporary ban by regulators (please see question 3.2).

- 1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?**

The concept of fintech is new to the Moroccan legal sphere. Thus, there is to date no specific regulation prohibiting a particular type of fintech business. However, the creation and operation of a fintech business should be analysed on a case-by-case basis, considering the existing legislation and regulation applicable to banking, finance and insurance.

However, the situation is quite different concerning cryptocurrency (please see questions 3.1 and 3.2).

2 Funding For Fintech

- 2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?**

For both new and growing businesses, investing in Morocco is based on the juxtaposition of equity financing, private equity, traditional bank financing and many other types of funding.

Generally, new corporations resort to 60 per cent self-financing, and the remaining 40 per cent is provided by banks and ultimately by possible State subventions; therefore, private equity financing is still underdeveloped and fails to foster the emergence of innovative start-ups.

Besides this, several Moroccan State and private programmes aiming at promoting fintech are ongoing. The main incentive programmes are developed by the Casablanca Finance City (“CFC”) and the Banque Centrale Populaire (“BCP”).

- 2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?**

There are not yet any specific incentives for investment in tech/fintech businesses, but they are available for encouraging the creation of and investment in small and medium-sized corporations.

More particularly, with respect to tax and customs incentives, the Moroccan tax law referred to as the “*Code Général des Impôt*”, which is amended each year by the financial law, provides for several exemptions such as VAT and corporate tax on new businesses during their first five years.

In addition, the Moroccan investment charter of October 3, 1995 is due to be replaced with a new version in 2019, which should come with important changes targeting the development of regions and possibly the enhancement of new business models, including new technologies and fintech.

It should be noted that Moroccan private equity laws, in particular Law No. 41-05 of February 14, 2006 relating to Venture Capital Organizations (“*Organismes de Placement en Capital Risque*”) as amended and supplemented, provide several tax incentives for investors and their target companies.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

An IPO in Morocco requires an issuing entity to be a joint-stock company “*société anonyme*” or a so-called limited partnership with a share capital “*société en commandite par actions*”. The implementation of an IPO is subject to conditions provided by the stock exchange law, “*Loi relative à la Bourse des Valeurs*” of September 21, 1993 as amended and supplemented, which provides for the eligibility of a corporation to enter into an IPO. Such an operation can be undertaken with one of the three listing markets – the principal market, the development market or the growing market:

- the principal market is reserved for large entities, with a minimum share equity of 50 million Moroccan Dirhams (“MAD”), which have been active for at least three financial years. In order to be admitted into such a main market, the aforesaid entities must issue a number of shares exceeding 250,000 with a minimum value of MAD 75 million;
- the development market is reserved for medium-sized entities, with a minimum turnover of MAD 50 million, which have been active for at least two financial years. In order to be admitted into such development market, the aforesaid entities must issue more than 100,000 shares with a minimum value of MAD 25 million;
- the growing market is reserved for fast-growing entities which have closed at least one financial year. In order to be admitted into such growing market, such entities must issue more than 30,000 shares with a minimum value of MAD 10 million; and
- the bond market is reserved for entities which have been active for at least two financial years; these entities may issue bonds with a value of more than with MAD 20 million and for a maturity exceeding two years.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

To the best of our knowledge, there have been no notable exits by the founders of fintech businesses in Morocco.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

There is not yet any specific regulatory framework to regulate fintech businesses operating in Morocco. However, the general common law regulatory framework is *de jure* applicable, and any fintech business, as with any other corporation, must comply with the applicable Moroccan law.

As such, any fintech business must comply with Moroccan corporate laws, and, if a business is carrying out financing and banking activities, preliminary authorisations should be obtained from mainly BAM and the Moroccan market finance authority (“AMMC”).

The following activities are regarded as regulated activities, and any entity which carries these out requires a licence from BAM: (i) receiving deposits from the public; (ii) providing loans; (iii) issuing payment cards; (iv) providing investment services; (v) delivering

foreign-exchange operations; (vi) financing leasing transactions; (vii) guaranteeing transactions and undertaking securities operations; (viii) developing factoring operations; (ix) entering into gold, precious metals and coins operations; (x) providing insurance brokerage; (xi) providing payment services such as funds transfers, performance of payment transactions as an intermediary between payers and suppliers, supplying card payment transactions etc.; and (xii) other activities that are connected or similar to the aforementioned services.

In each service or group of services above, the applicant entity is granted a single licence by BAM. This licence lists each regulated activity that the entity is permitted to undertake.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

There is not yet any Moroccan regulation specifically directed at cryptocurrencies or cryptoassets.

However, and with reference to a number of media channels, the Moroccan exchange authority (“*Office des Changes*”) informed the public on November 21, 2017 that any transaction carried out via cryptocurrency is considered a breach of the Moroccan exchange laws and would trigger sanctions and penalties. Indeed, any funds transfer to or from Morocco should be carried out through licensed intermediaries such as banks, and only in lawful foreign currencies which are listed by BAM.

A second conjoint media announcement, dated November 21, 2017 and published by BAM and the AMMC together with the Moroccan ministry in charge of finance, warned the public that any use of cryptocurrencies as a method of payment would be a clear breach of the applicable laws, since no protection is offered to customers. The two announcements have not made a distinction between the different types of cryptocurrencies.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

Financial regulators and policy makers in Morocco are receptive to fintech innovation and technology-driven new entrants. In particular, the bank’s Law No. 103-12 of December 24, 2014 (“*Loi relative aux Etablissements de Crédits et Organismes Assimilés*”) provided for alternative access payment services to persons duly licensed, other than banks. The payment services banks monopoly then ended, which was a strong signal for the liberalisation of finance activities, giving possibilities to, among others, fintech corporations. However, there is no regulatory “sandbox” option for fintechs in Morocco.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

As far as there is no specific regulatory framework for fintech businesses, fintech businesses which are established outside Morocco cannot freely and without licence enter the Moroccan financial market.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

The collection, use and transmission of personal data is governed in Morocco by Law no. 09-08 of February 18, 2009 relating to the protection of natural persons with respect to processed personal data (“Law no. 09-08”). This law provides for personal data processors’ obligations and rights with respect to the persons whose personal data is processed. The obligations of any personal data processors are (i) to not process any personal data without the consent of the concerned person, (ii) to declare the process of personal data to the Moroccan competent authority, the “*Commission nationale de contrôle de la protection des données à caractère personnel*” (“CNDP”), and (iii) to apply for the CNDP’s authorisation in order to transfer the processed personal data outside of Morocco, or in order to process personal data considered as sensitive data. The rights of persons whose personal data is processed are the rights to information, to access, to modification and to objection.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

Law no. 09-08 is indeed applicable when the personal data processor is not located in Morocco. The personal data processor is the person who defines the means and purposes of personal data processing.

Therefore, if the means used in order to collect, store and transfer personal data are located in Morocco, the personal data processor located in a foreign country should appoint and communicate the identity of its representative in Morocco to the CNDP, declare to the CNDP its processing of personal data, and apply for an authorisation from the CNDP for the transfer of personal data outside of Morocco.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

The sanctions that apply for failing to comply with data privacy laws are: (i) imprisonment from three months to one year and fines from MAD 20,000 to MAD 200,000 for making/receiving a personal data processing declaration/authorisation and using personal data for other purposes than that agreed or declared; (ii) imprisonment from three months to one year and fines from MAD 20,000 to MAD 200,000 for processing the personal data of a non-consenting person; and (iii) imprisonment from six months to two years and fines from MAD 50,000 to MAD 300,000 for processing sensitive data.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

Law no. 07-03 of November 11, 2003 relating to automatic data processing system crimes (“Law no. 07-03”) may be applied when any fintech businesses operating in Morocco faces a breach of their security systems. Therefore, Law no. 07-03 sanctions any fraudulent

access to automatic data processing systems by imprisonment from one to three months and fines from MAD 2,000 to MAD 10,000. When such fraudulent access result in the removing or modifying of processed data, the sanctions are doubled. In addition, any impeding of the functioning of automatic data processing systems is sanctioned by imprisonment from one to three years and fines from MAD 10,000 to MAD 20,000.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

Law no. 43-05 of April 17, 2007 relating to anti-money laundering lists the acts which are considered as AML crimes along with the related sanctions. Such a list is not an exhaustive one and it includes, among others, the acquisition/transfer of assets in order to hide the origin of such assets when they are the result of the following offences: narcotic trafficking; human trafficking; immigrant trafficking; weapon trafficking; terrorism acts; corruption; fraud on monies; bill of exchanges; promissory notes; and any other means of payment.

Fintech businesses are necessarily subject to AML legislation. Firstly, fintech businesses must not be used as a means to launder money. Secondly, and as licensed entities, fintech businesses must comply with legal obligations which consist of controlling any transaction they carry out on behalf of their clients. They should disclose any doubtful transactions to the competent authorities.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

There are no other regulatory regimes which are applicable to fintech business operating in Morocco except civil law principles, and, among others, the commercial, competition, consumer and corporate laws.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

The hiring and dismissal of staff in Morocco are regulated by the Moroccan labour law of 2004. There are two main types of employment contracts. The first is the fixed-term contract (“*Contrat à Durée Déterminée*”) concluded for a period of one year, renewable once. Where the fixed-term contract is extended further, it automatically becomes a permanent contract. The second is the permanent contract (“*Contrat à Durée Indéterminée*”), concluded for a non-fixed term.

Otherwise, an employment contract may be terminated by the resignation of the employee, their dismissal for gross misconduct or for technological, structural or economic reasons.

The hiring of foreign persons is subject to a restrictive regulation by which such foreign person should conclude a foreign employment contract with their local employer, and may be subject to a selective authorisation for working in Morocco should his activity in Morocco be possibly undertaken by a Moroccan resident with equivalent professional skills (please see question 5.3).

5.2 What, if any, mandatory employment benefits must be provided to staff?

Under Moroccan law, social security and mandatory illness insurance (“AMO”) are the obligatory benefits that every employer must provide to its employees.

Social security covers the risks of sickness, maternity, invalidity, old age and death, and it also serves family allowances. Social security is financed by contributions from both employers and employees.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

In Morocco, the recruitment of a foreign national is subject to the grant of an employment contract authorisation (visa). The employment contract must be drafted in accordance with the standard form contract for foreign employees in Morocco. The application for the visa is made through the online service “TAECHIR” (www.taechir.travail.gov.ma), which sets out the supporting documents to be included in the application package.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Industrial property is governed by Law no. 17-97 of February 15, 2000 on industrial property, as amended and supplemented. This law covers all aspects of the protection of inventions, including patents, designs and trademarks.

Also, Law no. 2-00 of February 15, 2000 on copyrights and neighbouring rights, as amended and supplemented, deals with the other aspects of intellectual property, which relate to copyright. It should be noted that software/computer programs are protected in Morocco not by patent, but by copyright.

Applications for the protection of patents, trademarks and industrial designs are filed with the Moroccan Office of Industrial and Commercial Property (“OMPIC”).

In order to be patentable, the invention must be new, inventive and have an industrial destination. The patent title protects the invention for a period of 20 years in Morocco.

Trademarks and service marks are protected where they are lawful, distinctive and available. The registration of a trademark confers protection of a period of 10 years, which is indefinitely renewable.

The design must be new and differentiated. It gives the design’s right holder five years of protection, which is renewable four times.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

The ownership of IP deriving from industrial property such as patents, designs and models and trademarks results from the registration of such rights with OMPIC. The owner of IP rights may be the inventor, its successors, the employer where the invention has resulted from technical, human and financial means made available to the inventor, employee or the third person who acquired the invention.

Also, the ownership of IP deriving from a literary and artistic work belongs to its author since its creation does not require registration. However, it is recommended to file a declaration of the literary and artistic work with the Moroccan Copyright Office in order to obtain a sound protection. The protection is granted to the author throughout his life and a further 70 years after his death. As for moral rights, they are unlimited in time and are imprescriptible and inalienable. However, the economic rights would be the property of the employer where the literary and artistic work has been created according to an employment contract.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

The registration with OMPIC of an industrial property right in Morocco confers protection only in Morocco. Thus, protection outside of Morocco is granted through: (i) filing for the right on an international scale, which could be carried out by filing with each national office of the targeted countries for protection; (ii) filing with the regional office for countries adhering to a regional IP protection system; or (iii) a filing with the World Intellectual Property Organization (“WIPO”) to benefit from registration in all countries adhering to the various intellectual property protection treaties.

Ultimately, the protection of intellectual property rights is granted by their registration at the national level with OMPIC and at the international level with the WIPO.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

The exploitation of an intellectual property right is carried out directly by its owner, who enjoys an exclusive right of exploitation throughout the duration of the protection.

However, the linked rights to an industrial property title may be transferred in whole or in part. They may be subject, in whole or in part, to an exclusive or non-exclusive licence or to a pledge.

It should be noted that under Moroccan law, some legal restrictions on exploitation and licensing exist, such as the obligatory granted licences for the purposes of national defence.

**Nihma Elgachbour**

Hajji & Associés
28 Bld. Moulay Youssef
20070 Casablanca
Morocco

Tel: +212 522 487 474
Email: n.elgachbour@ahlo.ma
URL: www.ahlo.ma

Nihma Elgachbour is a lawyer, holds a Master's degree, and is a PhD student in Business Law. She joined Hajji & Associés in 2017 and intervened in major projects in Morocco, including those related to renewable energy, oil & gas exploration and exploitation, the international financing of corporations, aviation, and local and international mergers and acquisitions.

**Ayoub Berdai**

Hajji & Associés
28 Bld. Moulay Youssef
20070 Casablanca
Morocco

Tel: +212 522 487 474
Email: a.berdai@ahlo.ma
URL: www.ahlo.ma

Ayoub Berdai is a lawyer and holds a Master's degree in Business Law. He joined Hajji & Associés in 2018.

HAJJI & ASSOCIÉS

AVOCATS

Hajji & Associés is an independent Moroccan law firm which has developed, since the mid-1990s, high-level expertise in the international business law field.

The activities of the firm cover particular areas of international finance, the restructuring of companies, mergers and acquisitions, energy and infrastructure, market entry plans, IT law, commercial litigation and international arbitration.

The firm maintains privileged professional relationships with large international law firms, which generally support their clients' investment projects in Morocco with the assistance of Hajji & Associés.

Netherlands

Björn Schep



Willem Röell



De Brauw Blackstone Westbroek

1 The Fintech Landscape

- 1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).**

There are several thriving fintech hubs in the Netherlands, such as Amsterdam (centre of the Dutch financial sector), Delft and Eindhoven (technical universities). For some time now, we have seen a lot of activity in the fields of advanced analytics, blockchain, mobile, biometrics, robotics, artificial intelligence and machine learning. Fintech has thus gained a steady foothold in the Netherlands, and all sorts of fintech businesses have emerged in the Dutch market. As such, the Netherlands is home to “traditional” fintech businesses (payments, asset management, credit provision, etc.) – of which payments unicorn Adyen is a prime example – as well as more specialised forms of financial innovators, operating under buzzing common denominators, such as InsurTech, BigTech, PensionTech, LegalTech and RegTech. Since “Brexit”, many UK-based fintechs have chosen Amsterdam as their new HQ or are considering doing so.

Besides new initiatives from start-ups and scale-ups, established financial companies in the banking and insurance sectors are also very active with regard to innovation. Banks and insurers in the Netherlands have set up internal innovation platforms and launched spin-offs. Furthermore, pension funds and asset managers are becoming more interested in how innovation may impact and improve their business models.

In general, we see the fintech environment becoming more mature and more professional. As new business models prove themselves, more capital, time and effort flow into fintechs. Dutch regulators and decision makers have always been receptive to fintech businesses, and try to facilitate fintechs as much as possible. As the fintech environment matures, regulations should be expected to play a bigger role in the foreseeable future, legitimising these developments even further and potentially strengthening the fintech ecosystem.

- 1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?**

There are no specific rules or regulations that prohibit or restrict fintech businesses in the Netherlands. However, as in most jurisdictions, the financial services sector is heavily regulated. Therefore, certain types

of fintech businesses need to comply with “regular” financial regulatory policies, rules and regulations. This is the case for fintech businesses that provide a regulated financial service, such as offering consumer credit, payment services or insurance services. This remains true if the business is more “tech” than “fin”.

Both the Dutch Central Bank (DNB) and the Netherlands Authority for the Financial Markets (AFM) realise that existing rules sometimes do not fit well with new fintech solutions, and they have a positive and constructive attitude towards innovation in the financial services sector (see question 3.3 on special fintech treatments).

In the past, AFM and DNB have, however, issued warnings against cryptocurrencies and ICO tokens because of the absence of supervision, deposit guarantee schemes and lack of recourse. The AFM has used enforcement measures against companies offering securities based on cryptocurrencies without a licence. More recently, the regulators have recognised the public interest in cryptocurrencies and ICOs and acknowledged their potential for SME financing.

2 Funding For Fintech

- 2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?**

The Netherlands has a solid banking industry and has an increasingly popular listing venue, Euronext Amsterdam, which is accessible to fintech businesses above a certain size.

While small and growing fintech businesses are less likely to have access to traditional bank financing or to the capital markets through an IPO or bond issuance, venture/seed capital firms are active in the Dutch market to provide early-stage financing. In addition, some fintech businesses choose to partner with incumbent financial institutions to finance their operational and development costs. Crowdfunding is less common in the Netherlands, but may grow in popularity as an additional source of finance.

- 2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?**

From a tax perspective, the Netherlands is an attractive hub for investing in or expanding fintech businesses in Europe. This is in

part due to the extensive treaty network of the Netherlands, which provides, in many cases, for reduced or no withholding taxes on incoming dividends, interests and royalties. Moreover, with respect to outbound payments, the Netherlands currently has no withholding tax on interests and royalties – while the dividend withholding tax is, in most cases, restricted by domestic law, tax treaties and EU law. In addition, the Netherlands has a broad participation exemption with respect to incoming dividends and capital gains derived from qualifying equity investments.

The following specific tax incentives may also be available to fintech businesses in the Netherlands:

Innovation box

The innovation box regime provides for profits derived from certain qualifying self-developed intangibles (for example, software) being taxed at an effective rate of 7% if certain conditions are met.

R&D wage tax credit

The WBSO (R&D tax credit) of the Ministry of Economic Affairs is intended to provide entrepreneurs with an incentive to invest in research. If certain conditions are met, the R&D tax credit effectively provides for a reduction of wage tax and national insurance contributions due by employers in connection with R&D activities in the Netherlands.

30% ruling

Qualifying expats in the Netherlands are entitled to a substantial income tax exemption of up to 30% for a maximum period of five years, resulting in only the remaining 70% being subject to income tax.

Plans of the current government

In order to further improve the attractiveness of the Netherlands, the government has decided to reduce the maximum statutory corporate income tax rate from 25% in 2019 to 20.5% in 2021.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

Prior to listing securities on a Dutch regulated market, Dutch regulatory law requires the business to prepare a prospectus. The content of a prospectus document is governed by European rules. The prospectus has to be approved by the AFM. For businesses incorporated under the law of a different EU/EEA Member State, the approval granting authority is, in principle, the home state regulator. These businesses may “passport” their approved prospectuses into the Netherlands. Subject to certain equivalency standards, the AFM will allow businesses incorporated under the law of a non-EU/EEA Member State to use a non-EU prospectus, in order to acquire a listing on the Dutch regulated market.

Furthermore, a business will need to comply with relevant corporate law. For example, the business will need to have a corporate structure in place that allows shares to be freely transferable and tradeable.

A business will also need to comply with the regulations of the local regulated market. However, unlike some regulated markets, Euronext Amsterdam does not have substantive ongoing requirements. For Dutch businesses, the “comply or explain” governance recommendations, pursuant to the Dutch Corporate Governance Code, apply.

Finally, a business will need to comply with ongoing requirements, such as the EU market abuse and transparency rules (disclosure of inside information, notification requirements for shareholders, disclosure of trades by certain key insiders).

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

The Netherlands has become one of the main global fintech hubs, with a significant increase of fintechs opening shop here since Brexit. Although the IPO of Adyen in 2018 was the biggest on Euronext Amsterdam in years, the trend in the Dutch fintech sector is to collaborate with venture capital firms or to partner up with incumbents, rather than to sell a fintech business in its entirety. For instance, in January 2018, ING (advised by De Brauw Blackstone Westbroek) acquired a 75% stake in payments service provider Payvision, valuing the company at EUR 360 million.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

There is no specific regulatory framework applicable to fintech businesses in the Netherlands. Whether a fintech business falls within the scope of a specific financial regulatory framework depends on the specific services it intends to provide. Often, fintech activities pertain to regulated activities for which, in principle, a licence from DNB or the AFM is required. As a result, a fintech business providing such an activity will, in principle, be subject to the same regulatory framework as traditional financial entities (but a special “fintech treatment” is possible; see question 3.3).

Regulated activities include, among other activities, offering consumer credit, acting as an intermediary in financial products (for example, insurance and consumer credit), acting as a bank, offering insurance and providing payment services.

The Netherlands adheres to a functional financial supervisory model (twin-peaks model). In this model, DNB is charged with the supervision of prudential rules (for example, capital adequacy), whereas the AFM oversees compliance with market conduct rules (for example, KYC). Additional supervision may come from the Dutch Data Protection Authority (AP) and the Dutch Competition Authority (ACM).

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

Currently, no regulation specifically directed at cryptocurrencies or cryptoassets is in place. This will change as the Revised Fourth Anti-Money Laundering Directive (commonly referred to as the 5th AMLD) entered into force on 9 July 2018, and must be implemented by all EU Member States by 10 January 2020. In the Netherlands, the proposed implementation act extends the scope of Dutch AML legislation to include certain virtual currency service providers, and introduces an obligation for these providers to obtain a licence from DNB. To obtain such a licence, a provider must demonstrate the ability to comply with specific AML legislation, and that its day-to-day policymakers are fit for their position and their integrity is beyond doubt.

The licence obligation applies to any business providing exchange services between virtual currencies and fiat currencies or custodian wallet services within or from the Netherlands. This means that virtual currency service providers located in other countries will also be subject to the licence obligation if they provide their services

on a cross-border basis to clients located in the Netherlands. The proposed implementation act includes an exemption for providers that have obtained a similar authorisation in another EU Member State. The proposed implementation act is not yet final and may be altered significantly.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

The financial regulators and policy makers in the Netherlands are very receptive to fintech businesses, and try to support fintech businesses as much as possible. The Netherlands is one of the few EU Member States to have both an innovation hub and a regulatory sandbox, and the attitude towards fintech is becoming more and more elaborate and mature.

Regulators

Innovation hub

To support businesses that seek to implement innovative financial business models or products, but are unsure about the specific relevant rules, DNB and the AFM set up the InnovationHub in 2016, later joined by the ACM. The InnovationHub offers new businesses and incumbents the opportunity to submit questions about supervision and regulations directly to DNB, the AFM or the ACM, regardless of whether they are currently subject to a regulatory framework.

Regulatory sandbox

Following the successful introduction of the InnovationHub, DNB and the AFM created a regulatory sandbox to further facilitate innovation and to enable businesses to launch their innovative financial products without unnecessary regulatory hindrance. In the context of the regulatory sandbox, the relevant regulator will assess whether the applicants and their innovative concepts comply with the underlying purposes of applicable financial markets regulations rather than with the strict letter of the law. This will enable and encourage the regulators and any business wishing to launch an innovative financial concept to enter into a constructive dialogue. The regulatory sandbox is open for start-ups and established financial companies active in the Netherlands.

Partial authorisation

In 2017, in addition to the InnovationHub and the regulatory sandbox, partial authorisation was introduced, providing companies with the possibility to obtain authorisations with requirements or restrictions, or an opt-in authorisation. Partial authorisation may be issued when a financial institution does not wish to engage in all operations governed by a full authorisation or is not yet able to meet all eligibility requirements for such an authorisation. It may be granted on a temporary basis, but may also have a more permanent nature. As such, partial authorisation may be used by businesses to develop a fully-fledged financial institution step-by-step.

In December 2018, the AFM and DNB published a joint report with recommendations to (i) introduce a licence for certain crypto service providers (see question 3.2), and (ii) amend European legislation to facilitate security tokens as funding options for small businesses.

In January 2019, the AFM published its agenda with key activities for 2019, one of which is the prevention of irresponsible use of technology and data. The AFM performs studies on robo-advice on financial products, cryptocurrencies and ICOs, and the use of data in the insurance sector.

Policy-makers

The Minister of Finance sent his agenda for the financial sector for the coming years to Parliament on 17 December 2018. This agenda is based on three focus areas, one of which is innovation (including fintech). The minister, among other things, intends to:

- increase diversity in the financial sector by conducting research on the risks and opportunities of fintech, and by introducing measures to stimulate the entrance of new innovative (fintech) parties;
- promote proportionality in regulation and supervision, and to put this on the European agenda; and
- research efficiency benefits of blockchain technology in payments and securities transactions.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

Offering financial services or financial products to consumers in the Netherlands can trigger Dutch financial regulatory law, which, in principle, requires prior authorisation by the relevant Dutch regulator (either through a national application for a licence or notification of the relevant regulator, or through “passporting” an EU Member State authorisation). There are various exemptions and exceptions to this main rule, depending on the specific circumstances. The InnovationHub and regulatory sandbox are also available for fintech businesses outside the Netherlands who want to become active here.

Regulators, however, do allow reverse solicitation. In this context, the regulators apply the “initiative test” to determine whether financial services and products are offered “in the Netherlands”. According to this test, financial services and products of a business with its statutory seat outside of the Netherlands are considered not to be offered in the Netherlands when the services or products are provided solely on the initiative of the client. Subsequently, there would be no requirement to obtain prior authorisation by the relevant Dutch regulator. Note, however, that undertaking marketing or advertising activities within the Netherlands will frustrate the outcome of the initiative test. Furthermore, if the financial company were to have a large client base in the Netherlands, there would be a risk that the relevant Dutch regulator would take the position that the financial company may no longer rely on the initiative test.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

As of 25 May 2018, the processing of personal data in the Netherlands is regulated by the General Data Protection Regulation (GDPR). The GDPR directly applies in all EU Member States. The Dutch GDPR Implementation Act clarifies, within the limits allowed by the GDPR, the application of the new legal framework in the Netherlands.

In principle, the GDPR applies to fintech businesses established in the EU and, in some cases, also established outside the EU.

The GDPR regulates any form of processing of personal data, including its collection, use and transmission within and outside the EEA. Unlike the previous legal regime, the GDPR applies both to companies that determine the purpose and the means of processing personal data (controllers) and to companies processing personal data on behalf of the data controllers (processors), such as cloud service providers.

The GDPR maintains the principle-based approach to personal data protection. The general principles that must always be observed require that companies:

- process personal data lawfully, fairly and in a transparent manner;
- collect personal data only for specified, explicitly defined and legitimate purposes;
- process and store personal data no longer than required for the purpose of the processing; and
- adopt and maintain appropriate measures to ensure the security personal data.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

The GDPR applies to the processing of personal data in the context of the activities of a company (controller or processor) in the EU, irrespective of whether the processing takes place in the EU or not. Furthermore, the GDPR also applies to companies (controller or processor) established outside the EU if they: (i) offer goods or services to individuals in the EU; or (ii) monitor the behaviour of individuals in the EU. Thus, an EU fintech company must comply with the GDPR even if it carries out all processing of personal data outside the EU. Similarly, a non-EU fintech company must comply with the GDPR if it provides services to customers in the EU.

The GDPR restricts transfers of personal data outside the EEA, unless a country is seen as having an adequate level of personal data protection. So far, only 12 countries, including Canada, Israel, New Zealand, Switzerland and Japan, are recognised as having adequate protection. The transfer of personal data is also unrestricted for US recipients that adhere to the “Privacy Shield Framework”. To transfer personal data to other countries outside the EEA, controllers must put in place appropriate safeguards; for example, the inclusion of the Standard Contractual Clauses adopted by the European Commission in an agreement between contracting parties. In addition, under the GDPR, Binding Corporate Rules (BCRs), codes of conduct and certification schemes are explicitly recognised as appropriate safeguards. In the absence of appropriate safeguards, data controllers may transfer personal data outside the EEA data based on specific derogations, such as explicit consent of the data subject or necessity of data transfer for the conclusion or performance of a contract with a data subject. These derogations, however, can only be used for occasional and not repetitive transfers.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

The GDPR significantly increased penalties for violations of personal data protection rules throughout the EU. Companies that do not comply with the GDPR are subject to fines of up to EUR 20 million, or 4% of the annual worldwide turnover of an undertaking, per violation, whichever is higher. European Data Protection Authorities (DPAs) interpret the concept of “undertaking” – borrowed from EU competition law – broadly to include the whole

“economic unit” rather than a legal entity of a data controller or processor. As a result, under certain circumstances, DPAs may use the revenue of the whole group to calculate fines under the GDPR. Sanctions under the GDPR apply to controllers and processors. DPAs can also issue temporary or definitive injunctions on data processing and place companies under regular audits.

In addition, companies may also be obliged to compensate for damages suffered by individuals as a result of infringement of the GDPR.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

The Netherlands has implemented the EU Network and Information Security (NIS) Directive by the Dutch Cybersecurity Act, which took effect on 9 November 2018. The NIS Directive and the Dutch Cybersecurity Act require operators of essential services and digital service providers to notify competent authorities of serious cybersecurity breaches. This obligation applies to the following categories of financial institutions:

1. credit institutions;
2. trading venues (regulated markets, multilateral trading facilities or organised trading facilities);
3. central counterparty clearing institutions;
4. central security depositories; and
5. providers of settlement services.

DNB will adopt a list of specific organisations that fall under this obligation. Under the Dutch Cybersecurity Act, penalties for violation of the cybersecurity breach notification requirement include an administrative fine of up to EUR 5 million.

When it comes to the security of personal data, the GDPR also outlines data security obligations for companies that process personal data, including fintech businesses. Under the GDPR, these companies must implement “appropriate technical and organisational measures” to ensure a level of security for personal data “appropriate to the risk”. The GDPR also requires data controllers to report personal data breaches to DPAs within 72 hours after “becoming aware” of the breach and to data subjects “without undue delay”, if their privacy is put at risk.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

The two main sources of anti-money laundering law are the Dutch Criminal Code (DCC) and the Act for the Prevention of Money Laundering (WWFT).

Money laundering under the DCC is a broad concept. It entails, among other things, handling (i) property acquired through an offence, or (ii) the proceeds of crime. Moreover, persons who are negligent or wilfully blind in recognising that funds or assets have been derived from criminal property commit a criminal offence. The offence of money laundering is punishable by a maximum of eight years’ imprisonment or a fine of up to EUR 83,000.

Under the WWFT, specific financial institutions are required to undertake certain customer due diligence before they establish business relationships. Whether a financial institution falls within the scope of the WWFT depends on the regulated activity of the fintech business. Risk-based due diligence must be conducted, for example, if the company has any doubts in regard to the veracity of information provided by the client or when incidental transactions of at least

EUR 15,000 occur. Furthermore, enhanced customer due diligence might be required when a customer can be identified as a politically exposed person. Enhanced customer due diligence is likely required when dealing with cryptocurrencies. Other requirements from the WWFT are the duty to report unusual transactions and the requirement to observe sufficient recordkeeping. Penalties upon infringement could result in a maximum of four years' imprisonment or fines up to EUR 83,000. In addition, the Dutch Minister of Finance may impose an order for incremental penalty payments and administrative fines with a maximum of EUR 5 million per infringement. Refer to question 3.2 for the proposed implementation act of the 5th AMLD into Dutch national law, which currently looks to specifically include certain virtual currency service providers.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

There is no legislation in place in the Netherlands aimed specifically at the fintech sector. Fintech businesses that provide services to consumers may be subject to, for example, the EU Consumer Directive (2011/83/EU), which is implemented in the Dutch Civil Code. This Directive lays down requirements on, for example, the provision of information to consumers. Fintech businesses that provide their services to consumers online may also be subject to the EU Directive on Privacy and Electronic Communications (2002/58/EC). This Directive is implemented in Dutch law and requires businesses to notify consumers and obtain their consent for the use of cookies.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

The legal framework with regard to the hiring of staff is limited. Several laws prohibit employers from discriminating based on age, sex or religion when hiring employees. The employment agreement has no prescribed form and can be temporary or permanent. However, certain restrictive provisions (for example, probationary period, non-competition clause, unilateral changes clause, penalty clause) must be agreed on in writing.

Under Dutch dismissal law, there are two ways in which the employment agreement can be terminated unilaterally by the employer:

- i. giving notice to the employee after having obtained a dismissal permit from the Employee Insurance Agency; or
- ii. requesting that the court dissolve the employment contract.

The law provides for eight limited grounds for dismissal, and the relevant ground determines which termination route must be followed.

In order to unilaterally terminate the employment agreement, the employer must demonstrate that there is a reasonable ground (that is, the conditions of at least one of the limited grounds have been fully met) and that it is not possible to reassign the employee within a reasonable period to a suitable alternative position within the company.

In practice, employment agreements are more often terminated by means of a mutual termination agreement. It is common for employers

to pay a severance payment upon termination. An employee who has been employed for 24 months or more is entitled to a statutory transition payment if employment is terminated by the employer. The amount of the transition payment depends on the salary, age and seniority of the employee. The transition payment is capped at EUR 81,000 gross, or one gross annual salary if the annual salary of the employee exceeds EUR 81,000 gross (2019 figures).

In certain situations, the dismissal of an employee is prohibited, among other things, during pregnancy or maternity leave, or during the first two years of illness.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Staff are entitled to at least:

- i. the statutory minimum wage;
- ii. a vacation allowance of 8% of the employee's annual salary; and
- iii. vacation days to an amount of four times the amount of days worked per week (20 vacation days per year on the basis of a full-time contract).

During the first two years of illness, an employee is entitled to at least 70% of his salary, with a minimum of the statutory minimum wage and a maximum of the maximum daily wage (as defined by social insurance law). In practice, many employers pay their employees up to 100% of the employee's salary during the first, or even the second, year of illness. During this period, the employer and employee must work together to reintegrate the employee. After this two-year period, the obligation to pay the salary ends, unless the Employee Insurance Agency is of the opinion that the employer did not do enough to reintegrate the employee. In that case, the two-year period in which the employer is obliged to continue to pay an employee's salary can be extended by a maximum of one year.

Mandatory employment conditions can also follow from collective bargaining agreements, applicable to a specific industry or to a company or group of companies. It is generally not possible for an employer to deviate from a collective bargaining agreement to the detriment of an employee.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

When hiring staff, a Dutch company must recruit first from within the EEA or Switzerland. Employees from EEA countries and Switzerland do not need a work or residence permit. Only if a company is able to prove that it cannot find any suitable employees within the EEA or Switzerland will it be allowed to recruit from other countries. These employees will usually require a work and residence permit.

This does not apply in the case of highly skilled migrants. In order to bring highly-skilled migrants to the Netherlands, the Immigration and Naturalization Service must recognise the employer as a sponsor. Recognised sponsors can make use of an accelerated application procedure for residence permits. The highly-skilled migrant must, among other conditions, earn a sufficient independent long-term income that is in accordance with market conditions. Refer to question 2.2 for the 30% income tax exemption for qualifying expats.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Innovations and inventions are primarily protected by patents but, depending on the type of invention, can also be protected to a certain extent by other intellectual property rights, such as copyrights (software), database rights and design rights. Know-how and technical information are also protected as trade secrets to the extent the information is kept secret.

Patents

Inventions can be patented for a period of up to 20 years if they are novel, involve an inventive step and are susceptible to industrial application. In contrast to the US, software *as such* and business methods are excluded from patentability in Europe. However, an invention devised in a software context can be patentable if it is claimed in the context of the technical system in which it operates (for example, a physical device in which the software is integrated).

A Dutch patent may be applied for at the Dutch Patent Office. Dutch patents are not preliminarily reviewed by the Dutch Patent Office and are not subject to opposition proceedings. A Dutch patent can also be obtained as part of a European patent, which is a bundle of national patents.

Additionally, the EU patent package – aimed at introducing a European patent with unitary effect and the Unified Patent Courts – is pending. The European patent with unitary effect is not a bundle of national patents, but can be directly enforced in all participating states, among which are the Netherlands, through the Unified Patent Courts. Whether this new system will actually enter into effect, and when it might happen, is not yet clear, since German ratification has been delayed due to a constitutional complaint. In addition, the uncertainty around a possible Brexit might also impact the launch of the Unified Patent Courts.

Trade secrets

Information is protected to the extent that it (i) is secret, meaning it is not generally known or readily accessible, (ii) has commercial value because it is secret, and (iii) has been subject to reasonable steps to keep it secret. This follows from the Dutch Trade Secrets Act that implements the European Trade Secrets Directive, which in turn is the implementation of Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS).

Technical data, such as software code and algorithms, can be protected by the Dutch Trade Secrets Act, provided that the abovementioned criteria are met. However, independent creation and reverse engineering do not fall within the scope of trade secret protection, so for software to be effectively protected, it is important that the trade secret encompassed within it not be reduced from its functionalities.

The Dutch Trade Secrets Act provides for protection against misappropriation of trade secrets, that is, unlawful acquisition, use or disclosure by third parties. The owner of a trade secret has a number of available IP-style remedies, such as injunctions, recalls, damages and evidential seizures. Additionally, actions can be taken against third parties for misappropriation where that party did not know, but should have known, about the misappropriation, or was made aware of the misappropriation. Furthermore, action can be taken against infringing goods that “significantly benefit” from the misappropriation.

Copyrights, database rights, design rights, trademarks

Except for the protection of the source code of software (which arises by operation of law), copyrights play a limited role in

protecting innovations and inventions since technical information regarding functional aspects is exempt from copyright protection. Software code is eligible for copyright protection if it is original, in the sense that it is its author’s own original intellectual creation. This protection also extends to preparatory design work leading to the development of a computer program, provided that no further creative steps are needed in order to create a computer program. The underlying algorithm itself, on the other hand, is not protected by copyright; neither are works resulting from strictly algorithmic processes.

A database is protected by a (*sui generis*) database right insofar as the database is the result of a substantial investment in either the obtaining, verification or presentation of its contents (“sweat of the brow protection”).

Both Benelux and Community designs can be relied upon to protect the appearance of a product insofar as the design is novel and has individual character. The branding of innovations and inventions can be protected through trademarks. Both design rights and trademarks have to be registered.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

In principle, a Dutch patent will be owned by the patent applicant. Any other party, which claims that it is entitled to the patent, can initiate court proceedings.

If an invention was made by an employee, the employee is entitled to the patent unless the nature of the employee’s service entails the use of the employee’s special knowledge for the purpose of making such inventions. For inventions made during training or by employees of educational or research institutions, the employer and the institutions, respectively, are generally entitled to the patent. However, this is not mandatory law. Employment agreements therefore generally contain arrangements to ensure that all inventions and related rights are owned by the employer.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

Various treaties and multi-jurisdictional rights apply in the Netherlands with regard to intellectual property, such as the Paris Convention for the Protection of Industrial Property, TRIPS, the European Patent Convention (EPC) and the Patent Cooperation Treaty (PCT).

Under certain circumstances, foreign rights (such as patents) can be enforced in the Netherlands, but only with respect to the territories in which such rights are valid. For example, a Dutch court can grant an injunction for a German patent, but only with respect to Germany.

As indicated under question 6.1, if the EU patent package becomes effective, it will provide for European patents with unitary effect, which may be directly enforced in the Netherlands.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

Licensing is commonly used for monetising IP rights. The licensee generally has the authority to perform the acts that would normally be infringements, in exchange for licence fees. Further details

should be specifically agreed upon in licensing agreements. Specific restrictions relating to patents are compulsory licences, acts with regard to research on the patented matter (the research exception) and prior use. A special tax rate of 7% applies for profits and losses resulting from patented inventions.

Acknowledgment

The authors would like to acknowledge Christian Godlieb for his contribution in the preparation of this chapter. Christian is an associate in De Brauw Blackstone Westbroek's Financial Markets Regulation practice group and specialises in innovation in the financial sector. He regularly publishes on the development of regulation on that topic. In 2018, Christian co-authored the Netherlands chapter of *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019*.

Tel: +31 20 577 1474 / Email: Christian.Godlieb@debrauw.com / LinkedIn: <https://www.linkedin.com/in/christian-godlieb-02746a22>.



Björn Schep

De Brauw Blackstone Westbroek
Claude Debussylaan 80
1082 MD Amsterdam
Netherlands

Tel: +31 20 577 1358
Email: Bjorn.Schep@debrauw.com
URL: www.debrauw.com

Björn Schep is a senior associate in the firm's Financial Markets Regulatory Practice Group and specialises in financial law and, in particular, investment management and financial markets regulation. Björn was seconded to Slaughter and May in London in 2012, where he worked in the Financial Regulation group. In October 2017, Björn completed the Executive Master Insurance Studies/Enterprise Risk Management at the Amsterdam Business School.

He regularly advises insurers, banks, investment firms and financial services providers on applicable financial regulatory requirements, such as licence requirements, prudential requirements and market conduct requirements. Björn has assisted large established banks and insurers in the Netherlands with their discussions with DNB and the AFM in connection to new innovative ideas. Björn has worked with several fintech start-ups, mostly advising them on market access issues. In 2018, Björn co-authored the Netherlands chapter of *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019*.



Willem Röell

De Brauw Blackstone Westbroek
Claude Debussylaan 80
1082 MD Amsterdam
Netherlands

Tel: +31 20 577 1358
Email: Willem.Roell@debrauw.com
URL: www.debrauw.com

Willem Röell advises a wide range of financial institutions on financial regulatory matters as member of De Brauw's Financial Markets Regulatory Practice Group with previous experience in financial litigation. Willem is part of the firm's Fintech team advising fintechs on, for example, licensing requirements, prudential requirements and market conduct requirements, and has been researching blockchain developments, including cryptocurrencies and smart contracts, since 2014. Willem is frequently invited to speak about the legal aspects of working with new technologies, such as distributed ledgers and payment solutions. In 2018, Willem co-authored the Netherlands chapter of *Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019*.

Willem is active for several charitable organisations with a focus on education, human rights and art.

DE BRAUW BLACKSTONE WESTBROEK

De Brauw is the largest law firm in the Netherlands, with offices in Amsterdam, Brussels, Frankfurt, London, Shanghai and Singapore. Our goal is to always be one step ahead of the pack, and to be at the forefront of new developments. This is why we were the first Netherlands-based firm to open offices in New York and London, to publicly offer our clients alternative fee arrangements, to start a public discussion about the way lawyers should be trained, and to increase and improve the role of visual design in our advice. And this is why we are one of the first in making a start with artificial intelligence pilots, managing our know-how, and building a due diligence tool. We have in-depth knowledge of the financial services sector. We combine all required expertise and are currently developing innovative solutions for fintech.

New Zealand

Andrew Dentice



Rachel Paris



Hudson Gavin Martin / The Blockchain Boutique

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Fintech is the fastest-growing segment of the New Zealand technology sector, increasing 42% year-on-year in 2018. This growth has been fuelled by local start-ups cultivated by fintech accelerator programmes, as well as the entry of offshore businesses attracted by low corruption, the ease of doing business and New Zealand's proximity to Australia and Asia.

One hallmark of the New Zealand fintech scene is the close collaboration between established financial institutions such as banks and insurers with start-ups and financial market regulators. Industry working group FinTech NZ serves as a central liaison point for this vibrant ecosystem, and its member businesses are applying technology to the full range of financial services: payments; investing; crypto-micro saving; robo-advice; peer-to-peer lending; crowd-funding; financial literacy; and insurtech.

Two current initiatives are expected to unlock further opportunities for fintechs operating in New Zealand in the near term:

- In December 2018, the Government announced a major digital identity project to be led by the Department of Internal Affairs in collaboration with the private sector. This initiative is expected to help fintechs meet privacy, anti-money laundering and other know-your customer requirements (for example, as part of the responsible lending regime for consumer credit).
- In addition, an “open banking” pilot initiated in 2018 by Payments NZ – a bank consortium – is developing standardised application programming interfaces (API) to enable data sharing between banks and fintechs.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

No, there are not.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

The New Zealand Government provides funding for early-stage businesses through three main channels:

- Callaghan Innovation provides grants and repayable loans to technology-based early stage ventures, with most funding supporting research and development activity.
- The New Zealand Venture Investment Fund has NZ\$245 million funds under management, of which NZ\$50 million is held in a seed co-investment fund to support young technology companies.
- The Icehouse – which also receives some private funding – invests in early-stage businesses through two investment funds and its angel investor network.

Funding support is also delivered by state and private sector-backed technology accelerators.

In addition, many young businesses have raised capital through licensed equity crowdfunding platforms and peer-to-peer lenders, in addition to credit lines obtained from banks and finance companies.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

The New Zealand Government announced a NZ\$1 billion fund for research and development (R&D) and a new R&D tax incentive in the 2018 Budget.

The main features of the R&D tax incentive, which is available from the beginning of a business's 2019/2020 income year, are:

- a credit rate of 15%;
- a NZ\$120 million cap on eligible expenditure;
- a minimum R&D expenditure threshold of NZ\$50,000 *per annum*; and
- a broad definition of what constitutes eligible R&D.

Until the new incentive takes effect, loss-making start-ups will still have access to a limited form of refundable tax credits. A more comprehensive refund system will be introduced in April 2020, replacing R&D growth grants from Callaghan Innovation.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

Securities law

To IPO, a business must make a regulated offer of equity securities in accordance with the Financial Markets Conduct Act 2013 (**FMC Act**). The FMC Act requires issuers to make prescribed disclosures in a “product disclosure statement” (**PDS**) which should be underpinned by a robust due diligence process to ensure the content is not false or misleading, nor likely to mislead. Other material information must be uploaded to an online register and kept up to date during the term of the offer.

Exchange requirements

The business will also need to meet the listing requirements of NZX, New Zealand’s stock exchange. NZX has a wide discretion to approve or reject listing applications and may impose specific conditions on the business in relation to governance, minimum expected value of the listed shares, and minimum shareholder spread and hold criteria.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

The most notable fintech IPOs in New Zealand have been:

- the early listing of Xero, a New Zealand financial SaaS company, in 2007. Xero has a current market capitalisation of NZ\$7.5 billion; and
- Pushpay – a payments company focused on the faith and non-profit sectors – which raised NZ\$9 million in a 2014 IPO, but is now valued at over NZ\$1 billion.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

New Zealand’s technology-neutral financial regulation has generally accommodated fintech without the need for specific concessions or enabling legislation.

Fintechs operating in New Zealand may need to comply with the following regulations, depending on the specific nature of their activities:

- **Licensing requirements:** Any fintech that engages with retail customers in New Zealand needs a licence to provide financial advice, take deposits, manage funds, operate a financial product market, operate a “disclosure-lite” equity crowd-funding or peer-to-peer lending business, provide discretionary investment management services or issue derivatives. In addition, a fintech that carries on insurance business in New Zealand needs to be licensed by the Reserve Bank of New Zealand (**RBNZ**). Notably, no licence is required to transmit money or to provide credit.
- **Registration requirements:** Any fintech business that undertakes a licensed activity (see above) or which has a physical place of business in New Zealand and provides a financial service must register on the public Financial Service Providers Register. Registration is a mechanical process which can be undertaken online and does not indicate regulatory approval. If services are offered to retail clients, the business must also join an approved scheme which gives consumers access to free dispute resolution services.

- **Anti-money laundering regulations:** Any fintech that handles funds in the ordinary course of its business is likely to be a “reporting entity” and is, therefore, subject to New Zealand’s anti-money laundering legislation. See question 4.5 for further detail.
- **Prudential regulation:** All registered banks, non-bank-deposit takers, and insurers are subject to prudential regulation by the RBNZ, including capital adequacy, liquidity, governance and disclosure requirements. In addition, the licensing criteria of the Financial Markets Authority (**FMA**) includes some minimum prudential standards. Fintechs which provide support services to licensed institutions may find that their outsourcing arrangements are subject to the RBNZ’s or the FMA’s outsourcing rules.
- **Conduct regulations:** Any fintech business participating in New Zealand’s financial markets is subject to minimum conduct standards, including fair dealing standards which are primarily enforced by the FMA. Following the Royal Commission into the banking and insurance sector in Australia, the RBNZ and FMA have taken a joint review into the conduct and culture of New Zealand banks and insurers. While the results of the New Zealand review were far less condemning than the Australian equivalent, it is expected that New Zealand regulators will strengthen their focus on conduct in the future and this will extend to fintech players.

In addition, fintechs must comply with applicable corporate, taxation, anti-trust and financial reporting and consumer protection laws.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

There is no cryptocurrency-specific or cryptoasset-specific regulation in New Zealand to date.

Securities and financial laws

Any cryptographic token with the features of an equity security, a debt security, a managed investment product (**MIP**) or derivative (as defined in the FMC Act) would automatically be regulated as a “financial product” under that statute, irrespective of its technical form. Similarly, the Anti-Money Laundering and Countering the Financing of Terrorism Act 2009 (the **AML Act**) captures any activity transacted with cryptocurrencies or cryptoassets which is, in substance, a regulated financial activity.

The FMA has issued guidance setting out its interpretation of how existing securities and financial services laws apply to cryptocurrencies and cryptoassets, including when issued in “initial coin offerings” and similar events. The guidance also considers associated service providers, such as brokers, exchanges, and wallet providers dealing in cryptocurrencies and cryptoassets.

Taxation

The Inland Revenue Department (**IRD**) has also issued guidance confirming that there are no special tax rules for cryptocurrencies and that ordinary tax rules apply. The IRD’s guidance uses the term “cryptocurrency” broadly to encompass all cryptographic tokens, beyond currency tokens. The effect of the IRD’s guidance is to confirm that it will treat all cryptocurrencies and cryptoassets as property for tax purposes, unless a contrary decision is reached on the relevant facts in a private binding ruling.

The IRD has announced that it is considering a range of issues related to cryptocurrency at present, and further guidance is expected imminently.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

New Zealand's key financial market policy-makers and regulators are receptive to fintech.

The FMA, in particular, has been proactive in meeting with the fintech industry. When an inadvertent legislative barrier to robo-advice was identified (namely, a requirement that only a human could provide financial advice), the FMA exercised its exemption power in 2018 to permit digital advice to be provided when minimum conditions are met.

The Ministry Of Business, Innovation & Employment (MBIE) is also supportive of fintech initiatives, working with industry group FinTech NZ and participating in the FinTech Regulatory Roundtable to explore opportunities for fintech growth. MBIE also commissioned a major 2018 report into opportunities for the local blockchain industry and supports New Zealand's industry-led open banking trials. A particular area for focus for MBIE is developing a digital identity solution which will accelerate many fintech opportunities.

Given its mandate to maintain a sound and efficient financial system, the RBNZ has taken a more cautious "wait-and-see" approach to fintech. However, it has publicly stated that it does not wish to hinder fintech growth and acknowledges fintech's potential to enhance the efficiency of the financial sector.

New Zealand does not have a regulatory sandbox or accelerator hub for fintech. The FMA's rationale is that, given New Zealand's relatively light regulatory requirements and the approachability of the relevant regulators, a concessionary regulatory environment is not needed. In practice, industry-led groups such as FinTech NZ and the FinTech Regulatory Roundtable have had good traction with the regulators so that any regulatory barriers have been identified and solutions advanced without the need for a formal "sandbox" initiative (although fintechs need to be well advised in advance to ensure a decent hearing when directly approaching the regulators to test their ideas).

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

It is relatively straight-forward for offshore fintechs to access New Zealand customers.

If the fintech is offering its financial services to New Zealand retail clients, then it will need to comply with the applicable regulations outlined in question 3.1. Depending on the nature of the fintech's business, this will include compliance with market conduct rules, disclosure and governance requirements, any applicable licensing regime and consumer protection laws.

On the other hand, if the fintech limits its offers to eligible wholesale clients, then generally the only applicable financial regulation is compliance with fair dealing rules. These comprise anti-hawking provisions and prohibitions against misleading or deceptive conduct, and false, misleading or unsubstantiated representations in relation to financial products.

A foreign fintech would also need to assess whether its New Zealand-based activities resulted in it "carrying on business" for the

purposes of the Companies Act 1993, in which case it would need to register a foreign branch and submit audited financial statements to the Companies Office. A fintech with a registered foreign branch in New Zealand should also consider whether it falls within the territorial scope of New Zealand's anti-money laundering laws.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

Collection, storage, use and disclosure of personal data (described in New Zealand as "personal information") is regulated by the New Zealand Privacy Act 1993 (**Privacy Act**). The Privacy Act sets out 12 "information privacy principles" that apply to all individuals and organisations that deal with information about identifiable individuals.

The Credit Reporting Privacy Code 2004 (**Code**) applies specifically to credit reporters and modifies the application of the information privacy principles to credit information. The Code also prescribes requirements for subscriber agreements, access agreements and other documents relating to the collection of credit information from individuals.

In addition to credit reporting, codes of practice also exist in respect of health information and telecommunications information.

Fintech businesses must comply with the Privacy Act to the extent they collect, hold and use personal information about individuals (such as customers, prospective customers, local employees or agents) in relation to their New Zealand operations. Compliance with the Code may also be required in the context of any credit reporting activities.

A new Privacy Bill is likely to be passed in 2019 which introduces various changes to New Zealand's privacy law, including certain changes intended to bring the law more in line with the European General Data Protection Regulation.

In addition, rules apply to the transmission of certain data under the AML Act, as discussed in question 4.5.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

Overseas-based organisations that operate in New Zealand are required to comply with the Privacy Act. Whether an organisation "operates in New Zealand" will depend on the nature of its New Zealand operations, including its physical presence in New Zealand. The New Zealand branch of an overseas organisation will generally be subject to the Privacy Act.

Transfer of personal information outside New Zealand is not restricted by the current Privacy Act. However, the Privacy Commissioner may prohibit a transfer of personal information from New Zealand to another country if they reasonably believe the information will not be subject to comparable safeguards in the other country (for example, compliance with EU data protection law), or the transfer would be likely to contravene the principles set out in Part Two of the OECD Guidelines. This power is not used regularly.

Personal information transferred out of New Zealand will be subject to certain information privacy principles, although an organisation

will not breach any of these principles in respect of any action that the organisation is required to take by or under the law of any place outside New Zealand (section 10).

Accordingly, where an organisation wishes to transfer personal information outside New Zealand, it must ensure the personal information will be subject to acceptable privacy standards in the foreign country. The organisation will continue to be responsible for the security of that information while it is held overseas, and will be liable for any privacy breaches committed by overseas agents, so it should be comfortable that reasonable steps have been taken to protect information from unauthorised use or disclosure.

The Privacy Bill, once passed, will introduce new restrictions on the transfer of information overseas. Under the new regime, entities will need to meet certain criteria in order to transfer information overseas, including agency arrangements, individual consent, comparable privacy safeguards in the foreign jurisdiction and contractual safeguards.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

A complaint may be made under the Privacy Act in respect of an “interference with the privacy of an individual” (section 66).

In the first instance, a complaint will be investigated by the Privacy Commissioner. If the Commissioner considers the complaint has merit, it may attempt to secure a financial settlement between the parties, although it is unable to impose a binding damages award (section 74).

A complaint may be referred to the Human Rights Review Tribunal (HRRT) by the Commissioner or an aggrieved individual themselves. If the HRRT finds there has been privacy interference, it may grant an award of damages to compensate for pecuniary loss, loss of a benefit, or humiliation, loss of dignity, and injury to the feelings of the aggrieved individual. The HRRT is not required to award damages and a number of non-pecuniary penalties are also available (section 85).

There is no limit on the damages that may be awarded. Penalties for less serious cases may range from NZ\$5,000 to NZ\$10,000, while more serious cases can range from NZ\$10,000 to around NZ\$50,000, and the most serious cases will range from NZ\$50,000 upwards. The highest award to date is around NZ\$168,000.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

New Zealand does not have any cyber security laws or regulations that are likely to apply directly to fintech businesses.

However, telecommunications network operators are required to have interception capability in their networks under the Telecommunications (Interception Capability and Security) Act 2013 (TICSA). Should fintech businesses utilise telecommunications networks in the provision of their services or provide services to telecommunications operators, it is possible that network operators will attempt to pass through their TICSA obligations in their contracts.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

New Zealand’s anti-money laundering legislation is the AML Act. A fintech business will need to comply with the requirements of the AML Act if it meets the broad activity-based definition of a

“financial institution” (or other species of “reporting entity”), assuming an exemption is not available.

If a fintech is a reporting entity, it must:

- register with a supervisor (the RBNZ, the FMA or the Department of Internal Affairs, depending on the nature of its activities);
- complete an assessment of the risk of money laundering and terrorism financing that relates to its business, and keep it updated;
- prepare a compliance programme responding to that risk assessment, and keep it updated;
- undertake due diligence at the required level (simplified, standard or enhanced) on its customers;
- actively monitor transactions and comply with suspicious transaction and other reporting requirements;
- appoint a compliance officer; and
- submit annual reports to its supervisor and comply with audit requirements.

Additional financial crime laws are contained in the Crimes Act 1961 and the Terrorism Suppression Act 2002.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

To the extent applicable, fintech businesses will need to comply with other general regulatory regimes for businesses delivering goods and services in New Zealand:

- **Consumer protection:** The Consumer Guarantees Act 1993, Fair Trading Act 1986, Contract and Commercial Law Act 2017 and Unsolicited Electronic Messages Act 2007 will apply to businesses’ consumer interactions, transactions, marketing and contracts.
- **Competition law:** The Commerce Act 1986 prohibits anticompetitive behaviour such as cartel conduct (e.g. price fixing) and abuse of market power.
- **Consumer finance and securities:** The Credit Contracts and Consumer Finance Act 2003 (CCCFA) and Personal Property Securities Act 1999 regulate the provision of consumer credit and, in the case of the CCCFA, includes responsible lending requirements for consumer lenders.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

New Zealand has a comprehensive set of employment laws across multiple statutes and common law. The principal legislation is the Employment Relations Act 2000 (ERA).

Hiring

Every employee must have a written employment agreement with at least the minimum legal entitlements discussed in the next section. The employment agreement may also provide additional negotiated terms, including in relation to a trial period, notice periods for resignation and termination, redundancy payments, overtime rates and long service leave.

Employers may impose a trial period of up to 90 days during which the employment can be terminated at any time. From 9 May 2019,

trial periods will be restricted to businesses with less than 20 employees. Specific rules must be strictly complied with to ensure the trial period is valid.

Fixed term contracts are also valid if strict statutory requirements are met and there is a genuine reason based on reasonable grounds for the fixed term.

Dismissal

- *General dismissal:* To dismiss an employee, an employer must act in good faith and follow a fair and reasonable process to avoid risking a personal grievance claim. The employee is entitled to request a written statement of the reasons for dismissal.
- *Dismissal during trial/probationary period:* An employee's employment can be terminated at will during a valid trial period. From 6 May 2019, businesses with 20 or more employees will be able to use a probationary period to assess an employee's skills against the role's responsibilities, and can follow a prescribed process for managing performance issues and ending employment if the issues are not satisfactorily resolved.
- *Dismissal for serious misconduct:* An employee can be dismissed for serious misconduct without prior notice or payment, provided strict steps are followed and the employer's actions are fair and reasonable.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Holidays and other leave

Each employee is entitled to at least four weeks' paid annual leave and 11 paid public holidays per year.

After six months' continuous employment, an employee is also eligible for sick leave and bereavement leave.

Parental leave and other pregnancy-related benefits are set out in the Parental Leave and Employment Protection Act 1987. Employees on primary carer leave receive a government-funded payment for the duration of the leave equal to the greater of the employee's ordinary weekly pay or average weekly income, up to a maximum of approximately NZ\$540 gross per week.

Flexible working arrangements

An employer has a "duty to consider" a request for flexible working from an employee and may only refuse this on recognised business grounds specified in the ERA. The employer must notify the employee of its decision in writing and give reasons for any refusal.

KiwiSaver contributions

Employers must make compulsory contributions to voluntary workplace savings scheme KiwiSaver for every employee that is a member of a KiwiSaver scheme. The current contribution rate is 3% *per annum* of the employee's gross salary or wage.

Additional requirements

In addition to the above, minimum entitlements include access to breast-feeding breaks and facilities, rest and meal breaks in some circumstances, and employment-related education leave.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

Employees from outside New Zealand must hold a valid work visa issued by Immigration New Zealand, unless they are a citizen or resident of Australia or are eligible for an exemption.

A fintech business can apply to become an accredited employer with Immigration New Zealand to fast-track work visas for foreign employees.

A work visa is granted subject to the candidate meeting minimum criteria for health, character, and skills relevant to the visa category (for example, skilled migrant, essential skills or specific purpose). There is an additional visa category for employees of companies relocating to New Zealand.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

New Zealand has a robust patent system. Patents are available for novel, inventive and useful inventions that are a "manner of manufacture" (as defined by the Statute of Monopolies). Patents are not available for inventions that are contrary to public order or morality.

Patents for computer programs as such are not available, but inventions that include implementation by a computer program are able to be patented. The key relevant question will be whether the contribution the invention makes lies in the computer program, in which case it is not patentable in New Zealand.

New Zealand's copyright law protects most creative works, and protects computer programs as literary works.

New Zealand has a strong trade mark registration system. New Zealand law also protects unregistered trade marks through passing off and the Fair Trading Act, which prohibits misleading or deceptive conduct in trade.

New Zealand operates on a common law system, which provides strong protection for trade secrets and other confidential information.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Generally the creator of the IP is the owner under New Zealand law.

An inventor is the person who is entitled to apply for a patent, although this right can be assigned.

The creator of the copyright work is usually the owner of the relevant copyright. The exceptions to this are:

- literary, dramatic, musical or artistic works made by an employee in the course of their employment (unless contracted otherwise), in which case the employer is the owner of the copyright; and
- commissioned photographs, computer programs, paintings, drawings, diagrams, maps, charts, plans, engravings, models, sculptures, films or sound recordings, in which case the commissioner is the owner of the copyright (unless contracted otherwise). This "commissioning rule" is worth specific attention, as it differs from the default position in many other jurisdictions that a contractor who creates a work will own the copyright unless contracted otherwise.

Ownership of IP can be assigned.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

New Zealand is a party to the Berne Convention, so nationals of other Berne Convention countries and copyright works created in

other Berne Convention countries automatically have copyright ownership in New Zealand. There is no copyright register in New Zealand.

Registered trade marks and patents are national rights in New Zealand, so need to be applied for here.

In some cases a reputation in a trade mark can be obtained in New Zealand through use in other countries, which can be used to prevent others using or registering the same or similar marks, but this can be difficult to achieve without any use in New Zealand.

If a breach of confidential information or trade secret occurs in New Zealand, it can be addressed under New Zealand law, even if that confidential information originated outside of New Zealand.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

IP can be exploited or monetised in New Zealand through use by the owner, or assignment or licensing of the IP to third parties.

An exclusive licensee has the ability to sue for patent or copyright infringement. A licensee can sue for trade mark infringement, if the owner of the trade mark registration does not.

There are no particular rules that apply to exploiting or monetising IP in New Zealand. A compulsory licence can be granted in relation to patents that are not being exploited.



Andrew Dentice

Hudson Gavin Martin
2 Commerce Street
Auckland 1143
New Zealand

Tel: +64 9 3087 314
Email: andrew.dentice@hgmlegal.com
URL: www.hgmlegal.com

Andrew is a technology lawyer at Hudson Gavin Martin in Auckland – with a focus on data, platforms and “as a Service” business models. He regularly helps fintech clients navigate complex legal issues to execute their business strategy – whether providers or customers, incumbents or challengers. He is recognised as a “Next Generation Lawyer” in the 2019 *The Legal 500* rankings for TMT, where he is praised as having “stacks of common sense and instinctive good judgement”.

Andrew sits on the Executive Council for FinTech NZ and is a member of the NZ Fintech Regulatory Roundtable – a cross-industry group considering key regulatory issues in financial services and technology.

Prior to joining HGM, Andrew led the FinTech & Innovation commercial legal practice at Barclays in the UK, where he provided strategic advice on the bank’s technology and innovation projects – in areas such as cloud, cyber security, open banking and APIs.



Rachel Paris

The Blockchain Boutique
57 Owens Road
Epsom, Auckland
New Zealand

Tel: +64 21 414 514
Email: rachel@theblockchainboutique.io
URL: www.theblockchainboutique.co.nz

Rachel is financial services and capital markets lawyer and the founder of specialist fintech and blockchain advisory practice, The Blockchain Boutique.

The Blockchain Boutique collaborates with Hudson Gavin Martin to support mutual fintech clients as part of a strategic relationship between the two firms.

Previously, Rachel was a banking and finance partner for almost 10 years in major New Zealand commercial law firm Bell Gully, where she founded the Fintech team and advised blue-chip financial institutions, corporates and private equity funds on a range of finance and capital markets transactions. Rachel has also worked in London for top firms Allen & Overy and Olswang.

Rachel has been ranked for many years as a leading lawyer in both banking and finance and investment funds in global legal directories including *Chambers Asia-Pacific*, the *IFLR 1000* and *The Legal 500*, and holds an L.L.M. (International Finance) from Harvard Law School.

**Hudson
Gavin
Martin**
Technology, Media and IP Lawyers



Hudson Gavin Martin is a boutique corporate and commercial law firm with a focus on Technology, Media and Intellectual Property – specialisms which have converged, and are now at the forefront of many major transactions and decisions in modern business.

Our grouping of practice specialties and industry expertise is unique in New Zealand. We don’t see the law as a separate discipline, but as one element of your wider business strategy.

We act for organisations of all sizes and stages (from large listed companies, to government bodies, to tech start-ups) on a full range of corporate and commercial transactions. We give industry-relevant, expert and cost-effective advice – and we love what we do.

Hudson Gavin Martin is pleased to collaborate with Rachel Paris and The Blockchain Boutique on this Guide, and as part of a strategic relationship to support mutual fintech clients.

Nigeria

Yinka Edu



Tolulope Osindero



Udo Udoma & Belo-Osagie

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Mobile payments, mobile lending and personal finance are the most prevalent fintech businesses in Nigeria.

Payments: The payments and remittances subsector remains the most active (and arguably) the most developed area of the fintech sector in Nigeria. Following the release of the Payments Systems Vision 2020 (“PSV 2020”) of the Central Bank of Nigeria in 2007, Nigeria has witnessed an increase in the number of mobile and electronic payments solutions. One of the recommendations of the PSV 2020 was to encourage electronic payment methods. The innovations in this subsector include the adoption of blockchain, Unstructured Supplementary Service Data (“USSD”) services for payments by operators and the use of artificial intelligence via chatbox. Licensed banks have also adopted the use of a USSD service for payments and transfer services. Competition among the various participants has resulted in new and simplified solutions for funds transfer and payments services.

Lending: We have seen an increase in mobile lending in Nigeria. For websites that offer mobile lending, the application and review process is completed online or on mobile phones and loans are mostly provided without collateral. These lenders target retail and SME loans and actively use machine learning and data science for credit analysis. These lenders are gaining market share from micro finance banks and other retail banking divisions of traditional banks.

Personal Finance: Several fintech businesses and some banks now offer personal savings solutions which are available on mobile phones. In order to be able to take deposits, you need a banking licence, and so fintech businesses are often teaming up with existing banks and other financial institutions to offer this service.

Blockchain: There are entities using blockchain technology for payments and other operations in Nigeria. There are also Bitcoin exchanges and other Bitcoin wallet providers in Nigeria.

Reward and donation crowdfunding are also prevalent in Nigeria and there are a few digital insurance providers.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

Further to a warning from the Central Bank of Nigeria, banks and other regulated financial institutions are restricted from trading or dealing in virtual currencies. The CBN has also issued a warning to the public that virtual currencies are not legal tender in Nigeria and that dealers or investors in virtual currencies have no legal protection in Nigeria.

Also, under Nigerian law, private companies are restricted from offering their securities to the public. The Securities and Exchange Commission (the “SEC”), based on its interpretation of the current regulations, does not permit crowdfunding as it is deemed to be an invitation to the public. The SEC has undertaken to consider regulatory amendments to permit equity crowdfunding in Nigeria.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

Equity, debt and mezzanine funding are available to new and growing businesses in Nigeria. Except where the articles of association of the company provide otherwise, companies are permitted to raise debt from individuals, banks, financial institutions and, subject to regulatory requirements, from the capital market. There are no special funding requirements for fintech businesses. Mostly, we have seen fintech companies raise equity rather than debt as investments have mainly come from venture capitalist and private equity firms.

In addition to this, there are funds set up by certain individuals and entities that are available to small- and medium-sized businesses and we have increasingly seen private equity funds that are focused on African fintech.

Also, the Government has provided funding options to “small businesses” at friendly rates to small businesses through the Bank of Industry.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

There are currently no special incentive schemes for investment in fintech specifically. We have discussed below some of the incentives

that are generally available in Nigeria that may be relevant to tech and fintech investment.

Deduction for Research & Development: Section 26 of the Companies Income Tax Act, Chapter C21 LFN 2004 (“CITA”) provides that companies and other organisations that engage in research and development activities for commercialisation are to enjoy 20% investment tax credit on their qualifying expenditure for that purpose. The CITA also provides that the profits reserved by a company for purposes of research and development are tax-deductible, provided such reserves do not exceed 10% of the total assessable profits for that company.

Pioneer Status: Companies classified as operating in a pioneer industry or engaged in the production of pioneer products are entitled to apply for pioneer status; and, when granted, such companies enjoy corporate tax relief/holidays for an initial term of three years starting from the date that the pioneer company commences business, which may be extended for a further period of one year, and a further one-year term subject to factors such as the relative importance of national development of the industry at the relevant time.

Incentives for Venture Capital Companies: Under the Venture Capital (Incentives) Act, Chapter V2 LFN 2004 (“VCA”), companies that invest in Venture Projects may be eligible for the following:

- accelerated capital allowance for equity investment by a Venture Company in a Venture Project for the first five years of their investment;
- reduction of withholding of tax on dividends declared by Venture Projects to Venture Companies for the first five years from 10% to 5%;
- export incentives such as export expansion grants if the Venture Project exports its products;
- exemption from payment of capital gains tax on gains realised by Venture Companies from a disposal of equity interest in the Venture Project; and
- exemption from company income tax for a period of three years, which may be extended for an additional final period of two years.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

In order for a company to IPO, it must be a public company and its constitutional documents must show that it is a public company. It must also have audited accounts for the preceding five years with a minimum of two years’ operating track record.

Currently, the Nigerian Stock Exchange is considering the changes that may need to be made to the Exchange’s rules to permit small businesses to raise funds on its platform.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

None that we are aware of.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

Lending: An entity that wishes to provide marketplace lending may do so by registering as a bank or Other Financial Institution (“OFI”)

pursuant to the Banks and Other Financial Institutions Act, Chapter B3 LFN 2004. Banks and OFIs are licensed and supervised by the CBN. In addition to this, a marketplace lender may be registered as a money lender in accordance with the Money Lenders Law of the state in Nigeria which it wishes to operate from. There are geographical limits on money lenders and restrictions on the interest rate they can charge.

Payments: The CBN regulates mobile payments pursuant to the CBN Guidelines on Mobile Money Services in Nigeria 2015 (the “Mobile Money Guidelines”), the CBN Guidelines on Operations of Electronic Payment Channels in Nigeria, the CBN Regulatory Framework for the use of Unstructured Supplementary Service Data in Nigeria, CBN Guidelines on International Money Transfer Services in Nigeria and other regulations. The Mobile Money Guidelines define a mobile money operator as an entity that provides “the infrastructure for the mobile payment systems for the use of participants that are signed-on to their scheme”. Mobile money operators must be licensed by the CBN on such terms and conditions as contained in “Appendix I” to the Guidelines. The activities of other participants in the payment space such as Switch Companies, Payments Terminal Service Providers and Card Scheme Providers are also regulated by the CBN.

Banking Services: In 2018, the CBN introduced the payment service bank category (“PSB”). A PSB is a bank that is authorised to, among other functions, accept deposits, provide payment and remittance services and also issue electronic wallets. A PSB should operate in rural and underbanked locations. PSBs are regulated under the CBN Guidelines for Licensing and Regulation of PSBs in Nigeria (2018).

In addition, the Nigerian Communications Commission (“NCC”) also regulates fintech businesses where the service offered involves mobile phones pursuant to the Licence Framework for Value Added Services (“VAS”) issued by the NCC. A VAS Provider is any person or organisation that engages in the provision of value added mobile/fixed services, including premium rated services, and such provider is required to obtain a licence from the NCC. The use of airtime for the repayment of loans to a mobile lender could constitute a premium rated service, the provision of which requires the approval of the NCC.

Asset Management: An entity that wishes to provide asset-management services or securities-trading services may be registered with the SEC.

There are no regulations for reward- and donation-based crowdfunding.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

Presently, there is no regulation specifically directed at cryptocurrencies or cryptoassets. Banks are mandated by the CBN to ensure that any existing customer that is a virtual currency exchanger should have effective AML and CFT controls.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

Financial regulators and policy makers are generally interested in promoting technology companies and solutions and this applies to fintech businesses. As the primary regulator of banks and OFIs, the

CBN plays a major role in determining the ease of entry or otherwise into the financial services space. As far as we are aware, the CBN has encouraged new entrants into the payments system through its promotion of the cashless policy. The CBN launched a regulatory sandbox for fintechs but we are not aware if the sandbox is now operational. Also, the SEC is also working towards a regulatory sandbox where start-ups and businesses can test innovation products, services, business models and delivery mechanisms relating to capital markets.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

There are no regulatory hurdles that are particular to a foreign fintech business other than the requirement that any foreign entity that wishes to carry on business in Nigeria is required to incorporate a Nigerian entity for it to do so. Once incorporated, the local entity becomes subject to the rules and regulations that apply to other local entities. In addition to local incorporation, the foreign entity may be required to obtain a licence from the CBN, SEC, NCC or a money lender's registry in order for it to provide the service in Nigeria.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

In 2019, the National Information Technology Development Agency (the "NITDA") released the NITDA Data Protection Regulations 2019, which replace the 2017 Regulations. The NITDA Regulations:

- place an obligation on anyone or any organisation involved in data processing or the control of data to develop security measures to protect such data;
- provides that data processing by a third party should be governed by a written contract between the third party and the Data Controller, i.e. any person or body that determines the purposes for and the manner in which personal data is processed or is to be processed;
- provide that a Data Subject has the right to object to the processing of his data at any time. Consequently, the Data Subject has the right to (a) object to the processing of his personal data by the Data Controller for marketing purposes, and (b) be expressly and manifestly offered the mechanism for objection to any form of data processing at no cost whatsoever to the Data Subject;
- require public and private organisations in Nigeria that control data of natural persons to make available to the public their respective data protection policies, which should conform with the provisions of the Regulations.

Fintech companies which collect and use customers' data must comply with the NITDA Regulations.

In addition, the following legislation and regulations have provisions on the use, collection or transmission of data in Nigeria which could apply to a fintech business:

- a. Cyber Crime (Prohibition, Prevention) Act 2015. Under this Act, a financial institution ("FI"), which may include a fintech company, is required to: verify the identity of customers carrying out electronic financial transactions; observe adequate "know-your-customer" processes; keep all traffic data and subscriber information as may be required by the NCC for a period of two years; and preserve, release or retain any traffic data or subscriber information upon the direction of a law enforcement agency.
- b. Under the CBN's Consumer Protection Framework, FIs regulated by the CBN must safeguard the privacy of customers' data, adopt data protection measures and implement staff training programmes to prevent the unauthorised disclosure of data.
- c. The Consumer Code of Practice Regulations 2007 issued by the NCC provides that all licensees must take reasonable steps to protect customer information against "improper or accidental disclosure" and ensure that such information is securely stored. It also guarantees that customer information is "not transferred to any party except as otherwise permitted or required by other applicable laws or regulations". Under the NCC's Consumer Bill of Rights, consumers have the right to personal privacy, to protection from unauthorised use of their records and personal information, and to reject intrusive communications and technology. A fintech business that is regulated by the NCC is enjoined to protect this right.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

The NITDA Regulations apply to entities that handle data of Nigerian citizens.

- a. Under the NITDA Regulations, the transfer of data must be carried out under the supervision of the Honourable Attorney General of the Federation ("AGF") or in very limited circumstances, such as where explicit consent of the Data Subject is obtained and the consequence of the absence of the AGF's decision has been made clear to the Data Subject.
- b. FIs are required to notify the CBN and the Nigerian Financial Intelligence Unit ("NFIU") if they intend to engage in information sharing and they must ensure that they have established and will maintain adequate procedures to protect the security and confidentiality of the information.
- c. The NCC's Registration of Telephone Subscribers Regulations 2011 provide that no subscriber information shall be transferred outside Nigeria without the prior written consent of the NCC.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

The penalties for a breach of the NITDA Regulations (in addition to any other criminal liability that such breach might give rise to) are:

- a. in the case of a Data Controller dealing with more than 10,000 Data Subjects, payment of the fine of 2% of its annual gross revenue of the preceding year or payment of the sum of N10,000,000.00 (ten million Naira), whichever is greater; or
- b. in the case of a Data Controller dealing with less than 10,000 Data Subjects, payment of the fine of 1% of its annual gross revenue of the preceding year or payment of the sum of N2,000,000.00 (two million Naira), whichever is greater.

There are no specific sanctions for the sharing of information without the approval of the CBN.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

Yes. The Cyber Crime (Prohibition, Prevention) Act 2015.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

An FI regulated by the CBN must comply with the CBN (Anti-money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations 2013. Under the Regulations, such FI must adopt a policy on AML and combat the financing of terrorism and must also have policies and procedures to address any risks for customers in relation to AML and the financing of terrorism.

In addition, the following financial crime laws may apply to fintech businesses as they apply to financial institutions generally:

- Money Laundering (Prohibition) Act 2011 (as amended).
- Corrupt Practices and Other Related Offences Act, Chapter C31 LFN 2004.
- Economic and Financial Crimes Commission (Establishment, etc. Act), Chapter E1 LFN 2004.
- Terrorism (Prevention) Act, No. 10 of 2011.
- CBN Anti-money Laundering/Combating the Financing of Terrorism (AML/CFT) Risk-based Supervision Framework 2011.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

In addition to the above, agreements for the transfer of technology between a foreigner and a fintech business in Nigeria should be registered with the National Office for Technology Acquisition and Promotion.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

The principal law governing the employment of persons in Nigeria is the Labour Act, Chapter L1 LFN 2004 (the “Labour Act”), but this law only applies to junior and non-professional staff.

The terms of the employment of senior staff are governed primarily by the contract of employment and principles of Nigerian case law, as well as any collective agreements.

In general, an employer can terminate the employment of an employee for good, bad, or no reason at all, provided the required notice is given. Notwithstanding this, the National Industrial Court has begun to apply international labour law and principles and had, in one of its recent decisions, ordered that an employee, whose contract was terminated, be reinstated; and in another case, extended the amount of damages that can be awarded in the case of wrongful termination.

In terminating contracts, employers must comply with the terms of the employment contracts, such as giving the required notice or

salary *in lieu*. An employer must also adhere to the terms of other applicable employment documentation and ensure that the employee has received all accrued contractual entitlements to avoid actions for wrongful termination by employees.

In addition, an entity in Nigeria that wishes to employ an expatriate must apply to the Federal Minister of Interior for approval to do so.

5.2 What, if any, mandatory employment benefits must be provided to staff?

- a. The Labour Act contains specific provisions on annual leave, overtime, sick leave and maternity leave entitlements. With respect to senior staff, these matters are primarily determined contractually.
- b. There is no obligation on an employer or an employee to contribute to the health insurance scheme under the National Health Insurance Scheme Act, Chapter N42 LFN 2004. An employer may, however, be in breach of the Act if, after electing to contribute to the insurance scheme, it fails or refuses to remit its contribution.
- c. The Pension Reform Act 2014 requires employers to contribute to the pension fund of their employees. Employers contribute a sum equal to 10% of each employee’s monthly salary as its contribution to the contributory pension scheme, and remit this contribution, together with each employee’s contribution which is to be deducted at source (8% of the employee’s monthly salary), to the employee’s retirement savings account. Employers are also required to obtain life insurance cover for all their employees for a value of no less than three times the annual emoluments of all the employees.
- d. Employees are entitled to receive compensation if injured at work under the Employee’s Compensation Act 2010. Every employer is required to make a minimum monthly contribution of 1% of its total monthly payroll into the Employee’s Compensation Fund.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

There are no special routes for fintech businesses to bring employees from outside Nigeria. The same rules apply to all local entities. An entity in Nigeria that wishes to employ an expatriate must apply to the Federal Minister of Interior for an expatriate quota position approval for the relevant number of expatriate personnel it intends to employ. The expatriate quota approval entitles the entity to employ and bring in any employee for the positions approved. The number of expatriate quota positions is limited and the company must justify the number applied for and explain why the posts cannot be filled by Nigerians. Once the approval is granted, the employee must obtain a Combined Expatriate Residence Permit and Aliens Card, which is the authorisation that enables an expatriate to reside and to work in Nigeria.

The exception to the requirements above is where a temporary work permit (“TWP”) is obtained. A TWP is a permit (which is valid for three months and may be renewed for a subsequent period of three months) which is granted to an expatriate invited by corporate bodies in Nigeria to provide specialised skilled services, such as after sales installation, maintenance and repairs of machines and equipment.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Innovations and inventions are generally protected by Nigerian intellectual property (“IP”) laws. The Copyright Act, Chapter C28 LFN 2004 (the “Copyright Act”) protects literary works (including computer programs), musical works, artistic works, cinematographs and broadcasts. The Patents and Designs Act, Chapter P2 LFN 2004 (the “Patents and Designs Act”) protects industrial designs as well as inventions which are new or an improvement upon an existing patented invention, result from inventive activity and are capable of industrial application. The Trade Marks Act, Chapter T13 LFN 2004 (the “Trade Marks Act”) protects owners of registered trade marks. Owners of unregistered trade marks are not protected by the Trade Marks Act but are entitled to seek relief under the common law principles applicable in Nigeria. A person whose IP rights are infringed is entitled to institute legal proceedings in the requisite Nigerian court and obtain reliefs (which may include damages, order for account, injunctions and delivery-up of the infringing articles, etc.) against the infringing party. Infringement of copyright also constitutes a crime punishable with a term of imprisonment under the Copyright Act.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

In Nigeria, recognised IP rights include trade marks, patents, industrial designs and copyright. Ownership of any of these IP rights confers the right to exclusively use, exploit and appropriate the IP, subject to the duration of time prescribed by law. Trade marks expire after seven years from the date of the application and are renewable for successive periods of 14 years; patents expire after 20 years and are not renewable; industrial designs expire after five years from the date of the application and may be renewed for two further consecutive periods of five years each, and the duration of copyright depends on the nature of the copyright that is created and ranges between 50–70 years.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

Trade marks, patents and industrial designs must be registered in accordance with the procedure prescribed in the relevant legislation in order to enjoy protection under Nigerian law. Copyright subsists

automatically in a work from the moment the work is created. Registration is, therefore, not a prerequisite to copyright protection under Nigerian law. The Nigerian Copyright Commission (the “Copyright Commission”), however, administers and operates a notification/depository scheme. Under this scheme, creators of copyright works or persons who have acquired any copyright in respect of eligible works may give notice of/register their copyright with the Copyright Commission. The purpose of this scheme is to provide notification to the Copyright Commission of the creation and/or existence of a work and also serve as evidence of authorship/ownership in legal proceedings in which there are competing interests.

Nigeria is a party to several treaties such as the Patent Cooperation Treaty 1970 (the “PCT”), the Agreement on Trade-Related Aspects of Intellectual Property Rights 1995, the Paris Convention for the Protection of Industrial Property 1979, etc.; however, most of these treaties are currently not being enforced in Nigeria because the Nigerian Constitution requires treaties to be domesticated as local law before they can be enforced, and the treaties have not yet been domesticated. We should, however, mention that although the PCT is yet to be domesticated, the Nigerian patents registry continues to accept and accord foreign priority to PCT national phase applications. The patent rights granted subsequent to the applications are protected and enforceable under Nigerian law. The Berne Convention for the Protection of Literary and Artistic Works 1886 has been domesticated; therefore, works originating from other contracting states are protected under the Nigerian copyright laws to the same extent as Nigerian nationals are.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

IP rights are tradeable just like any other property. They may, therefore, be assigned, transferred or licensed for monetary consideration. With respect to copyright, the moral right of the author (i.e. the right of the author to claim authorship of his work, in particular that his authorship be indicated in connection with the work) is perpetual, inalienable and imprescriptible. Trade marks, patents and designs do not have a similar requirement; hence, the owners of these rights are allowed to trade their rights in whatever manner they may choose to. Other than restrictions regarding moral rights (in relation to copyright) and the prohibition of contracts that may be illegal or contrary to public policy, there are no limitations on the exploitation of IPs and they are governed by contracts. Where any IP right is assigned, transferred or licensed, the parties are required to comply with the provisions of the respective IP laws regarding registration (or notification in the case of copyright) and payment of the prescribed fee.

**Yinka Edu**

Udo Udoma & Belo-Osagie
St. Nicholas House (12th floor)
Catholic Mission Street
Lagos
Nigeria

Tel: +234 1 4622 30710
Email: yinka.edu@uubo.org
URL: www.uubo.org

Yinka Edu is a Partner in the firm's Banking and Finance team and heads the firm's capital markets and Fintech teams. She has been involved in a diverse range of financial and capital markets transactions including the establishment of debt issuance programmes (by sovereign, sub-sovereign, supranational and corporate issuers), a global depository receipt programme, derivatives, M&A, equity issuances and the establishment of collective investment schemes.

Yinka is ranked in ranked as a Tier 1 Lawyer in the *Chambers Global Fintech Guide 2018*. She is also ranked in *Chambers Global* for her expertise in banking & finance and corporate/commercial practice and is commended for her banking and finance and capital markets work in the current edition of *Who's Who Legal*. Yinka is a thought leader in her field and publishes articles on securities finance, fintech and M&A. She has been described as a "hard core professional with a deep knowledge of legal issues in commercial transactions".

Yinka is at the forefront of the firm's activity in the fintech space and has advised clients in relation to the regulatory regime for fintech businesses in Nigeria.

**Tolulope Osindero**

Udo Udoma & Belo-Osagie
St. Nicholas House (12th floor)
Catholic Mission Street
Lagos
Nigeria

Tel: +234 1 4622 30710
Email: tolulope.osindero@uubo.org
URL: www.uubo.org

Tolulope Osindero is a Senior Associate in the Banking and Finance team with a focus on fintech, syndicated lending, project finance, structured finance and corporate advisory. She routinely advises local and international clients on a day to day basis on issues concerning the creation of security and restructuring of debts. She advises on the formation, licensing and operational requirements for fintech entities in Nigeria, investment in fintech start-ups, financial products with technological features, crowdfunding projects and market place lending in Nigeria. She has contributed to publications on trends in fintech in Nigeria and is recognised as an "Associate to Watch" in the *Chambers Global Fintech Guide 2018*.



Udo Udoma & Belo-Osagie is a corporate and commercial full-service law firm with offices in Nigeria's major business centres. UUBO has been described in international rankings as one of Nigeria's "Magic Triangle" law firms. We aim to structure timely, practical and creative legal solutions founded on a philosophy of providing bespoke legal advice that is accessible, commercially-oriented and consistently sound in principle. The firm maintains a policy of actively seeking to develop fresh skills and acquire new expertise in our niche areas, thus enabling us to respond quickly to the rapid changes that occur in the world of business and finance. Our "hands-on" and collaborative approach across the diverse sectors in which our clients operate enables us to achieve our objective of finding solutions and providing tailored advice that is accessible, commercially-oriented and consistently sound on principle. The firm embraces diversity, which is seen in the backgrounds, range of experience and "hands-on" collaborative approach of our team. This has contributed to recurring high rankings underscored by what is currently one of the highest ratios of internationally recognised Partners per firm in the Nigerian market.

Norway

Markus Nilssen



Vanessa Kalvenes



BAHR

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

- Vipps AS (owned by a consortium of Norwegian banks, with DNB Bank ASA as the majority owner) offers mobile application payment services. Vipps, being the largest fintech business in Norway with three million users, has been offering swift and simple solutions for carrying out P2P transactions in Norway since 2015. Since beginning in 2015, its business has evolved rapidly, with an important milestone being a merger in 2018 with the Nordics' two largest market players within card payment services and digital identify solutions, BankAxept and BankID, respectively. The main purpose of the merger was to make the businesses better equipped for facing the anticipated fierce competition from international suppliers of technology and payment services, which are expected to enter the Norwegian market over the next few years. The merged company is working on expanding its business within invoice payment services and e-commerce, the main goal being to simplify invoice settlement and online payments through joint innovation and technology.
- Several crowdfunding platforms have been established in recent years. Examples of crowdfunding platforms for businesses, especially within the SME segment, include Monner, Funding Partner and Kameo. Perx, which is a crowdfunding platform for consumer loans, is another example. There are also a number of reward-based crowdfunding platforms in the Norwegian market, such as Spleis, bidra.no and funde.no, to mention a few.
- Quantfolio is a Bergen-based Fintech company delivering 'AI-in-a-box' components for banks and wealth managers with a digital presence. The company is partially owned by Sbanken (formerly Skandiabanken).
- Cloud insurance is a Software-as-a-Service (SaaS) for insurance companies, agents and brokers, and is, according to the company itself, already in use in over 20 countries across five continents. The company's aim is to provide the insurance industry with a leaner, customer-focused and fast-moving way of doing insurance business.
- Myshare.live connects entrepreneurs with crowd funders by broadcasting live pitch sessions on the web and making them available to the broader public in real time. This allows the audience to invest exclusively during the sessions.

- Spiff and its competitor Spare (owned by DNB Bank ASA) are mobile applications which aim to make it social, easy and fun to save and invest for everyone without regard to the users' income. Both Spiff and Spare strive to be easy to understand and put the customer directly in charge of his/her savings using a smartphone.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

Not in particular. However, the Norwegian regulatory environment presents a challenge to several fintech businesses due to strict licensing requirements for the conduct of 'financing activities'. To this end, an initiative has been made to set up a 'regulatory sandbox' in Norway, which purpose is to enable fintech start-ups to test their innovative products, technology and services on a limited number of customers under close supervision by the Norwegian Financial Supervisory Authority. Prevailing licensing requirements will apply accordingly within the sandbox, but the regulator may ease certain requirements based on a principle of proportionality if the relevant legal framework is open to exemptions. Trading in cryptocurrency is subject to AML requirements; see question 4.5 for further information.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

Albeit small on a global scale, the Norwegian start-up scene has experienced a rapid growth in recent years. This is most likely a result of both the continuing global interest in innovation and expectations of growth in the tech industry, as well as the dramatic drop in crude oil prices since the summer of 2014, which cost thousands of jobs in the oil industry. The redundancies created by the oil crisis pushed several well-qualified members of the workforce into new ventures, while investors deterred by losses in the oil sector looked elsewhere for suitable investment opportunities.

Traditionally, Norwegian start-ups have funded themselves through a combination of private capital and bank loans. Norway has a relatively small base of significant private investors, and the Norwegian venture capital scene is still in its early days. The 'angel investor' base has grown in recent years, and as a result, start-up equity funding has become more accessible. There are several ongoing initiatives to further develop the Norwegian angel investor

scene, such as the 'Angel Challenge' by Startup Norway where investors can participate with as little as NOK 50,000 each.

However, banks and governmental agencies are still the most important sources of funding for emerging companies in Norway, and a number of new initiatives have been taken in recent years. By way of example, Norway's largest bank, DNB Bank, has launched 'DNB NXT Accelerator' together with StartupLab in order to promote fintech innovation, and the Sparebank 1 Group has launched a crowdfunding platform called 'Spleis' which is intended to facilitate easier funding for projects. On the public side, Innovation Norway plays an important role as the Norwegian Government's primary vehicle for supporting innovation and development of Norwegian enterprises and industry. They provide support to start-ups and growth companies in the form of funding, advisory services, networking opportunities and other resources. Further, the government-funded venture capital fund Investinor is one of Norway's largest venture investors with more than NOK 4.2 billion under management and 76 companies currently in its portfolio. In April 2017, the fund facilitated the first listing of one of its portfolio companies when BerGenBio ASA, a biotech company, was listed on the Oslo Stock Exchange. Following this, the fund has facilitated two further listings of its portfolio companies, namely the listings of the pharmaceutical company Calliditas Therapeutics AB on Nasdaq Stockholm in June 2018 and the tech-company poLight ASA on the Oslo Stock Exchange in October 2018.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

Norway has recently enacted two incentive schemes to attract more investments to the start-up sector. The first scheme allows investors to claim a deduction for equity investments in start-up companies against their taxable income. The other scheme allows employees of start-ups who receive share options as part of their remuneration to defer taxation of such options so that they are not taxed on their gains when the options are exercised, but rather at the later point in time when the shares received from the option are sold. Unfortunately, both of these incentive schemes are quite narrow in scope, and have been widely criticised. In a recent policy document, the government has signalled that it intends to strengthen the incentive scheme for employee's share options to make it more attractive.

Norway currently has a wealth tax rate of 0.85%. The wealth tax only applies to individual taxpayers who are tax resident in Norway. For shares, only 75% of the market value shall be calculated for wealth tax purposes, which would also apply for share investments in venture capital.

Norwegian corporate investors (i.e. limited liability companies and similar entities) in Norwegian businesses organised as limited liability companies and similar entities, including tech/fintech businesses, would be exempt from taxation on any gain from such investments under the participation method. Three per cent of the dividend would be taxed as ordinary income with a rate of 22% (25% for financial enterprises), giving an effective tax rate on dividends of 0.66% (0.75% for financial companies). If the investing company owns more than 90% of the share capital and the voting rights, no tax will be levied on the dividends.

Foreign investors are not subject to Norwegian taxation on gains from investments in Norway, unless such investments are made in connection with business activities carried out or managed from Norway. Dividends to foreign investors are subject to a Norwegian

withholding tax at a rate of 25%, unless the recipient qualifies for a reduced rate according to an applicable tax treaty.

Foreign corporate investors (i.e. limited liability companies and similar entities), which are genuinely established and carry out genuine economic activities within the EEA, are not subject to Norwegian withholding tax under the participation method.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

Companies seeking a listing of its shares on the Oslo Stock Exchange must satisfy the stock exchange's criteria for listing, the most important of which are as follows:

- the company's shares must be assumed to be of public interest, be freely transferable and likely be subject to regular trading;
- at the time of listing, the market value of each share must be at least NOK 10 and the total market value of the shares to be listed must be no less than NOK 300 million;
- at the time of listing, the company must have at least 500 individual shareholders each holding shares worth at least NOK 10,000, and a minimum of 25% of the company's shares must be held by the general public;
- the company must demonstrate that it has a satisfactory equity capital and sufficient liquidity to continue its operations for at least 12 months after listing;
- the company must have at least three years' operating history, and must have produced annual, audited accounts for at least three years prior to the application for listing; and
- the company's board of directors and management must meet applicable suitability requirements. At least two of the directors must be independent of the company's management, larger shareholders and material business contacts.

If some of these criteria are not met, the company seeking an IPO may decide to apply for a listing at Oslo Axess instead. Oslo Axess is a marketplace for small cap companies and has less strict requirements for listing. It is operated by the Oslo Stock Exchange. Finally, companies who do not qualify for a listing on either the Oslo Stock Exchange or Oslo Axess may apply to become listed on Merkur Market, an MTF operated by the Oslo Stock Exchange.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

There have not been any notable IPOs in the Norwegian fintech scene to date. However, there have been several acquisitions and consolidations of various scales, the most notable of which are the co-investment by more than 100 local Norwegian banks in DNB Bank's mobile payment platform Vipps, which consolidated Vipps' position in the Norwegian payments market and led to the exit of Mobilepay from Norway in late 2017, and the merger of Vipps, BankAxept and BankID in 2018.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

'Fintech' is not a regulated activity in itself. However, Norwegian

legislation imposes a licensing requirement on, among other things, the following activities and services:

- Financing activities.
- Insurance business.
- Deposit-taking.
- Payment services and e-money.
- FX business (spot trading in foreign exchange).
- Investment services and activities.

The licensing requirements for the above-mentioned services may present a challenge for fintech start-ups intending to market their products and services to customers in Norway. By way of example, the definition of a licensable ‘financing activity’ includes ‘the intermediation of credit and guarantees, or other participation in the financing of business other than one’s own’. Clearly, this is a rather wide definition which can capture a wide array of fintech-related activities. As further discussed in question 3.3 below, it has been decided to establish a ‘regulatory sandbox’ in Norway by the end of 2019. The purpose of the sandbox is partially to boost fintech innovation notwithstanding the strict regulatory environment in Norway, as well as serve as a useful tool for the Norwegian regulator to gain insight into such businesses and the challenges they face.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

Providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers are subject to AML requirements, including registration and supervision by the Norwegian Financial Supervisory Authority. Please refer to question 4.5 for further details.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

In a letter dated 12 November 2018, the Norwegian Ministry of Finance mandated the Norwegian Financial Supervisory Authority to establish a regulatory sandbox for the fintech industry before the end of 2019. The purpose of the sandbox is to give new fintech businesses, who often have limited knowledge of the vast regulatory framework and supervision to which the financial industry is subject, a better understanding of the requirements which apply to their business. To this end, the sandbox is meant to provide for testing under close supervision by the Norwegian Financial Supervisory Authority and more proportional regulatory requirements. The expectation is that a regulatory sandbox will better the prospects of new innovative services entering the market scene, as well as give the supervisory authorities a better understanding of the challenges connected with new technology and business models.

Businesses must apply to the Norwegian Financial Supervisory Authority and must meet certain eligibility criteria in order to qualify for participation in the sandbox. A project will be eligible for testing in the sandbox if it is subject to financial regulation, is genuinely innovative and expected to be beneficial to consumers or the financial system as a whole. Furthermore, the sandbox will only be open to projects which are dependent on testing in order to realise their business goals. Applicable licensing requirements for the business

will apply accordingly in the sandbox, but the regulator may ease certain requirements based on a principle of proportionality to the extent that the prevailing regulatory framework allows exemptions.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

Other than the licensing requirements and limited access to participate in the regulatory sandbox, both mentioned above, there are no particular regulatory hurdles applicable to fintech businesses attempting to access new customers in Norway.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

The collection, use and transmission of personal data is regulated by the Norwegian Personal Data Act (the Act), implementing the General Data Protection Regulation (EU) 2016/679 (GDPR). The Act came into effect on 20 July 2018 and contains certain national specific rules supplementing the GDPR.

The old Personal Data Act and Regulation stated that financial institutions must have a personal data licence in order to handle their customers’ personal data. Under the Act, this is no longer a requirement.

The new Act introduces a new obligation for companies to perform a data protection impact assessment (DPIA) before carrying out processing activities that is likely to result in high risk to individuals’ ‘rights and freedoms’. The reference to the ‘rights and freedoms’ of the data subjects primarily regards the rights to data protection, privacy and other fundamental rights. Use of new technology can trigger the need to carry out a DPIA and thus fintech companies can be subject to this obligation for certain processing activities.

A fintech company obligated to perform a DPIA must also consult the Norwegian Data Protection Authority prior to processing where a DPIA indicates that the processing would result in a high risk in the absence of measures taken to mitigate the risk.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

The Act applies to undertakings and physical persons established in Norway, where personal data is processed in the context of the activities of such establishment. This means that neither the nationality or place of residence of the data subject nor the physical location of the personal data are decisive.

The Act also applies to those not established in the EEA when they process personal data about data subjects in Norway in connection with the offering of goods or services, or monitoring their behaviour within Norway.

The Act allows for international transfer of data within the EEA area and also to the US, based on the Privacy Shield framework.

Furthermore, the international transfer of personal data may be transferred to countries approved by the European Commission by using the EU's standard contractual clauses, or on the basis of Binding Corporate Rules. Besides this, international transfer of data to third countries may take place by applying to the Norwegian Data Protection Authority. The applicant must, among other things, guarantee that the data will be adequately protected.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

The Norwegian Data Protection Authority may issue an administrative fine for violation of the provisions set out in the Act. Administrative fines are, however, not applicable automatically, but imposed on a case by case basis. Non-compliance with the provisions of the Act may be subject to administrative fines of up to EUR 20 million, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

The Data Protection Authority may also take a range of additional actions in the event of infringements of the Act, such as issue warnings or reprimands, order that the processing of personal data in violation of the provisions of the Act shall cease, or they may impose conditions which must be met in order for the processing to be compliant with the Act. Administrative fines can be imposed in addition to or instead of the said measures. The Data Protection Authority may impose a daily fine for each day of non-compliance with the order (subject to applicable grace periods).

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

There is currently a regulation on the use of information and communication technology (Nw: *IKT-forskriften*) which applies to most of the financial services industry, including banks and systems for payment services. The regulation gives each business falling under its scope certain duties with respect to planning and organisation, risk analysis, security, etc.

The directive on security of network and information systems (EU) 2016/1148 (the NIS Directive) is expected to be implemented in the EEA Agreement and consequently also in Norwegian law in the future. The timing of such implementation is currently unclear.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

The Norwegian Anti-Money Laundering Act and Regulations implement the 4th AML Directive.

Entities conducting licensable services (*cf.* question 3.1 above) are subject to the Anti-Money Laundering Act and Regulations, and are obligated to report any suspicious transactions to the Norwegian Economic Crimes Unit.

Such companies are obligated to apply customer due diligence measures (KYC) upon, among other things, establishment of customer relationships and before completing transactions with a value of NOK 100,000; or more for non-established customers, KYC verification is based on, among other things, a valid proof of identity and verification of beneficial owners.

A person who wilfully or with gross negligence breaches obligations set out in the AML Act may be subject to a fine or, in severe circumstances, imprisonment of up to one year.

As of 15 October 2018, providers engaged in exchange service between virtual currencies and fiat currencies and custodian wallets providers are subject to AML requirements, including registration and supervision by the Norwegian Financial Supervisory Authority.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

See question 3.1 above.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

Hiring:

There are few rules regarding the hiring of employees in Norway, and the hiring process is, to a large extent, subject to the employer's discretion. However, there are no particularly onerous requirements or restrictions that are frequently encountered by businesses regarding hiring, so that:

- The provisions on non-discrimination apply in the hiring process. This implies that discrimination on the basis of political view, union membership, age, part time/temporary employment, gender, ethnicity, religion or philosophical belief, disability, sexual orientation, sexual identity or gender expression, is prohibited.
- An employee who has been made redundant, or is employed part-time, has a preferential right to a new appointment/extended post in the company.

Dismissal for cause:

Norwegian law does not recognise at-will employment, and termination of an employment agreement must be for a 'valid cause' based on particular circumstances connected with the business or the employee in question.

The minimum notice period for dismissal is one month, unless otherwise stated in a collective agreement. The minimum notice period is prolonged for employees who have reached certain age levels and/or have been employed in the company for a certain period of time. In Norway, the parties usually agree on a mutual notice period of two or three months.

During the notice period, the employee is, as a general rule, entitled and obliged to remain in his/her position, perform work and receive an ordinary salary and other benefits pursuant to his/her employment agreement.

Upon a formal termination of the employee's employment, the employee has an unconditional right to dispute a termination, demand negotiations and file legal proceedings. Until a dispute has finally been resolved, the employee is, as a general rule, entitled to remain in his or her position and receive salary and other benefits.

Dismissal without notice:

An employer may dismiss an employee with immediate effect (i.e. without notice) if the employee is guilty of a gross breach of duty or other serious breach of the employment agreement.

Dismissal without notice is considered a severe action due to the fact that the employee's employment is terminated immediately, and that he/she is not entitled to salary or other benefits after the termination date.

In the event of a dispute concerning the lawfulness of a dismissal without notice, the employee is not entitled to remain in his/her position while the case is pending unless the court decides otherwise.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Salary:

The salary is agreed between the employer and the employee. Employees covered by collective bargaining agreements will be paid a salary pursuant to the collective agreement.

Overtime compensation:

Employees in Norway are entitled to overtime compensation of at least 40% in addition to their ordinary hourly salary for hours worked outside of the statutory normal working hours. A different level of overtime compensation may be stipulated in a collective bargaining agreement. However, employees in leading positions or employees in particularly independent positions are not subject to the rules on overtime payment.

Holiday and holiday pay:

Employees in Norway are entitled to an annual holiday of four weeks and one day. However, Norwegian companies often grant the employees an annual holiday of five weeks, as do most collective agreements.

Holiday payment from an employer is calculated on the basis of salary paid in the preceding calendar year. The holiday pay shall amount to 10.2% of the salary if the employee is entitled to four weeks and one day, and 12% if the employee is entitled to five weeks' holiday. Normally, the employer pays holiday pay in June instead of the ordinary salary, regardless of when the employee takes holiday.

In addition, the employee will be entitled to time off on public holidays.

Pension:

Norwegian companies have a legal obligation to establish pension plans for their employees. Thus, all employees are entitled to an occupational retirement pension, i.e. a pension financed primarily by the employer (with the possibility for employee's contributions at a given level). This scheme is additional to the retirement benefit/pension that the employee receives from the Norwegian National Insurance Scheme.

Occupational injury insurance:

All employers are obliged to take out occupational injury insurance which shall cover occupational injury and occupational disease for the employee.

Daily cash benefits in the case of illness:

The employer is obliged to pay sick pay during an employee's illness for a period of 16 days, after which the employee is entitled to sickness benefits from the National Insurance Scheme for a maximum period of one year.

Parental leave:

In connection with childbirth and care for the child during the first year of the child's life, the parents are entitled to a total of one year's leave of absence. The period may, however, be prolonged to 59 weeks if the parents choose 80% coverage from the Norwegian National Insurance Scheme.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

Citizens from countries outside the EEA and Switzerland wishing to work in a company in Norway have to apply for a residence permit. Citizens from the EEA and Switzerland can work in Norway without having to apply for such permit, but must register with the police within three months after arriving in Norway. Citizens from the Nordic countries do not need to register with the police.

All foreign citizens moving to Norway must have a tax card with a personal identification number to work in Norway, and must provide the postal address to the Norwegian authorities. If the employee intends to stay in Norway for a period of more than six months, the employee must report to the National Registry within eight days of arrival.

There are no special rules or routes available to individuals who work for fintech businesses.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Norwegian IP law is based on International and EU Intellectual property regulations. IP regulations within the EEA area are essentially harmonised.

Patents:

Inventions which may be used for industrial purposes may be patented pursuant to the Norwegian Patent Act by filing an application to the Norwegian Industrial Property Office (NIPO). An invention may also be protected for industrial use in Norway by applying to the European Patent Office for a patent registration (see question 6.3 below).

The invention must represent something new, meaning that the invention must not have been made known to others before the day on which the patent application was filed. Furthermore, the invention must contain a so-called 'inventive step', which means that the invention must differ in a significant way from the existing technology in the area. As a general rule, computer programs may not be patented. However, a patent for computer programs may in some cases be granted if the program has 'technical character' besides representing something new and containing the necessary inventive step.

If a patent is granted and registered, the patent is protected for a maximum of 20 years from the day the patent application was filed.

Design:

A creator of a design, for instance a web page or a user interface, may file an application to NIPO for design registration pursuant to the Norwegian Design Act. A design registration may only be granted for a design which represents a new appearance. A design should be considered representing a new appearance if it does not appear identical to the informed user (as defined by the CJEU) compared to other designs at the day of application. Also, if a creator of a design for instance applies for an international design registration through the Hague System, and subsequently files an

application to NIPO within six months after, the application shall gain priority from the day the international application was filed (grace period). Furthermore, the design must have individual character. If a design registration is granted, the design is protected for a five-year period (and may be prolonged for a maximum period of 25 years).

Trademarks:

Trademarks, meaning figurative marks, logos, word marks etc., may be registered by applying to NIPO pursuant to the Norwegian Trademark Act. A trademark registration may only be granted if it can be used to differentiate a product from others, meaning it must have the ability to indicate the product's commercial origin (thus being distinctive from other marks). If a trademark is granted, the trademark is protected for a period of 10 years from the day of application and may be successively prolonged for new 10-year periods.

Copyright:

The Norwegian Copyright Act may also provide legal protection for creators of intellectual or creative works, for instance computer programs (source code), photos, lectures and scientific works, provided that they are a product of an individual and creative process. The copyright cannot be registered, but will begin to exist from the moment the work is created.

Legal protection of a copyright pursuant to the Copyright Act is limited to 70 years after the creator's year of death.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

The holder of a trademark, patent or design is usually the legal or physical person named as the designated rights holder in the NIPO's database.

Furthermore, a company may acquire IP rights arising in case of an employee's execution of work for the company. Securing such IP rights is usually regulated in the employer's contract with the employee. For inventions, the employee has the right to fair compensation pursuant to the Norwegian Employee Invention Act. Meanwhile, unless otherwise agreed upon, an employer is secured copyright to computer programs developed by the employee pursuant to the Norwegian Copyright Act. For other copyrights, employers may only secure copyright as far as to the extent necessary.

Ownership to copyrights is harder to prove in case of an infringement, since the copyright cannot be registered by NIPO. Unless otherwise agreed upon, a physical manifestation of the creator's work defines his/her ownership and right to use it.

Following the adoption of Norway's new Copyright Act in 2018, creators and performing artists have a statutory right (except in consumer relations) to a 'reasonable compensation' for rights to original works, from the person the rights are assigned to.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

As a starting point, local registration in Norway is necessary to protect the commercial exploitation of trademarks, designs and patents in Norway. Trademark protection in accordance with the Norwegian Trademark Act may also be granted without registration by way of consistent and comprehensive use over a period of time.

Furthermore, to obtain protection in Norway for holders of a European patent registration, the holder of the patent registration must translate the patent claims to Norwegian and subsequently send the claims to NIPO. Trademark holders outside Norway may also secure trademark protection in Norway by applying through the Madrid Protocol system administered by WIPO. Design holders outside Norway may secure design protection in Norway by submitting an application to WIPO through the Hague system.

Copyright holders may protect and enforce their copyrights without consideration to local or national rights pursuant to the Berne Convention. A state which has ratified the Convention is obligated to provide copyright holders with the same copyright protection without consideration of their country of origin.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

Registration of patents, trademarks or designs gives the right-holder an exclusive right to exploit the rights for industrial and commercial purposes. Furthermore, the holders of such rights may enter into licence agreements with third parties granting an exclusive or non-exclusive right to exploit the IP right.

Copyright holders may also enter into similar licence agreements. Any such licence agreement will be subject to the Norwegian Copyright Act's mandatory rules on, among other things, consumers' rights to private copying, the right to quote from a copyright-protected work, and the use of a copyright-protected work for educational purposes.

Some copyright holders, such as musicians and authors, submit their rights to a collection society, which manages the copyright holders' interests and enters into licence agreements on behalf of the copyright holder.

Acknowledgment

The authors would like to thank their colleague Thomas Kristoffer Granrud for his assistance in the preparation of this chapter. Thomas is an associate with BAHR. He has worked with BAHR's finance group since 2017. He holds a Master of Laws from the University of Oslo.

**Markus Nilssen**

BAHR
Tjuvholmen allé 16
PO Box 1524 Vika
NO-0117 Oslo
Norway

Tel: +47 2101 6604
Email: marni@bahr.no
URL: www.bahr.no/en

Markus Nilssen is a partner with BAHR. He has worked in BAHR's finance group since 2008. He holds an LL.M. in business law from the UCLA School of Law.

**Vanessa Kalvenes**

BAHR
Tjuvholmen allé 16
PO Box 1524 Vika
NO-0117 Oslo
Norway

Tel: +47 2201 6889
Email: vakal@bahr.no
URL: www.bahr.no/en

Vanessa Kalvenes is a senior associate with BAHR. She has worked with BAHR's finance group since 2015. She holds a Master of Laws from the University of Oslo.

BAHR

As one of the most international law firms in Norway, BAHR has successfully advised leading Norwegian and global clients since 1966. Today, BAHR's practice covers all the key commercial disciplines, with a particular focus on domestic and international transactions, commercial law advice and dispute resolutions.

In order to enhance our understanding of business sectors and commercial relationships, and assist in sharing expertise and information, BAHR's lawyers are arranged into industry groups, as well as practice groups. The groups contain expertise from across the firm, spanning the full spectrum of client needs from transactional assistance to tax, commercial advice to finance, and IP to dispute resolution.

We are not a member of any international alliance, but benefit from a well-developed, non-exclusive network with leading law firms in many jurisdictions in Europe, the US and the Middle and Far-East.

Peru

Ljubica Vodanovic



Alejandra Huachaca



Vodanovic Legal

1 The Fintech Landscape

- 1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).**

Nowadays, there are more than 75 fintech businesses operating in Peru. The types of fintech businesses are the following:

- Payments and transfers: sending money, either locally or internationally, to make payments or transfers between accounts. It includes payment facilitators (gateways).
- Crowdfunding: money loans in small amounts raised by the general public for the general public.
- Currency exchange: exchange of one currency for another.
- Business finance management: digital platforms for the management of resources, assets and liabilities of a legal entity (invoice management, accounting management, asset management, etc.).
- Personal finance management: digital platforms and/or digital financial advice that help individuals make better financial decisions and manage their money (income and expenditure of money, reduce operating expenses, better interest rates or low commissions, etc.).
- Loans: financing granted by legal entities with their own resources, using digital platforms for any or all stages.
- Marketplaces for loans and/or savings: digital platforms that connect individuals or legal entities interested in obtaining a loan or opening a savings deposit with financial companies that provide such services.
- Cryptocurrency platforms: digital platforms that allow the purchase, sale, transfer and, in general, operations with cryptocurrencies.
- Insurtech: insurance marketing and contracting using technology.
- Credit score: evaluation and assignment of credit score to individuals.
- Savings: digital platforms that facilitate an individual's savings through a system of collaboration, so that the money is distributed or used according to defined goals or objectives.
- Investments: digital platforms and/or digital financial advice that help investors make a better investment decision and/or manage investment portfolios.

Two notable fintech innovation trends of the past year are digital payments and the use of QR codes, which provide for Peruvians an agile and efficient means for daily transactions. A factor that has enabled digital payments to take off is the recent exponential growth of e-commerce in Peru.

- 1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?**

At the moment there are no prohibited fintech businesses in Peru.

Notwithstanding, there are some reserved activities that require a licence from the competent authority to be carried out, such as: (i) financial intermediation, which is reserved only for financial entities under the supervision of the SBS (*Superintendencia de Banca, Seguros y AFP*); (ii) public offering of securities under the supervision of the SMV (*Superintendencia del Mercado de Valores*); (iii) provision of insurance, only for insurance companies under the supervision of the SBS; and (iv) issuing of e-money, which can be carried out only by companies operating under the supervision of the SBS. Those mentioned activities require a licence and the fulfilment of the applicable regulation (risk management, corporate governance, prudential regulation, conduct of business and AML/CFT).

Cryptocurrency-based businesses have no specific regulation but are governed by all the applicable laws like any other business. Even if there is no specific prohibition, the SMV and the Peruvian Central Bank have given statements about the dangers surrounding cryptocurrencies (e.g. fraud). Regarding initial coin offerings (ICOs) in Peru, it is of our understanding that it will be necessary to request a previous authorisation from the SMV because of its similarity with a public offering of securities regulated by the Peruvian Law of Stock Market.

2 Funding For Fintech

- 2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?**

The fintech industry in Peru gains the funding for the development of their businesses through:

- Savings and founders' loans.
- Friends, family and fools.
- Crowdfunding, businesses incubators and venture capital.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

The investment in fintech businesses is recent and premature in Peru. For that reason, currently, there are neither special incentive schemes nor special tax treatments for enterprise or venture capital investments in fintech businesses.

Even if there is no specific tax incentive for investments in technological companies, the Law of Income Tax contemplates a special retention rate considerably lower (4.99%) than the general regime (30%) for loans originated from abroad, only if the requirements established in the law are fulfilled. This may encourage foreign investment in Peruvian businesses, although it is not specific for the fintech or the technological industry.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

In Peru, under the definition of the Capital Markets Law, a public offering of securities is the invitation, adequately disseminated, that one or more individuals or legal entities offer to the general public, or to certain segments thereof, to carry out any legal act referring to the placement, acquisition or provision of securities. Additionally, according to the Law, an initial public offering is a public offering carried out by a legal entity. In brief, to IPO in our jurisdiction, the requirements are the following:

- Invitation: manifestation of will.
- By a legal entity.
- Adequately disseminated: offered through suitable means to make the content known to the recipients.
- To the general public.

Additionally, to carry out an IPO it is necessary to record the securities in the stock market register and to keep and communicate to the public all the related documentation (e.g. informative leaflet, financial statements and value classification), based on the principle of transparency.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

The Peruvian fintech market is young and incipient. Most of the Peruvian fintech enterprises were founded between 2016 and 2018. For that reason, there is no record of a sale of business or IPO.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

In Peru, four authorities have jurisdiction in matters of financial services: SBS as the authority for the supervision of indirect financial intermediation, lending transactions and e-money; SMV in charge of the offering of securities and the supervision of the direct financial intermediation; BCRP (*Banco Central de Reserva del*

Perú) carries out the supervision of the payment services; and INDECOPI (*Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual*), which is the authority for the protection of the financial consumer.

Fintech businesses operating in Peru do not have specific regulation. Nevertheless, they must comply with the applicable laws, such as: personal data protection; consumer protection; tax; and the civil code in terms of contracts. For carrying out lending and money exchange activities, fintech companies must obey the AML/CFT specific regulation. Moreover, those two types of fintech businesses must be subscribed in the registration database managed by the financial services supervisor (SBS).

Furthermore, the SMV and the BCRP are drafting the forthcoming Law of Crowdfunding, which is expected to be issued this year. According to this Law, the SMV will be the authority in charge of supervising lending and equity crowdfunding platforms in Peru. The authorities in charge have announced that this Law will balance the public objectives of safeguarding and the development of the crowdfunding industry in Peru.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

There is no specific regulation for cryptocurrencies or cryptoassets in Peru.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

Financial regulators and policy-makers in Peru are receptive to fintech innovation and are conscious about the importance of being technologically neutral in their norms. Their receptivity is manifested in their availability to attend to new entrants and to ask for feedback before taking action. Currently, as explained in question 3.1, the SBS, BCRP and SMV are working together on a normative proposal for the regulation of crowdfunding, asking for feedback regarding the fintech industry.

In Peru there is no policy for the application of regulatory sandboxes.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

Fintech businesses established outside Peruvian jurisdiction can operate in Peru. As a matter of fact, the Peruvian Constitution of 1993 allows foreign capitals and gives them guarantees for their protection. However, the lack of clarity and certainty in the regulation is a regulatory hurdle that every fintech business must overcome. An example of this can be seen in the outdated Peruvian regulation of financial services, such as the broad and blurry definition of deposit-taking activities stated in article 11° of Law 26702, under which an innovative financial service like lending crowdfunding can be understood as a deposit-taking activity. Hence, it is important to get appropriate advice in financial regulation to avoid unnecessary legal contingencies.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/ transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

In Peru, the collection, use and transmission of personal data is regulated under the Peruvian Law for the protection of personal data, Law N° 29733, and its related rules. It applies to fintech businesses operating in Peru, like any business that treats a client's personal data. The core legal provisions for the protection of personal data are the following: (i) the implementation of adequate data protection systems; (ii) the designation of the data bank manager; (iii) the prior consent of personal data owners for data processing; and (iv) the recognition to the owner's right to cancel or adjust the data provided.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

Personal data protection laws apply to all the data treated in Peruvian territory even if they are private or public entities established in Peru or abroad. Personal data laws allow cross-border transfers of data only if the target country maintains appropriate levels of protection as the Peruvian laws do.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

The sanctioning procedure for failing to comply with data privacy regulation is established in the Law N° 29733 and its related rules. Contraventions include any action or omission that violates or breaches any of the provisions of data privacy law. They are classified as minor, serious and very serious. The law specified the thresholds for the administrative penalties in the event of non-compliance of the regulation. Finally, data privacy laws also contemplate the possibility of imposing coercive penalties in case they do not comply with the incidental obligation to the sanction.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

In Peru there are neither cyber security laws nor regulations for the private sector. Nevertheless, fintech businesses operating in Peru as a good practice may comply with international cyber security standards, such as ISO 27032.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

Peru has issued several regulations in order to implement an AML/CFT policy. There is a general regulation for AML/CFT, Law N° 27693, which list the businesses obliged to inform any suspicious transaction to the UIF-Peru. Among the businesses included in the referred list are the ones dedicated to lending, money exchange and

crowdfunding. Therefore, fintech businesses that carry out such activities must implement all the requirements established on the Supreme Decree 020-2017 for the report of suspicious activities.

Additionally, for the development of lending and money exchange activities, there is a specific regulation that the fintech businesses must obey established in the Resolution N° 789-2018. Actually, lending and money exchanges businesses supervised by the UIF-Peru in matters of AML/CFT must be part of the registration database that is managed by the SBS according to the Resolution N° 6338-2012. The subscription is seven years long and needs to be renewed.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

The consumer protection regime is also applicable to fintech businesses operating in Peru because the Peruvian Code for Consumer Protection, Law N° 29571, provides a regulation based on transparency and suitability for the provision of financial services, and protects financial consumers by providing them with a space for claims if necessary.

The means of payment are also regulated in Peru, being listed in the Law N° 28194 (they include mainly bank transfers). The norm establishes the amount (US\$ 1,000), for which only such listed means of payment must be used.

Also, our jurisdiction contemplates an interest rate cap for lending transactions outside the financial system. On the contrary, loans provided by financial entities have no interest rate caps. Moreover, all financial services rendered outside the financial system (including those provided by fintech companies) are affected with value-added tax (VAT), unlike the services provided by financial institutions that are exonerated.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

The legal framework in the hiring of employees is based on the principle of supremacy of the reality, which means that in case of discrepancy between the practice and what was agreed in the contracts, the day-to-day situation will have greater value. In Peru, businesses can hire staff in three modalities: a determinate contract period; an indeterminate contract period; and part time (maximum four hours per day).

Moreover, in order to dismiss an employee, the decision must be based on a legal and objective cause. If the decision of the dismissal is arbitrary, the employee has the right to receive an indemnification for the damages. In case an employee (with a determinate contract period) is dismissed without a legal and objective cause, the indemnification is a remuneration and a half for each month not worked. And, in the case of an employee with an indeterminate contract period, the indemnification is a remuneration and a half for each year of work. Both cases have a maximum of 12 remunerations.

It should be noted that the greatest contingency associated with the dismissal of an employee is the possibility that, via a judicial process, he/she might be reinstated in the company and have recognised in his favour the payment of remuneration and social benefits accrued during the period between the dismissal and the

replacement. In addition, the employee could simultaneously sue the company for the payment of compensation for damages suffered, which includes emergent damage, loss of profits and moral damage.

5.2 What, if any, mandatory employment benefits must be provided to staff?

The mandatory employment benefits that must be provided to employees are the following:

- Minimum wage: this is not static, and is currently approximately US\$ 300.
- Vacations: 30 days for each year of services in the regular regime and 15 days for small businesses.
- CTS (compensation for years of service): equivalent to a complete remuneration and payable in two parts, one in May and the other in November.
- Gratification: twice a year (for Christmas and Independence Day) and which is equivalent to two complete salaries, according to the months of service.
- Health insurance: 9% of the total amount of the salary must be paid by the employer.
- Family assignment: if the employee has at least one child, he will receive 10% of the minimum wage.
- Participation in the company's profits: companies that generate third-category revenues with more than 20 employees are obliged to share a percentage of their earnings among their employees.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

There is no regulatory hurdle *per se*, but in order to bring employees from outside to Peru several immigration procedures must be fulfilled. For immigration procedures the company must be active in the SUNAT (*Superintendencia Nacional de Aduanas y de Administración Tributaria*). The procedures are different if the employee comes for a short period of time than if he stays longer. Additionally, the Ministry of Labour and Employment Promotion demands a special procedure for the approval of hiring foreign employees.

If foreign personnel are required to provide services in Peru, it is important to take into consideration the specific provisions regulated in the Law for the hiring of foreign workers, and its related rules.

In order for the foreign citizen to be able to work in Peru, two requirements must be fulfilled: (i) the employment contract must be registered within the Ministry of Labour; and (ii) the worker must have the enabling migratory quality that allows him to work. In other words, he must have the work visa approved by the National Superintendence of Migrations.

Regarding the application of employment rights and benefits, it is important to note that foreign workers have the same rights and obligations as national workers.

Finally, there are no special procedures for hiring foreigners in favour of fintech businesses.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

In Peru, innovations and inventions are protected under the Intellectual Property (IP) system. The Legal Decree 1075 is the main internal law, which follows the Decision 486 of the Andean Community Commission that establishes common-system IP rights. There are some constituent elements of intellectual property rights, which should be processed before the competent authority in the field of intellectual property protection – INDECOPI. The constituent elements are the following:

- Trademark: a sign or a combination of signs used to distinguish the goods or services of one enterprise from another.
- Patent: the protection must be available for eligible inventions in all fields of technology that are new, involve an inventive step and can be industrially applied.
- Geographical indication: a name or indication associated with a place that identifies a product, and identifies the product's special characteristics, which are the result of the product's origins.
- Industrial design: usually referred to the ornamental or aesthetic aspect of the objects.
- Copyright: referring to the rights of the authors in their literary and artistic works.

Inventions are protected in Peru in the form of patents and utility models. Both titles are obtained by the inventor or to whom he has ceded his rights of inventor. The peremptory period for patents is 20 years and 10 years for a utility model, counted from the presentation of the application for registration. The protection of a patent of invention or utility model is based on the principle of territoriality, according to which the patent is protected and therefore its holder has rights over it, in the territory where he obtained its registration.

There are three requirements for obtaining a patent of invention:

- a) Must be novel: should not exist in any other part of the world.
- b) Must have an inventive level: not be evident.
- c) Must have industrial application.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Intellectual property brings together industrial property and copyright. Both are protected in a different way. As long as the industrial property rights are protected from their registration at INDECOPI (the registry is constitutive of rights), the copyrights are protected from their first use.

For the ownership of IP rights, registration is required in order to be opposable against third parties and the registration must be processed under the competent authority (INDECOPI). The registration gives a right of exclusivity, for a period of time, to be able to appropriate and exploit that invention. The right of exclusivity has two aspects: to grant IP rights; and to avoid third-party use of the invention without permission.

Industrial property rights include patents, utility models and industrial designs, trademarks, and geographical indications. The registration of distinctive signs and new creations are also governed by the principle of territoriality. The holder of a distinctive sign has

the exclusive right to use the trademark in accordance with his interests: license the trademark to others; constitute guarantees; and transfer their rights to a third party. Moreover, the owner of a distinctive sign may object to the registration of distinctive signs which he considers to be affecting his rights and to file complaints for the infringement of his rights in the case of the use of identical or similar signs by third parties.

Copyrights do not need the recognition of the right from the Peruvian state, the single creation already gives the right over it – the register is only declaratory. The term of validity of a copyright is the total amount of years the author was alive, plus 70 years counted from his death. After this period, the work is passed into the public domain. The recognition is global and not territorial.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

Neither local nor national rights are required to enforce IP rights. Nationals or foreigners may request their registration and exercise the rights derived from them without inconvenience.

There are no treaties to recognise in another country, *per se*, a right obtained in our country. However, there are treaties signed between Peru and others, whereby reciprocal benefits are granted to the Contracting Parties. Thus we have the following:

- Andean Community: through “Decisions” there have been established principles and benefits for the member countries

(Bolivia, Colombia, Ecuador and Peru). In that way, Decision 486 establishes the possibility that the owner or applicant to a trademark in any of the member countries will be able to formulate Andean opposition against the registration of a trademark in another member country, only if a market interest is accredited through the registration request. Also, in the event of a cancellation due to the lack of use of a trademark, the owner of the trademark may present proof of use of the trademark generated not only in the country where the cancellation is requested, but also those generated in the other member countries.

- Others, such as: the Paris Convention; Washington Convention; Patent Cooperation Treaty; Singapore Treaty on the Law of Trademarks; Lisbon Agreement for the Protection of Appellations of Origin and their International Registration; Berne Convention for the Protection of Literary and Artistic Works; and Rome Convention.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

The owner of IP rights, as mentioned in question 6.1, gives exclusive rights to exploit or monetise them for a limited period of time established in the Legal Decree 1075. The exclusivity provided by IP rights allows legal measures to be taken in case of the infringement of such rights. However, there are not particular rules or restrictions to exploit IP rights.



Ljubica Vodanovic

Vodanovic Legal
Av. Mariscal La Mar 550
Miraflores
Peru

Tel: +51 1 326 8948
Email: lvodanovic@vodanovic.pe
URL: www.vodanovic.pe

Expert in Financial Regulation. Graduated with honours from the London School of Economics and holds an LL.M. specialised in Banking and Financial law (2002–2003). She has worked for 11 years (2002–2013) as Executive Coordinator in the Legal Department at the Superintendencia of Banking, Insurance and Private Pension Funds (SBS). She was Of Counsel at Philippi, Pietrocarrizosa, Ferrero, DU & Uria (former Delmar Ugarte Lawyers) (2013–2016).

She advises banks and financial and insurance organisations on regulation. Likewise, she also advises local and international companies interested in providing financial services in Peru. Moreover, she is considered one of the leading lawyers in banking and financial regulation in Peru, according to the 2018 and 2019 editions of *Chambers & Partners*.

In addition, she is in charge of the course 'The Financial System Regulation' at Pontificia Universidad Católica del Perú (PUCP) and Universidad del Pacífico (UP). She has also given presentations in seminars, conferences and workshops on topics related to Banking and Finance Law.



Alejandra Huachaca Barco

Vodanovic Legal
Av. Mariscal La Mar 550
Miraflores
Peru

Tel: +51 1 326 8948
Email: ahuachaca@vodanovic.pe
URL: www.vodanovic.pe

Graduated from the Universidad del Pacífico Law School in July 2018. She carried out her career's orientation in Financial Law, Privacy Law and Consumer Protection. Former member of FORSETI, a Law Magazine of the Universidad del Pacífico. Additionally, she participated in an academic exchange programme at Institut d'études politiques de Paris – Sciences Po (2016). She has worked at Vodanovic Legal since January 2017.

She speaks Spanish, English and French.



Vodanovic Legal is a legal firm specialised in financial regulation, focused on the use of technology for the provision of financial services. Vodanovic Legal aims to be the legal support that helps to develop a more efficient and inclusive financial market, that relies on technology to innovate and keep high standards of regulatory compliance.

The main Peruvian banks and financial institutions, as well as local and international non-regulated companies, come to the firm for legal advice on financial services. Due to the firm's extensive knowledge on financial regulation and the experience of its members who have worked in the Peruvian Supervisor of the financial system (SBS), the firm has an advantage that is unique in the local market. In fact, lawyers have a particular insight into the financial sector because they know how it works, what concerns arise, what norms apply and how the authorities interpret those norms.

The founding partner Ljubica Vodanovic has been recognised as a leading lawyer in financial regulation by the prestigious *Chambers & Partners* 2018 and 2019 editions.

Philippines



Gorriceta Africa Cauton & Saavedra

Mark S. Gorriceta

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

The Philippine fintech landscape is dominated by start-ups in the payments and remittances subsectors, followed by in the alternative finance and blockchain/cryptocurrency applications subsectors. Industry players have partnered with merchants to facilitate payment of products and services through mobile wallets. The remittances subsector became a heavily contested arena for market share due to the millions of overseas Filipino workers who avail of remittance services for their families. The alternative funding industry subsector in the Philippines includes various crowdfunding as well as loan management platforms. The Philippine blockchain space is also continuously growing – utilising this emerging technology for mobile payments, and several other companies offering blockchain-based products.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

Currently, there are no express prohibitions applicable to fintech businesses in the Philippines. As regards restrictions for fintech businesses, due to lack of specific regulations, virtual currency trading platforms currently cannot operate in the Philippines. Virtual currency exchange (VCE) and digital payment platforms, on the other hand, are regulated based on the regulatory sandbox approach adopted by the Philippine Central Bank (BSP). Moreover, commodities futures trading, which involves trading of asset-backed tokens, is also currently suspended by the Philippine Securities and Exchange Commission (SEC). Finally, initial coin offerings (ICO) cannot be conducted absent proper registration with the Philippine SEC and compliance with its forthcoming Final ICO Rules.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

There are two broad types of funding available to new and growing

businesses in the Philippines: private and public. On the one hand, private funding generally includes those from bank loans, investors, and venture capital funding. On the other hand, public funding takes the form of initial public offerings (IPOs) and crowdfunding.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

Yes, there are several statutes that provide special incentive schemes for fintech businesses and small/medium-sized businesses in the Philippines.

For fintech businesses, the Special Economic Zone Act of 1995 provides incentives such as tax holidays and exemption from national and local taxes for new businesses in the special economic zones designed as agricultural, industrial, commercial, financial, and fintech centres. Meanwhile, the Cagayan Special Economic Zone Act of 1995 envisions a “freeport for financial technology solutions and offshore virtual currency businesses”. It offers special tax rates and permanent residency status for foreigners with special skills and their families.

For fintech companies within the definition of small/medium-sized businesses, the Magna Carta for Micro, Small, and Medium Enterprises establishes government assistance for said businesses in the form of, among others, direct and indirect project lending, rediscounting of loan papers, and financial leasing.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

For a business to conduct an IPO in the Philippines, the following general conditions must be complied with:

- 1) minimum capitalisation requirement of either (a) PhP 500 million for corporations under the Philippine Stock Exchange’s (PSE) Main Board, or (b) PhP 100 million for corporations under the PSE’s Small, Medium, and Emerging (SME) Board, and, in either case, at least 25% of which is subscribed and fully paid;
- 2) three-year operating history prior to the listing application;
- 3) positive stockholder’s equity for three fiscal years prior to the listing application;
- 4) all subscribed shares of the same type and class applied for in the Listing Application shall be paid in full;

- 5) a covered company shall, at all times, maintain a minimum public ownership (MPO) of at least 20%. If the MPO of a covered company falls below 20% at any time after registration, such company shall bring that public float to at least 20% within a maximum period of 12 months from the date of such fall; and
- 6) the cumulative consolidated EBITDA must either be (a) at least PhP 50 million, for corporations under the Main Board, or (b) at least PhP 15 million, for corporations under the SME Board; and, in either case, for three full fiscal years immediately preceding the application for listing.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

In 2018, Uber Technologies, Inc. sold its Southeast Asia operations, which includes in its scope operations in the Philippines, to GrabTaxi Holdings Pte. Ltd.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

The fintech businesses in the Philippines are currently regulated by three key agencies: the SEC; the BSP; and the CEZA for fintech businesses that want to operate in the Cagayan special economic zone.

The SEC seeks to regulate ICOs with its release of the updated Proposed ICO Rules. It is also expected to regulate virtual currency trading in the near future.

The BSP regulates VCE platforms, electronic money issuers, and electronic or digital banking services and other electronic operations under BSP Circular Nos. 649, 942, 944, and 1033. It is also currently adopting a sandbox approach to fintech businesses operating or seeking to operate in the Philippines, provided that they comply with the requirements of the Anti-Money Laundering Act and the Terrorism Financing Prevention and Suppression Act.

The CEZA regulates the Cagayan special economic zone. It has recently branded itself as a fintech hub in the Philippines with its issuance of the Financial Technology Solutions and Offshore Virtual Currency Business Rules and Regulations (FTSOVCBRR) and the Digital Asset Token Offering (DATO) Rules. Under the FTSOVCBRR, a fintech business may secure a licence to operate in the CEZA. Meanwhile, the DATO Rules allow any issuer to conduct offshore offerings of its token, provided that it complies with the applicable laws of the jurisdiction/s where it intends to conduct its token offering.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

Yes. As mentioned in question 3.1, the Philippine SEC's ICO Rules are currently underway, with the Proposed ICO Rules released last August 2018 and updated last December 2018. With respect to the BSP, its Circular Nos. 942 and 944 provide for the rules to secure a VCE Certificate of Registration. A VCE platform is only allowed to convert cryptocurrencies to fiat and *vice versa*. It does not allow an order book type of exchange which is subject to the Philippine SEC's anticipated/future Virtual Currency Trading Rules.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

Yes. Given the gamut of recently issued, including anticipated, fintech regulations in the Philippines, financial regulators and policy makers are very receptive to fintech innovations and other technology-driven solutions. The BSP has also adopted a 'sandbox' approach for fintech companies with innovative technology solutions seeking to do business in the Philippines. Conditions for this 'sandbox' option are made on a case-by-case basis.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

As a consequence of the Anti-Money Laundering Act of 2001 (AMLA) and for the said non-resident start-up to be within the jurisdiction of the various implementing agencies, a business will be required to establish a domestic subsidiary or affiliate here in the Philippines for the purpose of securing the proper licences/permits before it can offer its fintech products and services.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

Yes. The Philippines regulates the collection/use/transmission of personal data by virtue of the Data Privacy Act of 2012 (DPA). The Philippine National Privacy Commission (NPC) is the agency tasked on its implementation and enforcement.

Under the DPA, fintech businesses processing personal information in the Philippines or of a Filipino citizen or resident are required to register its data protection officer (DPO) and data processing system(s) (DPS) with the NPC. It must also comply with the Advisories and Circulars of the NPC regarding its data processing activities, such as data sharing arrangements.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

The Philippine DPA applies extraterritorially if: (i) the act, practice, or processing of personal information relates to personal information about a Philippine citizen or a resident; and if (ii) the entity has a link with the Philippines by processing personal information in the Philippines, or even if the processing is outside the Philippines, as long as it is about Philippine citizens or residents.

Under the Philippine DPA, the international transfer of data, or any data transfer by the personal information controller, must be subject to a data sharing agreement which, among others, requires the data subject's consent.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

The National Privacy Commission (NPC) also has the power to issue a Cease and Desist Order or a temporary or permanent ban on the processing of personal information upon finding that the processing of the entity in question will be detrimental to the country's national security and public interest.

Additionally, under the DPA, various ranges of imprisonment and/or fines apply to the following violations:

- i) unauthorised processing of personal information and sensitive personal information;
- ii) accessing personal information and sensitive personal information due to negligence;
- iii) improper disposal of personal information and sensitive personal information;
- iv) processing of personal information and sensitive personal information for unauthorised purposes;
- v) unauthorised access or intentional breach;
- vi) concealment of security breaches involving sensitive personal information;
- vii) malicious disclosure;
- viii) unauthorised disclosure; and
- ix) combination or series of the aforementioned acts.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

Yes. Under the Cybercrime Prevention Act of 2012 (CPA), fintech businesses may incur corporate liability if any of the punishable acts under the CPA are knowingly committed on behalf of or for the benefit of a juridical person, by a natural person acting either individually or as part of an organ of the juridical person who has a leading position within, based on: (i) a power of representation of the juridical person, provided the act committed falls within the scope of such authority; and (ii) an authority to take decisions on behalf of the juridical person.

If the act committed falls within the scope of such authority or an authority to exercise control within the juridical person, it shall be held liable for a fine equivalent to at least double the fines imposable for the liability under the Revised Penal Code, up to a maximum of PhP 10 million.

However, if the commission of any of the punishable acts under the CPA was made possible due to the lack of supervision or control by a natural person, for the benefit of that juridical person by a natural person acting under its authority, the juridical person shall be held liable for a fine equivalent to at least double the fines imposable for the liability under the Revised Penal Code, up to a maximum of PhP 5 million.

Moreover, under the CPA, fintech businesses shall preserve the integrity of traffic data and subscriber information relating to its communication services (if present) for a minimum period of six months from the date of the transaction. Content data shall be similarly preserved for six months from the date of receipt of the order from law enforcement authorities requiring its preservation. Any order and compliance to preserve the computer data must be kept confidential.

Meanwhile, under the Access Device Regulation Act of 1998 (ADRA), fintech businesses issuing access devices that can be used to obtain money, goods, services, or any other thing of value or to

initiate a transfer of funds must comply with reportorial requirements to the Credit Card Association of the Philippines regarding access device frauds committed against its holders in the preceding calendar year, for consolidation and submission to the Philippine National Bureau of Investigation (NBI). Such fintech business shall also be continually regulated and supervised by the BSP.

Finally, under the Electronic Commerce Act of 2000 (ECA), fintech businesses acting as service providers of online services or network access have no authority to modify or alter the content of an electronic data message or electronic document which it received, or to make any entry therein on behalf of the originator, addressee or any third party, unless specifically authorised to do so. In relation to electronic documents, the obligation of fintech businesses is, therefore, to retain the document in accordance with the specific request or as necessary for the purpose of performing the services it was engaged to perform.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

Financial crime prevention in the Philippines is operationalised under the Anti-Money Laundering Act of 2001 (AMLA) and the Terrorism Financing Prevention and Suppression Act of 2012 (TFPSA). For fintech businesses, the main obligations under AMLA is to establish Know-Your-Customer (KYC) procedures for customer identification, as well as for record keeping, and reporting of covered and suspicious transactions. It also created the Anti-Money Laundering Council (AMLC) which acts unanimously to discharge the functions of the AMLA. A fintech business falling under BSP regulation is deemed to be a 'covered institution' which shall be required to report to the AMLC all 'covered transactions' generally within five working days from occurrence thereof. A 'covered transaction' is transaction in cash or other equivalent monetary instrument exceeding PhP 500,000.00. Further, under the TFPSA, the AMLC is likewise authorised to investigate or to issue *ex parte* orders to freeze funds that are in any way related to financing of terrorism or acts of terrorism when there is probable cause to believe that a fintech business is committing or attempting or conspiring to commit, or participating in or facilitating the commission of financing of, terrorism or acts of terrorism as defined under the TFPSA.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

Yes. Fintech businesses offering, selling, or marketing financial products or devices must consider the Consumer Act of the Philippines (CAP). The CAP provides penalties for various unfair and unconscionable sales acts and practices which, if committed by juridical persons, would make responsible natural persons of managerial positions accountable (i.e., the company's Chairman of the Board of Directors, President, General Manager, etc.).

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

Employment in the Philippines is essentially governed by the Labor Code of the Philippines and other applicable rules and regulations

issued by the Department of Labor and Employment (DOLE). The requirements of hiring employees depend on whether or not the applicant employee is a Filipino citizen. For instance, foreigners are required to secure an alien employment permit, among others.

Meanwhile, the legality of dismissing an employee is two-pronged. The employer must comply with both the procedural and substantive due process in terminating the services of the employees.

Accordingly, the employer can only validly dismiss an employee for just and/or authorised causes and only upon compliance with the twin-notice requirement (first notice specifying the causes for which the dismissal is sought, and second notice signifying the decision to terminate) under the law.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Aside from the mandatory benefits under the Labor Code, the following benefits are required to be given to employees under various pieces of social legislation:

- 1) enrolment of employees and employer contributions to the Social Security System (SSS);
- 2) enrolment of employees and employer contributions to the Home Development Fund, more popularly known as the PAG-IBIG Fund;
- 3) enrolment with the Philippine Health Insurance Company (PhilHealth); and
- 4) entitlement to retirement benefits, among others.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

The Labor Code requires non-resident aliens who wish to be employed in the Philippines to secure an Alien Employment Permit (AEP). Prospective employers must likewise secure an AEP for their prospective employees who are foreigners. The application shall be filed with the DOLE Regional Office having jurisdiction over the place of business of the employer. The application may, however, be denied if it is determined that there exists another potential employee in the Philippines who is competent, able, and willing to perform the work needed by the employer at the time of the application.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Intellectual property such as innovations and inventions are generally protected under the Intellectual Property Code of the Philippines (IP Code). The law categorises the protection of certain intellectual creations, to wit: (1) patents; (2) trademarks, service marks and trade names; and (3) copyright. Accordingly, inventions and innovations may be protected through patents provided that they satisfy the requirements under the law to be patentable. Among the rights of a patent holder is the right to restrain, prevent, or prohibit any unauthorised use or manufacture of the patented product or process.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

- 1) **Patent.** The rights arising from a patent belong to the owner or inventor of the patent and his/her heirs or assigns. When an invention is made by two or more persons, the patent shall be owned by them jointly as well as the rights arising therefrom.
- 2) **Trademark.** In order to be protected, trademarks are required to be registered in accordance with law. A certificate of registration is considered as *prima facie* evidence of ownership of the mark subject only to challenges from other persons with a stronger right over the mark, such as a prior user and the owner of an internationally known mark or brand.
- 3) **Copyright.** An original intellectual creation is automatically protected by copyright from the moment of its creation. Generally, the author of the work is considered as the owner of the copyright. Nevertheless, when the work was made in the course of employment, ownership thereof depends on the agreement of both parties. In the absence of any agreement, the copyright of any work created by virtue of the employee's regular duties belongs to the employer.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

International law forms part of the law of the land. Thus, the Philippines accords the rights protected under the treaties to which it is a signatory. The Philippines is a signatory to the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) which provides for the minimum standard for the enforcement and protection of intellectual property rights, as well as the Paris Convention for the Protection of Industrial Property.

Under the IP Code, any person who is a national or who is domiciled in a country which is a party to any convention, treaty, or agreement relating to intellectual property rights to which the Philippines is also a signatory, or in a country which extends reciprocal rights to Filipino nationals, is entitled to enforce his rights under such convention, treaty, or agreement in addition to other rights to which he may be entitled under the Philippine laws.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

Intellectual property owners are given certain moral and economic rights under the law. Intellectual property owners may enter into licensing agreements with other entities or 'technology transfer arrangements' where the licensor may earn a royalty or licence fee from the use of their intellectual property rights. Such agreements are, however, subject to requirements and prohibited clauses under the IP Code. Non-compliance with the mandatory provisions and requirements under the IP Code shall render the arrangement unenforceable unless registered with and approved by the Intellectual Property Office. Sale and/or transfer of intellectual property rights is also allowed.



Mark S. Gorriceta

Gorriceta Africa Cauton & Saavedra
15/F and 4/F Strata 2000
F. Ortigas Jr. Road
Ortigas Center, 1605 Pasig City
Philippines

Tel: +632 696 0687
Email: msgorriceta@gorricetalaw.com
URL: www.gorricetalaw.com

Mark S. Gorriceta is the Managing Partner and Head of the Corporate Group of Gorriceta Africa Cauton & Saavedra. Mark is considered the foremost Technology lawyer in the Philippines. He is also a ranked and leading lawyer in the fields of Capital Markets, Mergers & Acquisitions, Real Estate and Taxation.

Mark is considered a pioneering lawyer in the Philippines on the law on blockchain, virtual currencies, e-commerce and artificial intelligence. Mark is legal counsel to many of the largest and most influential tech and online companies in the Philippines.

A member of the Philippine Bar, Mark graduated law with honours and holds a Bachelor of Arts, Political Science degree from the Ateneo de Manila University. He also completed courses in Finance at the Asian Institute of Management. He completed two Masterclasses on Blockchain, Distributed Ledger & Smart Contracts in Singapore. Mark is enrolled in Harvard University's certificate programme in Corporate Finance.

Beyond Results®

GORRICETA 
GORRICETA AFRICA CAUTON & SAAVEDRA
www.gorricetalaw.com

Gorriceta is a leader in the Technology Law practice in the Philippines. It is also one of the leading firms in the country in the fields of Capital Markets, Corporate Law, Mergers and Acquisitions, Real Estate, and Taxation. Gorriceta was awarded "Rising Law Firm of the Year" in Asian Legal Business' 2016 Philippine Law Awards, and was a finalist for "Law Firm of the Year" in the Asian Legal Business 2017 and 2018 Philippine Law Awards. Gorriceta is also a recognised and ranked firm by various prestigious international organisations such as Asian Legal Business, *International Financial Law Review*, *International Tax Review*, *Chambers and Partners*, and the Asia Law Profiles. Gorriceta is considered the "**youngest biggest**" law firm in the Philippines today.

Poland

Jan Byrski, PhD, Habil.



Karol Juraszczyk



Traple Konarski Podrecki & Partners

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

The year 2018 saw the growth of fintech companies in Poland and this trend is likely to continue in the years to come. In addition to business and technology development, the legal environment in which fintech companies operate is also undergoing dynamic changes. These changes are attributable, to a large extent, to the transposition of EU directives (PSD2, AML4, MiFID2) to the Polish legal order and the entry in force of the General Data Protection Regulation (“GDPR”). Without doubt, the new regulations represented a challenge for fintech companies who had to adjust their operations to these requirements. At the same time, it is worthwhile to highlight the legal solutions introduced in Poland to facilitate the launch of business activity in the area of financial innovations such as, for instance, the introduction of a legal framework for the operation of small payment institutions.

One of the most strongly developing sub-sectors of the fintech area is the payment services market that is driven by the dynamic growth of e-commerce, where innovative payment methods (e.g. based on mobile applications or electronic wallets) are becoming increasingly popular at a much faster rate than traditional sales channels. The changes prompted by the transposition of Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market (“PSD2”) to the Polish legal system also contribute to the growing innovativeness of the payments market. The Directive imposes on the account servicing payment service providers (“ASPSPs”) the obligation to enable provision to third party providers (“TPPs”) of account information services (“AIS”) and payment initiation services (“PIS”). Another key element requiring adjustment of technological solutions by providers of payment services is the obligation to apply strong customer authentication (“SCA”), as regulated by the PSD2 Directive, and the regulatory technical standards developed on its basis by EBA and adopted by the Commission (EU) as a delegated Regulation. The time allowed for the adjustment of operations to the open banking requirements and SCA is set to expire on 14 September 2019.

It is worthwhile to note the growing interest in solutions based on the distributed ledger technology (blockchain) among financial

institutions. Banks began using this technology, *inter alia*, while fulfilling requirements stemming from the obligation to provide customers with documents in the form of a durable medium. This was linked to the position adopted by the Polish competition and consumer protection authority, according to which the transmission of documentation to a customer via an incoming electronic mail box did not meet the criteria set for the information to be deemed provided on a durable medium.

The high activity of companies from the fintech sector in Poland also relates to the provision of various types of financial services via online platforms or mobile applications. Technologically innovative solutions consisting of automated personal data processing, including profiling for the purpose of, for example, creditworthiness, assessment or evaluation of insurance risk, also using Big Data analysis, are becoming increasingly popular.

Without doubt, the Polish financial sector is one of the most technologically advanced and, consequently, implements innovative solutions relatively fast. It should be stressed that not only small and medium-sized enterprises, for whom there is an element of competitive advantage, opt for innovativeness, but also institutions such as banks, insurance firms or investment companies that see in the dynamically growing fintech segment not merely a threat from smaller entities, but also an opportunity to grow their own business.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

In principle, Polish law does not prohibit doing business in any of the areas of the fintech sector. The **Polish Financial Supervision Authority** (“PFSA”, also known by its Polish acronym “KNF”) is the body overseeing the financial market in Poland. Upon stating that the operations of the entities engaged in business activity in any given area may potentially give rise to a specific risk, PFSA may issue relevant communications or warnings.

In 2018, PFSA’s communication related, *inter alia*, to the operation of cryptocurrency exchanges. In principle, this type of business is not prohibited in the territory of Poland. The communication highlighted new obligations on the part of companies active in this area that stemmed from the recognition of cryptocurrency exchanges as the obligated institutions within the meaning of the Act on Preventing Money Laundering and Terrorist Financing of 1 March 2018, including obligations relating to customer identification and verification of customer identity.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

Various forms (methods) of funding based on both equity and debt are available in the fintech sector for start-ups in Poland. Selection of the appropriate form of funding shall depend upon multiple factors, including, but not limited to, the type of pursued business, drawbacks and advantages of individual sources of capital as well as the stage of development of a given company. Among the various sources of funding available to start-ups operating in the fintech sector in Poland, the following should be listed:

- grants from the European Union;
- support from venture capital and private equity funds;
- support from private investors (so-called business angels);
- support via business accelerators;
- support from strategic industry investors;
- loans, advances; or
- crowdfunding.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

Companies from the fintech sector may also take advantage of certain systemic schemes supporting activity in the area of innovations that are in place in Poland. Such schemes include:

- **Innovation Box** tax relief foreseeing the application of the preferential tax rate of 5% on the income of eligible intellectual property rights generated, developed or improved by the taxpayer through his research and development activity; and
- research and development activity (“**R&D**”) tax relief permitting the deduction of up to 100% of specific tax expenses from taxable income.

Fintech companies may also consider participation in the programmes supporting, *inter alia*, innovative start-ups that are financed by the Polish Development Fund (“**PFR**”). Within the framework of the programmes organised by PFR, also in co-operation with Bank Gospodarstwa Krajowego, both technical and financial support may be obtained for innovative projects, also in the fintech area. The launch of the Cashless Poland Foundation (*Fundacja Polska Bezgotówkowa*) should not be overlooked. This is a joint initiative of the participants of the payment services market, namely the Polish Bank Association (known by its Polish acronym “**ZBP**”), the Ministry of Entrepreneurship and Technology, acquirers and Visa and Mastercard payment organisations. The purpose of the programme is to eliminate costs on the part of entrepreneurs related to the installation of payment terminals and their use over the initial 12 months from their installation.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

The conditions for conducting an initial public offering (“**IPO**”) in Poland depend on whether the shares of a given company (issuer) are to be quoted on the Main Market of the Warsaw Stock Exchange (“**WSE**”, also known by its Polish acronym “**GPW**”) or the

alternative market, NewConnect. The details of the IPO process are defined by law, including the Act on Public Offering, Conditions Governing the Introduction of Financial Instruments to Organised Trading, and Public Companies of 29 July 2005.

Summing up, the key conditions that need to be fulfilled before holding an initial public offering in the Main Market of WSE include:

- drafting the information memorandum required by law and its approval by PFSA;
- registering shares in the National Depository of Securities (“**KDPW**”) and assigning them an ISIN code;
- absence of bankruptcy or winding up proceedings pending against the issuer, and unrestricted transferability of the shares being the object of the application for admission to trading in the regulated market;
- satisfying the minimum requirements relating to capitalisation at the level, in principle, not lower than EUR 15m (for the companies previously quoted in another regulated market or NewConnect market, the minimum capital requirement is EUR 12m);
- a minimum of 15% of votes covered by the application for admission to trading being mandatorily in the hands of diluted shareholders (i.e. holding less than 5% of the votes in the general shareholders’ meeting) accounting, at the same time, for at least 100,000 shares of a minimum value of EUR 1m at the most recent issue or selling price;
- the issuer fulfilling the obligation to publish financial statements together with the opinion of the entity authorised to audit financial statements from the three consecutive years preceding the year of submission of the application for admission to trading; and
- the management board of the Stock Exchange assessing positively, *inter alia*, the issuer’s financial condition, prospects for the issuer’s growth, the experience and qualifications of the members of the issuer’s governing bodies, and resolving to admit the shares to public trading.

Admission of the shares to listing in the alternative trading system (NewConnect) involves the satisfaction of less strict requirements compared to the Main Market and is characterised, *inter alia*, by a more straightforward and faster procedure of admission to trading, less extensive disclosure obligations and lower capital requirements. On the other hand, this market is characterised by a narrower investor base and a smaller number of options for raising capital.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

In mid-2018, a record transaction in the Polish fintech market was announced (the transaction was finalised towards the end of the year). MCI and Saltus investment funds sold Dotpay and eCard, companies ranked among the leaders of the payment processing market in Poland, especially in regards to e-commerce. The value of the transaction totalled PLN 315m. The companies were purchased by Nets, a Nordic company also acting as an acquirer and provider of payment services. The transaction follows the general global trend of consolidation among online payment operators.

It is worthwhile to note that on 20 June 2018, regulations came into force in Poland whereby the purchase or acquisition of a specific package of shares or interests in a domestic payment institution resulting in the attainment or overrun by the future owner of, respectively, 20%, 30% or 50% of the held voting rights or share capital, triggers the obligation to notify PFSA and submit the related documentation. Among other things, PFSA has the right to lodge an objection to such transaction within the set time limit.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

The companies operating in the fintech sector in Poland are highly varied, both in terms of the type of pursued business activity and its scale. Technologically innovative solutions are introduced by banks, insurance companies, providers of investment-like services (e.g. brokerage services) that, implicitly, are engaged in a regulated activity that requires the securing of an appropriate licence from the competent bodies.

Companies from the fintech sector frequently conduct an activity classified as provision of payment services consisting, *inter alia*, of maintaining payment accounts (e.g. e-wallets), executing payment transactions (*inter alia*, acquiring), issuing payment instruments, issuing electronic money or, ultimately, providing PIS and AIS services. In principle, pursuit of this type of activity requires the securing of the appropriate status of a payment services provider. The Polish Act on Payment Services transposing the PSD2 Directive foresees various forms of conduct of this type of business, including the most popular ones in Poland:

- **national payment institutions** (“NPI”, also known by its Polish acronym “KIP”) – authorised to provide all payment services and issue electronic money to a limited extent, with no restrictions as to the value of executed transactions, with a relatively long and formalised process for obtaining PFSA permits for the conduct of related activity;
- **small payment institutions** (“SPI”, also known by its Polish acronym “MIP”) – a simplified formula for conducting activity consisting of providing payment services (except for provision of PIS and AIS services) in the territory of Poland, introduced on the basis of the so-called national option envisaged in the PSD2 Directive. Launching of activity under this business model requires an entry in the SPI register kept by PFSA (and not the securing of a licence). The procedure for securing the entry is significantly less formalised and should be completed no later than within three months of the submission of a complete application. The average amount of payment transactions executed by a small payment institution during the preceding 12 months cannot exceed EUR 1.5m monthly, and, once this limit has been exceeded, there is a path permitting the submission to PFSA of an application for the licence to provide services in the form of an NPI and continue the previous activity, with no need for observing the limit until the end of the proceedings before PFSA; and
- **payment services bureau** (“PSB”, also known by its Polish acronym “BUP”) – the simplest form of business whereby money transfer services exclusively may be provided within the statutory limits.

AIS may be provided also in the form of a **provider offering only the account information services**, which, as in the case of small payment institutions, requires a relevant entry in the register. In some situations, business activity may be based on one of the statutory **exclusions of the obligation to pursue business activity in a regulated form** (e.g. by the entities issuing payment instruments within the framework of a restricted merchant network), with the possibility of their application necessitating a case-by-case analysis; it should not thus be treated extensively. PFSA keeps registers of companies operating within a restricted network or telecom entrepreneurs providing payment services.

Another type of activity pursued by companies from the fintech sector which is a regulated activity is the provision of **consumer**

credits, including loans, on the principles defined in the Act on Consumer Credit. Pursuit of an activity in the form of a lending institution in compliance with the statutory act requires, *inter alia*, entry in the register of lending institutions kept by PFSA.

Activity in the fintech sector is frequently conducted also in the **capacity of an outsourcing partner** of companies engaged in a regulated activity. The obligations and restrictions associated with the outsourcing of some activities to third parties, including the obligation to notify PFSA of the intention to enter into this type of contract and, in some cases, even the obligation to secure PFSA’s consent, as defined by law, shall burden such company. Both Polish and European authorities supervising the financial market shall issue the related recommendations and guidelines out of which the following should be highlighted:

- PFSA’s sectoral recommendations and guidelines on management of IT and ICT security areas;
- position of the PFSA Office of 23 October 2017 on the use of cloud computing services by supervised entities;
- EBA Recommendations on outsourcing to cloud service providers of 28 March 2018; and
- EBA Guidelines on outsourcing arrangements, the final draft of which was published on 25 February 2019, and is set to take effect on 30 September 2019.

The above recommendations and guidelines are relevant to companies from the fintech sector that operate as outsourcers or insourcers in the regulated market of financial services.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

There are no regulations in Poland which are specifically directed at cryptocurrencies or cryptoassets. However, cryptocurrency exchanges are the obliged institutions as set out in the Act on Preventing Money Laundering and Terrorist Financing of 1 March 2018 (which implements Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, the “**AML4 Directive**”). They shall apply customer due diligence measures and follow other obligations related to the obliged entities as set out in the AML4 Directive.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

Regulatory authorities in Poland actively support the growth of companies operating in the financial innovations sector. It is worthwhile to mention the following measures taken by PFSA in this respect:

- establishment of an Innovation Hub programme whereby the legal and organisational framework can be agreed with PFSA for an innovative product or financial service;
- initiation of the appointment of the Task Force for Development of Financial Innovations (FinTech) with the purpose of identifying hurdles of a legal, regulatory and supervisory nature to the development of financial innovations in Poland, and preparing proposed solutions that could eliminate or mitigate the identified hurdles;
- initiation of the appointment of a task force for blockchain technology and cryptocurrencies; and

- initiation of the appointment of the FinTech Inter-Ministerial Steering Committee.

PFSA has plans to launch a regulatory ‘sandbox’ option for fintechs, although the programme has not yet been started. As of June 2018, companies planning to launch products or services aiming to enhance innovativeness of the Polish financial market may apply to PFSA to issue **individual tax rulings on the rules and regulations governing the financial market**, according to the procedure envisaged in the provisions of the Act on Supervision over the Financial Market. The basic advantage of this approach is the fact that the measures taken by the company applying for the issuance of a tax ruling, to the extent in which the company has complied with PFSA’s tax ruling, cannot provide the basis for imposition of an administrative sanction by PFSA.

The measures should also be highlighted that are taken by other state authorities and sectoral organisations grouping entrepreneurs which support the development of the fintech sector in Poland, such as:

- establishment by the **Ministry of Digital Affairs (“MDA”)** of the Task Force for Distributed Ledgers and Blockchain, the task of which is to create and develop a friendly and safe environment for the new technological firms operating in this sector;
- publication by the MDA of a guide for entrepreneurs from the fintech sector relating to the enforcement of GDPR, presenting the MDA’s views on a number of key issues relating to that sector; and
- publication by the **Polish Chamber of Information Technology and Telecommunications (“PIIT”)** of a comprehensive guide entitled “Blockchain in Poland. Opportunities and Applications”.

In January 2019, within the framework of the FinTech Inter-Ministerial Steering Committee, PFSA presented a bill amending the regulations on the pursuit of fintech activity which foresees, *inter alia*, the introduction of a register of crowdfunding platforms and regulation of their operation, **the liberalisation of regulations governing use of cloud solutions and banking outsourcing, the introduction of a small e-money institution, the introduction of small insurance companies** as a separate category of entities operating based on the entry in the record, and the introduction of changes liberalising the operation of small payment institutions.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

The possibilities and principles of provision of regulated financial services in the territory of Poland by foreign companies depend on the type of the provided service and the service provider’s country of origin. As regards companies with registered offices in the Member States of the European Union, business activity may be pursued in the territory of Poland, in principle, based on the freedom to provide services on the principles defined in the EU law. In the case of provision of regulated services, a company that holds the relevant licence to provide the services, issued by the competent authorities of a Member State, shall be able to launch its operations in the territory of Poland subject to the fulfilment of the additional conditions. These conditions may envisage, *inter alia*, the obligation to notify the regulatory authority of the home country of the intention to launch operations in the territory of Poland and transmission by that authority of the required information to PFSA. Depending on the type of pursued business activity, financial services in the territory of Poland may be provided by the companies based in another EU Member State:

- through a branch;

- within the framework of cross-border business activity; or
- through an agent,

within the scope outlined in the licence issued by the competent regulatory authorities of the home Member State.

The principles of pursuit of business activity in the territory of Poland are also defined by the Act on Principles of Participation of Foreign Entrepreneurs and Other Foreign Persons in Economic Transactions in the Territory of the Republic of Poland of 6 March 2018.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/ transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

The principles of processing of personal data are regulated in Poland by the following legal acts:

- GDPR, effective as of 25 May 2018 in all Member States of the European Union.
- The Personal Data Protection Act of 10 May 2018 introduced to ensure effective transposition into the Polish legal order of the provisions of GDPR which regulates, *inter alia*, the principles of operation of the supervisory authority in the area of personal data protection in Poland (the President of the Personal Data Protection Office), principles of conduct of control proceedings, imposition of administrative and cash penalties and the principles of criminal liability.
- The Act of 21 February 2019 on changes of certain laws in connection with Enforcement of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR) – this Act introduces, *inter alia*, the exclusion of some information obligations burdening a controller from the fintech sector or defines the legal grounds for making decisions based on automated personal data processing, including profiling (e.g. for the purpose of assessment of creditworthiness, credit risk analysis or assessment of insurance risk).

The aforesaid legal acts apply to all companies pursuing business activity in the territory of Poland consisting of personal data processing, also including companies from the fintech sector. The definition of personal data processing under GDPR is very broad and covers any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, storage, adaptation, disclosure by transmission, etc. It is worth noting that in March 2019, the President of the Personal Data Protection Office has imposed the first administrative fine for the violation of obligations resulting from GDPR, in the amount of approximately EUR 250k. The violation concerned the failure to fulfil the information obligation under GDPR, related to the processing of personal data contained in the public register of entrepreneurs.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

The privacy protection regulations in force in Poland apply also to

companies established outside the Polish jurisdiction. After all, the territorial scope of application of GDPR is extensive and applies to:

- controllers and processors having their registered offices in the European Union, whether or not the processing takes place in the EU;
- the processing of personal data of the data subjects staying in the territory of the European Union by a controller or processor having no registered office in the EU, if processing operations involve offering products or services to persons in the territory of the European Union or monitoring their conduct; and
- processing of personal data by a non-EU controller operating an organisational unit at a location where, under the public international law, the law of a Member State applies.

The privacy protection regulations in force in Poland also apply to the operations consisting of the international transfer of personal data. Although the principle of free movement of personal data applies within the European Economic Area (“EEA”), their transfer outside the EEA requires the fulfilment of additional conditions to ensure continued protection of data subjects. Such protection may be assured, for instance, by means of binding corporate rules, application of the so-called standard data protection clauses in contractual relations, or securing of the data subject’s consent.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

Any breach of the personal data protection regulations entails the risk of:

- application of the supervisory measures by the President of the Personal Data Protection Office, including imposition of high cash penalties envisaged in GDPR (even up to EUR 20m or 4% of the global total annual turnover);
- a claim for compensation being lodged by a person who has suffered property or non-property damage as a result of a breach of GDPR provisions by a controller or processor; and
- incurring criminal liability in the cases envisaged in the regulations of the Personal Data Protection Act, including unlawful personal data processing or hindering control activities carried out by the supervisory authorities.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

The cyber security regulations in force in Poland stem from transposition of the Directive concerning measures for a high common level of security of network and information systems across the Union (the “NIS Directive”) to the Polish legal system. The national cyber security regulations include in the first place:

- the Act on National Cyber Security System of 5 July 2018;
- the Regulation of the Council of Ministers of 2 October 2018 concerning the list of key services and thresholds of materiality of the impact of an interfering incident on the provision of key services; and
- the Regulation of the Minister of Digital Affairs of 10 September 2018 concerning the organisational and technical conditions for companies providing cyber security services and internal organisational structures of operators of key services in charge of cyber security.

The Act on National Cyber Security System introduces in the Polish legal system a new category of companies, i.e. core service operators that are obliged to implement the security management system within the IT system used for the provision of the key

service. This system is meant to assure, *inter alia*, systematic risk estimation, incident management, and the application of measures preventing and mitigating the impact of incidents on the IT system’s security.

Core service operators include, *inter alia*, companies from the banking sector. Hence, it should be assumed that cyber security regulations may also affect the companies operating in the fintech sector.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

The Act on Preventing Money Laundering and Terrorist Financing of 1 March 2018 in force in Poland constitutes the transposition of the AML4 Directive. Companies pursuing a regulated activity in the market for financial services, companies from the fintech sector included, are obliged to fulfil their obligations in the area of prevention of money laundering and terrorist financing. These cover, *inter alia*, the obligation to apply financial security measures (including customer identification and verification of customer identity, identification of beneficial owners, assessment and ongoing monitoring of economic relations), identification of Politically Exposed Persons (“PEPs”), reporting of transactions above the stipulated thresholds and suspicious transactions, or to introduce internal procedures in the area of prevention of money laundering and terrorist financing.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

In addition to the regulations and legal regimes listed above, the following regulations may also be of material importance to companies from the fintech sector:

- **consumer protection**, including the Act on Consumer Rights of 30 May 2014 or the Act on Examination of Complaints by Financial Market Companies and on the Financial Ombudsman of 5 August 2015;
- **provision of services by electronic means**, including specifically the Act on Provision of Services by Electronic Means of 18 July 2002; and
- **eIDAS Regulation**, including Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

The principles of employment of personnel in Poland under contracts of employment are regulated, first of all, by the Polish Labour Code. In addition to contracts of employment, other forms of employment are also applied, such as contracts of mandate, agency contracts or B2B contracts, the nature of each of them being unique.

A contract of employment may be concluded for a definite term, an indefinite term or for the duration of performance of specific work or

for a trial period. A contract for an indefinite term is the most advantageous basis of employment to an employee, as it protects most extensively the durability of the employment relationship: the need to provide the grounds and substantive justification for termination by the employer; extension of periods of notice compared to definite term contracts; and the obligation to consult on the termination with trade union organisations, if operating at the employer's organisation). Termination of the employment contract, depending on the case, may take place with notice, with immediate effect, by the parties' agreement or upon the lapse of the term of the contract. Special protection against termination is extended to some employee groups, including employees in pre-retirement age (four years prior to becoming eligible for retirement), employees during a period of excused absence from work (e.g. on holiday or sick leave), pregnant women and female employees on maternity leave, or employees on parental leave.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Any person employed under a contract of employment benefits from protection defined in the labour law regulations (including the Labour Code) relating, *inter alia*, to:

- remuneration (minimum salary, entitlement to overtime and night-time work allowances);
- paid holiday leave entitlement (in principle, 26 days a year);
- parental allowances;
- right to rest in every 24-hour period and per week; and
- counting of the employment period towards the service period.

An employee employed under a contract of employment is mandatorily eligible for health insurance and social insurance (old age, disability, sickness and accident insurance).

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

EU citizens may work in Poland with no need to obtain a work permit or a residence permit. This means that they may be employed in Poland with no need to obtain any additional permits. Where a citizen of the European Union resides in Poland longer than three months, such person is obliged to register their stay with the Voivodship Office having jurisdiction over that person's place of residence.

Third state citizens, other than EU citizens, may work in Poland once they have obtained a work permit and a residence permit. If a foreigner is to be employed in Poland based on a local contract of employment, the obligation to secure the work permit, even before the planned employment, rests with the Polish employer. Prior to submitting documents for the work permit, the Polish employer is obliged to examine the local labour market to determine whether no Polish employees are seeking the position for which the foreigner is applying. On the other hand, where a foreigner is seconded to work in Poland, the obligation to secure the work permit rests with the foreign employer who intends to second a foreigner to work in Poland.

The above general rules are rendered more accurate in the detailed regulations and, in the case of persons originating from some countries (other than the Member States of the European Union), different principles may apply. No dedicated path or procedure relating to the employment of staff in the fintech sector applies in this respect.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

The primary legal acts defining the principles of protection of intellectual property rights in Poland are the Act on Copyright and Related Rights of 4 February 1994 and the Act on Industrial Property Law of 30 June 2000. The listed legal acts comprise regulations relating to protection of works, objects of related rights, industrial designs, trade marks and inventions. The Unfair Competition Act of 16 April 1993 defines the principles of protection of know-how and business secrets. On the other hand, the principles of database protection are comprised in the Database Protection Act of 27 July 2001. In Poland, a number of EU legal acts and international agreements that also relate to protection of intellectual property additionally applies.

A key feature of the Polish copyright protection system is the absence of the obligation to satisfy formal requirements for protection to be granted (e.g. appropriate copyright marking). It suffices to determine the work, i.e. its manifestation in any form. Any manifestation of creative activity of individual nature is a work. On the other hand, the ideas themselves or work concepts are not afforded copyright protection. Computer software, especially important for the fintech sector, is, in principle, subject to copyright protection if it satisfies the criteria of a work. On the other hand, they are not subject to patent protection.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Under Polish law, copyright is divided into the author's moral rights and the author's economic rights that, in principle, are vested originally in the author. The author's economic rights only may be the object of trading (transfer or licence), whereas the author's moral rights (such as the right to mark the work with one's name and surname, right to the work's integrity or deciding on the work being made available to the general public for the first time) are inalienable and stay with the author. In some cases, the author's economic rights may also arise for the benefit of the entities other than the author (in particular, for the benefit of the employer). In the remaining cases, the author's economic rights may be transferred or a licence may be granted in the form of a contract.

Similar rules apply when it comes to the rights to secure rights of protection for inventions, utility models, industrial designs or trade marks. These rights are originally vested, in principle, in the author, but where an invention, industrial design or utility model is produced under a contract of employment or another contract binding the author and the contracting authority (e.g. contract to perform a specific work or contract of mandate), the rights to secure protection rights pass to the contracting authority by force of law.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

As previously indicated, works and objects of related rights are afforded protection with no need for registration or placement of any marking on the work. The Polish Copyright Protection Act assures protection of works:

- whose author or co-author is a Polish national;

- whose author is a national of a Member State of the European Union or of a Member State of the European Free Trade Association (“EFTA”), or parties to the agreement on the European Economic Area;
- that have been published for the first time in the territory of Poland or simultaneously in that territory and abroad;
- that have been published for the first time in the Polish language; or
- that are afforded protection under international agreements to the extent in which their protection stems from those agreements.

Securing protection under a patent, right of protection for a utility model, right of protection for a trade mark or a right from registration of an industrial model requires the fulfilment of applicable formal requirements, such as notification to the competent authority and successful completion of the registration procedure. Depending on the type of right, the relevant notification may be made both before the Polish (the Patent Office of the Republic of Poland) and international authorities (e.g. EUIPO, WIPO), which allows for expansion of protection to a greater number of countries.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

Intellectual property rights are exploited or monetised in Poland through the conclusion of various types of contracts transferring rights (e.g. based on a sale contract), authorising another entity to exercise a right (licence) or contracts securing claims (e.g. pledge). In the case of industrial property rights, the object of trading may be both the rights themselves (patents, rights of protection for industrial designs, rights of protection for trade marks, etc.) as well as the expectative of those rights (i.e. the right to seek a patent or right of protection). In principle, a copyright contract or industrial property rights contract must be concluded in writing to be valid.

Trade in intellectual property rights may be restricted to a certain extent. This applies, *inter alia*, to the inability to sell the author’s moral rights or to use the work within the framework of the institution of permitted use. The Copyright Act introduces also special regulations governing the exercise of the author’s economic rights in computer software.



Jan Byrski, PhD, Habil.

Traple Konarski Podrecki & Partners
ul. Twarda 4
00-105 Warszawa
Poland

Tel: +48 22 850 10 10
Fax: +48 22 697 63 72
Email: jan.byrski@trapple.pl
URL: www.trapple.pl

Jan Byrski is a Partner at Traple Konarski Podrecki & Partners and head of the FinTech team. He specialises in legal protection of information (personal data, professional secrets, enterprise secrets) and in financial institutions (FinTech), IT and TMT law.

He provides legal advice to financial institutions operating on Polish and international markets. Jan Byrski is a legal expert at the Polish Chamber of Insurance (PIU) and the Foundation for Development of Non-Cash Transactions (FROB).

He participated in drafting an amendment to the Act on Personal Data Protection and the Act on Payment Services. He is Vice-President of the FinTech Committee of the Polish Chamber of Information Technology and Telecommunications (PIIT), a member of the IAPP and of the Working Group in Ministry of Digitalization (GDPR in FinTech and Blockchain).

Jan Byrski is the author and co-author of numerous academic and popular science publications. He is an assistant professor at the Chair of Civil and Business Law, Faculty of Finance and Law, at the Kraków University of Economics.



Karol Juraszczyk

Traple Konarski Podrecki & Partners
ul. Królowej Jadwigi 170
30-212 Kraków
Poland

Tel: +48 12 426 05 30
Fax: +48 12 426 05 40
Email: karol.juraszczyk@trapple.pl
URL: www.trapple.pl

Karol Juraszczyk specialises in new technologies law, in particular in payment services law, personal data protection law and issues related to anti-money laundering (AML). He has experience in the field of contract law, services provided by electronic means, consumer protection and e-commerce law. Karol Juraszczyk has represented a payment institution before supervisory authorities such as the Polish Financial Supervision Authority (KNF) and the General Inspector of Financial Information (GIIF).

Karol Juraszczyk has gained experience while providing legal services to a leading payment service provider operating on the Polish market. He has represented the company in due diligence processes and post-transactional integration. Before that, he was in the capital markets sector where he worked in compliance departments of two brokerage houses.

Graduate of the Faculty of Law and Administration at the Jagiellonian University. He is a legal advisor and a member of the Regional Association of Legal Advisors in Krakow.



Traple Konarski Podrecki & Partners is one of the leading law firms on the Polish market. It specialises primarily in the following areas: TMT, IT, financial institutions and payment services law (FinTech); intellectual property law; competition and consumer protection law; advertising and sales promotion law; real estate and public procurement. Our team is composed of 60 lawyers.

Top positions awarded to the Law Firm in domestic and foreign rankings, including *Chambers & Partners* 2019, further attest to its reputation. We have a base of over 100 regular clients, including Polish businesses and multinational corporations. The Law Firm also acts as a regular expert for numerous commercial chambers (Polish Chamber of Insurance [PIU], Polish Chamber of Information Technology and Telecommunications [PIIT], Foundation for the Development of Non-cash Payments [FROB], Union of Employers in the Internet Sector [IAB]).

Our lawyers have authored more than 200 academic publications, including books and monographs concerning mostly FinTech law, civil law, intellectual property law, new technologies law, advertising law and pharmaceutical law.

Portugal

Pedro Ferreira Malaquias



Hélder Frias



Uría Menéndez – Proença de Carvalho

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Although the FinTech market in Portugal is maturing, with more and more FinTech-related initiatives, businesses, events and non-profit organisations emerging in the market, the data regarding its players and numbers is still very fragmented and inaccurate.

According to public sources, the largest segments of the Portuguese FinTech market are digital payments, alternative financing and crypto and blockchain. However, there are also relevant players in other FinTech segments in Portugal, such as personal finance management, mobile-first banks, RegTech, etc. As for crowdfunding, the legal framework applicable to equity-based and lending-based crowdfunding activities entered into force on 10 February 2018.

Lastly, the Portuguese Government, the supervisory and regulatory authorities of the financial sector and the private sector have been very committed to supporting the emerging start-up ecosystem in Portugal. Lisbon being the host city of the annual Web Summit since 2016 (and scheduled to remain in Lisbon until 2028) and initiatives such as incumbents' accelerators, SIBS API Market, the Portuguese Government's tech programs and the Lisbon Investment Summit, just to name a few, are a clear testimony of this commitment.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

As a general rule, there are no FinTech businesses prohibited or restricted in Portugal *per se*. Nonetheless, FinTech businesses that provide regulated financial services, such as payments, deposit-taking, investment, advisory and management, insurance, or other regulated activities are subject to the general regulatory regime that applies to any company providing those services in the Portuguese market.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

New and growing businesses may fund their activity in different ways, including both traditional (e.g. banks and IPOs in Alternext) and more *avant-garde* (e.g. business angels, venture capital firms, incubators, etc.) sources, and both in the form of equity and debt.

Additionally, the Portuguese Government launched in the last few years several initiatives with the aim of offering alternatives to traditional sources of funding to start-ups in general, including FinTech businesses. Those initiatives range from (i) the funding of daily expenses of entrepreneurs, (ii) the funding of the acquisition of professional incubation services, (iii) sponsoring the participation of start-ups in international events, and (iv) to investment (through Portugal Ventures, which is the body responsible for public venture capital investment) and co-investment (with business angels and venture capital firms) schemes.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

The Portuguese tax framework includes tax benefits regarding investments in tech/FinTech businesses and in small and medium sized businesses ("SMEs") and venture capital investment. These tax benefits may apply at the level of the investors and/or at the level of the FinTech business.

At the level of the FinTech business, provided that certain conditions are met (e.g. taxable income not higher than EUR 200,000) and the company qualifies as a micro-entity, a simplified corporate income tax ("CIT") regime may apply, according to which the taxable income is determined through the application of a coefficient which ranges from 0.04 to 1 (e.g. 0.1 on the income deriving from supplies of services, 0.75 on income deriving from professional activities established for personal income tax purposes and 0.95 on the income deriving from the assignment of industrial property ("IP") rights).

SMEs benefit from a reduced CIT rate of 17% on the taxable income up to EUR 15,000, being the exceeding income subject to the general 21% rate.

Furthermore, SMEs may also be granted with CIT credits corresponding to 10% of retained earnings up to an amount of EUR 10 million, which are reinvested in eligible investments in the three tax years following the tax year in which the earnings were retained. The CIT credits are capped to 50% of the CIT due by the relevant company.

Companies that develop certain IP rights (independently or by subcontracting) and obtain income from the assignment of the temporary use of said IP rights are entitled to consider only 50% of the respective income for the purposes of assessing its taxable income. This benefit only applies if the assignee is not resident in a listed tax haven, uses the IP rights in a commercial, industrial or rural activity, and the results obtained by the assignee do not consist of the delivery of goods or supplies of services that create deductible costs at the level of the company that developed the IP rights or any related company.

There is a specific tax regime to support investment, which offers specific CIT credits to companies with activities in data processing, computing, information technologies, media and telecommunications. In this regard, provided that certain conditions are met and depending on the region of the Portuguese territory in which the eligible investments are made, companies investing in fixed tangible and intangible assets (e.g. patents, licences, know-how) may be granted CIT credits in an amount of 10% or 25% of investments up to EUR 15 million, and up to an amount of 10% of the investment amounts exceeding EUR 15 million. This deduction is capped to 50% of the CIT due in each tax year, and in certain cases, there may be no cap to the deduction with reference to investments made in the first three years of activity. Other real estate transfer tax, real estate tax and stamp tax exemptions may apply.

Companies may also be granted a notional CIT deduction of the company's taxable income, which corresponds to 7% of the amount of share capital contributed in cash by shareholders, or that resulted from the conversion of credits into share capital.

Finally, a programme called "Semente" ("Seed") is also available in order to encourage individuals investing in start-ups. According to this regime, and provided that certain conditions are met, an individual may be granted with a personal income tax credit ranging between EUR 2,500 and EUR 25,000, depending on the amount invested in the relevant start-up. The credit is deducted up to an amount of 40% of the personal income tax due by the investor.

A special tax regime also applies to venture capital investment funds. Under this regime, the income derived by the fund is exempt from CIT, while the income obtained by resident entities with holding participation units is generally subject to withholding tax at a 10% rate, and exempt in case of non-resident unit holders (unless the non-resident unit holder is resident in a listed tax haven, in which case the 10% rate applies).

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

The listing of securities on a regulated market operating in Portugal requires the approval of the Portuguese Securities Market Commission, as well as the respective market management entity (Euronext Lisbon), for which certain conditions must be met (e.g. publication of a prospectus).

In addition, Euronext Lisbon regulations require that adequate clearing and settlement systems are available in respect of transactions in the shares. The listing requirements applicable to the trading of shares in Alternext are more simple and flexible. While the procedural and documentation requirements are not very

different from those applicable to the listing on Euronext Lisbon, the admission to trading on this MTF may be requested provided that shares representing at least EUR 2.5 million are placed with a minimum number of three investors (which must not be related parties to the issuer), through either a public offering or a private placement of the shares. Accordingly, the issuer requesting the admission to the trading of shares on Alternext may not only benefit from the possibility of not having to prepare and register a prospectus with the Portuguese Securities Market Commission, but will always be waived from complying with requirements related to any minimum mandatory free float (as a percentage of the company's share capital).

Lastly, foreign issuers intending to list shares on a regulated market operating in Portugal may be subject to additional requirements (for example: public offer and listing prospectuses must be drawn up in a language accepted by the Portuguese Securities Market Commission; the Portuguese Securities Market Commission may ask for a legal opinion attesting the satisfaction of the general eligibility criteria concerning the shares and the valid existence of the issuer in accordance with its governing law; or the foreign issuer must appoint a financial intermediary for liaising with the market where the securities will be admitted to trading).

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

Yes. Raize successfully completed its IPO in July 2018.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

FinTech as such is not subject to a specific legal framework in Portugal. The only exception is crowdfunding.

Indeed, access to the crowdfunding activity, its supervision, the platforms, the beneficiaries, the investors, and the obligations, rights and formalities applicable to the relationships between all those parties are governed by: Law no. 102/2015, of 24 August; Law no. 3/2018, of 9 February; the Ministerial Order no. 344/2015, of 12 October; and the Portuguese Securities Market Commission's Regulation no. 1/2016, of 25 May. This legal framework regulates four types of crowdfunding: (i) donation-based; (ii) reward-based; (iii) lending-based; and (iv) equity-based. Donation-based and reward-based crowdfunding platforms must notify the Consumer General Directorate ("Direção-Geral do Consumidor") prior to starting their business, and equity-based and lending-based crowdfunding platforms must register with the Portuguese Securities Market Commission and are subject to the latter's supervision and regulations. It should be noted that the legal framework applicable to equity-based and lending-based crowdfunding activities only entered into force on 10 February 2018. The platforms may not provide investment advice or recommendations, as well as manage investment funds or hold securities. In addition, crowdfunding platforms are subject to investment, capital, conduct, compliance and organisation restrictions and strict information duties.

Nevertheless, as mentioned, if any FinTech business carries out a regulated activity, it will need to first obtain the necessary authorisation and/or registration with the competent regulatory authority(ies).

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

In Portugal, there are no specific regulations specifically directed at virtual currencies or the players in the virtual currencies market, such as virtual currency exchanges, virtual currency wallets, virtual currency miners or virtual currency issuers (virtual currency operators). This does not mean that virtual currencies or virtual currency operators are by all means unregulated. A case-by-case assessment in light of the specific characteristics of the relevant virtual currency or of the relevant virtual currency operator and the activities carried out by the latter in light of the existing legal and regulatory framework is required to reach any conclusions on whether the aforementioned activities constitute or not the pursuit of a regulated activity within the Portuguese territory.

The Portuguese regulatory and supervisory authorities of the financial sector have been alert to the virtual currencies phenomenon and have issued press releases highlighting the risks and uncertainties regarding virtual currencies and initial coin offerings (“ICOs”).

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

Yes. The Portuguese Government has been very committed to supporting the emerging start-up ecosystem in Portugal in general, including FinTech. The new agreement between the Portuguese Government and the Web Summit for at least 10 more years provides just part of the momentum. In 2017, the Portuguese Government launched the “StartUp Portugal Programme”, a four-year plan which focuses on three areas of operation: (i) ecosystem; (ii) funding; and (iii) internationalisation. This programme comprises initiatives of different spectrums, including the creation of a national network of incubators, fabrication laboratories (“FabLabs”) and makerspaces (“Makers”), the establishment of a free-zone for technology (promoting research, testing and creation of cutting-edge technologies), funding schemes (cash and services), a more favourable tax and social security regime for certain start-ups, and the support of the internationalisation of start-ups.

Portugal has no sandbox options for FinTechs. However, in September 2018, the Portuguese regulatory and supervisory authorities of the financial sector and the Portugal Fintech association have launched Portugal FinLab, an innovation hub whose purpose is to support the development of innovative solutions in FinTech and related areas through cooperation and mutual understanding.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

As stated above, FinTech refers to a large heterogeneous group of businesses. Therefore, depending on the solutions and the business model used by the relevant FinTech business, and the type of services it provides and its jurisdiction, there can be one of three scenarios:

- A FinTech business established in an EU jurisdiction and wishing to provide its services, which are subject to a specific regulatory framework, in Portugal: assuming that the

FinTech business is duly registered in its EU Home State for the purpose of providing the relevant financial services, it may provide, market or promote its services in Portugal pursuant to either the freedom to provide services, or the establishment of a branch in the Portuguese territory. Furthermore, the FinTech business must comply with general terms of law, including, but not limited to: legislation governing marketing materials; data protection; and consumers’ and employees’ protection, etc.

- A FinTech business established outside of the EU and wishing to provide its services, which are subject to a specific regulatory framework, in Portugal: the FinTech business may not provide, market or promote its services to customers in Portugal, including online (either via a website or by email), unless it has obtained the licence, authorisation, registration or approval required to provide the relevant regulated services. Furthermore, the FinTech business must comply with the general terms of law, including, but not limited to: legislation governing marketing materials; data protection; and consumers’ and employees’ protection, etc.
- A FinTech business established outside Portugal and wishing to provide its services, which are not subject to a specific regulatory framework, in Portugal: apart from having to comply with general terms of law, including, but not limited to: legislation governing marketing materials; data protection; and consumers’ and employees’ protection, etc. As the FinTech business is not carrying on a regulated activity, it does not have to comply with any specific regulatory framework. Furthermore, from a tax perspective, depending on the structure under which the activities are being performed in Portugal, a permanent establishment may be deemed to exist.

In this case, the tax authorities may allocate profits to the permanent establishment and tax under the general corporate income tax provisions.

The pursuit of regulated activities within the Portuguese territory by a non-authorised entity is deemed as a serious administrative offence subject to heavy fines, plus ancillary sanctions.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

The legal framework for the protection of personal data in Portugal is regulated by the Lisbon Treaty, the Charter of Fundamental Rights of the European Union, article 35 of the Portuguese Constitution, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) (“GDPR”), which repeals Directive 95/46/EC and, until approval of a new data protection law which provides for local rules and administrative proceedings adapted to the GDPR, the provisions of Law no. 67/98 of 26 October that transposed Directive 95/46/EC (the “Data Protection Law”) into the Portuguese legal system which do not contravene the GDPR. The new draft data protection law (the “Draft Bill”) is currently under discussion in the Portuguese Parliament and its approval is expected during the course of 2019.

In addition to this, the provisions regarding the protection of personal data in the context of Law no. 41/2004 of 18 August on the protection and processing of personal data in e-communications, as amended by Law no. 46/2012 of 29 August, which transposed Directive 2009/136/EC, also contains relevant rules regarding the sending of

unrequested communications for direct marketing purposes. On this topic, the European Commission also proposed in January 2017 a draft Regulation, which is currently under discussion, with the main objectives of replacing and modernising the applicable rules of privacy in electronic communications, adapting it to the current technical developments and accommodating it to the provisions of the GDPR, thus contributing to the reinforcement of consumers' trust in the Single Digital Market.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

The application of the Data Protection Law for foreign organisations is triggered by either the existence of a data processor or processing equipment in Portugal or, according to ECJ's decision on Google Spain (case C-131/12), the existence of an establishment in Portugal, the activity of which is inextricably linked to that of the foreign organisation. After the GDPR rules became applicable, the extraterritorial applicability of EU data protection legal framework is reinforced as a result of the GDPR's territorial scope rules under article 3.2 of the GDPR. Moreover, the GDPR's regime on international transfers is the only regime that currently applies to data transfers in Portugal.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

The GDPR sets forth that failure to comply with its main provisions can lead to fines of up to EUR 20 million or 4% of the global annual turnover for the preceding financial year, whichever is the greater.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

Yes, Law no. 109/2009 of 15 September implemented the European Council Convention on Cybercrime and the Council Framework Decision 2005/222/JHA on attacks against information systems. In addition, Law no. 41/2004 of 18 August, amended by Law no. 46/2012 of 29 August, contains a specific obligation for companies providing publicly available electronic communication services to promptly notify the Portuguese Data Protection Authority upon the occurrence of a personal data breach. Whenever the breach may adversely affect the personal data of users or subscribers (i.e. when it results, *inter alia*, in identity fraud, physical harm, significant humiliation or reputational damages), companies must also, without undue delay, notify the subscribers or the users of the breach so the latter can take the necessary precautions. The obligation of data breach notification now applies to all companies by virtue of the GDPR under the rules set forth therein.

Moreover, the provisions of the GDPR regarding the obligation of data controllers to implement appropriate technical and organisational measures to ensure a level of security appropriate to a risk, and to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and against all other unlawful forms of processing, should also be considered when dealing with cybersecurity issues in the context of personal data. In Portugal, there is no mandatory list of security measures to be implemented.

Finally, the approval of Directive (EU) 2016/1148 concerning measures for a highly common level of security of network and information systems across the EU (the "NIS Directive") on 6 July 2016, which was transposed into national law by Law no. 46/2018 of 13 August, together with the GDPR, is one of the most important pieces of legislation in the context of cybersecurity.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

Directives 2015/849/EU of the European Parliament, and of the Council of 20 May 2015, and 2016/2258/EU of the European Parliament and of the Council of 6 December 2016, on the prevention of the use of the financial system for the purpose of AML/CFT and on the access to anti-money laundering information by tax authorities, were implemented into Portugal by means of Law no. 83/2017 of 18 August, and of Law no. 89/2017 of 21 August ("AML Legal Framework"). This AML Legal Framework is applicable to a very significant set of institutions providing financial services in Portugal, including both institutions incorporated in Portugal and institutions acting through a branch in Portugal.

As to financial crimes, the Portuguese Criminal Code (Decree-Law no. 48/95) sets out that legal persons (e.g. companies) may be liable for certain criminal offences – identified in a closed catalogue (which comprises several financial crimes, such as embezzlement, counterfeiting of currency, money laundering, corruption, illegal taking of deposits and other repayable funds, insider trading, market manipulation, etc.) in case certain legal requirements are met.

Considering that the penalty of imprisonment cannot be applied to a legal person, the latter may be subject to the payment of heavy fines or even to its winding up, plus ancillary sanctions.

In this regard, it is worth mentioning that the Portuguese legal framework applicable to equity-based and lending-based crowdfunding platforms sets forth that these platforms must adopt written policies and procedures that are adequate and effective to prevent fraud, money laundering and financing of terrorism, and that they must make such policies available on the platform's website.

The recently enacted fifth AML Directive addresses specific risks associated with virtual currencies, aiming at bringing more transparency to the virtual currencies sector across the EU. Member States must implement this Directive by 10 January 2020. Portugal has not yet implemented it.

From a virtual currencies perspective, it is also worth noting that entities subject to the Portuguese framework on AML/CFT must pay special attention to the AML/CFT risks that: may derive from offering products or transactions likely to favour anonymity; may derive from developing new products and new commercial practices, including new distribution mechanisms and new payment methods; and that use new technologies, or technologies under development, both for new products and existing ones. Besides stricter risk management requirements being applicable, there are also additional KYC and KYT requirements that must be complied with in transactions involving any of these products or technologies.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

FinTech businesses cover a vast range of activities; thus, a case-by-case assessment is imperative. In any case, taking into account the overall picture of the FinTech ecosystem in Portugal, we would say

that the legislation more often put to the test is: (a) the Portuguese Banking Law; (b) the payment services act (Decree-Law no. 91/2018); (c) the consumer credit regime (Decree-Law no. 133/2009); (d) the Portuguese Securities Code (Decree-Law no. 486/99); (e) the distance marketing and conclusion of consumer services act (Decree-Law no. 95/2006, for financial services in particular, and Decree-Law no. 24/2014); (f) the data protection legal framework (Regulation (EU) no. 2016/679); (g) the electronic identification legal framework (Decree-Law no. 290-D/99, of 2 August, and Regulation (EU) no. 910/2014); (h) the unfair terms act (Decree-Law no. 446/85); (i) the e-commerce act (Decree-Law no. 7/2004); and (j) any other consumer-protection regimes.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

Under Portuguese law, there are two main types of employment agreements: employment agreements subject to a defined term (which may be fixed or unfixed); and employment agreements without term (open-ended agreements).

In addition, there are also several specific employment agreements governing particular activities, such as professional sportsmen, domestic work, temporary agency work and employment agreements on service commission.

As per the Labour Code, employers may only validly terminate open-ended employment agreements by means of: (i) mutual agreement; (ii) termination during the trial period; (iii) permanent and absolute incapacity of the employee or the employer to render or receive the work; (iv) total and permanent closure of the company; (v) fair dismissal; (vi) collective dismissal; (vii) termination of the work position; (viii) inability of the employee to adapt; (ix) desertion of the employee; or (x) retirement for age or disability.

Term employment agreements, on the other hand, may be terminated under the general rules applicable to open-ended employment agreements and at the end of the relevant term.

In view of the above, save for certain exceptional situations, employers may only unilaterally terminate open-ended employment agreements on disciplinary grounds (which require, among other aspects, a very serious breach of the employees' duties) or with recourse to redundancy procedures, which imply the existence of objective reasons and the payment of severance compensations. In both situations, somewhat complex legal procedures are required to be followed.

5.2 What, if any, mandatory employment benefits must be provided to staff?

The minimum national monthly wage for the private sector in 2019 is EUR 600. All employees working on a full-time basis, regardless of their citizenship, are entitled to it (in the islands of Madeira and Azores the minimum wage for 2019 is EUR 615 and EUR 630, respectively).

Furthermore, collective bargaining agreements usually set forth the minimum remuneration scale that has to be paid to employees rendering duties inherent to the professional categories established therein.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

European Union Citizens:

EU citizens may work in Portugal without a work permit. Nonetheless, certain formalities may have to be observed, depending on the duration of their stay and the nature of the activity.

Non-European Union Citizens:

Most non-EU citizens who intend to enter Portugal must hold a recognised travel document that must be valid for at least three months more than the expected duration of their visit (for example, a valid passport) and must hold a valid visa that is appropriate for the purpose of their visit.

There is no special route for obtaining permission for individuals who wish to work for FinTech businesses.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

The main Portuguese legal framework for industrial property rights is found in the new Industrial Property Code ("*Código da Propriedade Industrial*", the "CPI"), as recently approved by Decree-Law no. 110/2018 of 10 December, which repeals the prior existing CPI as approved by Decree-Law no. 36/2003 of 5 March, and implements the Trademark Directive and the Trade Secrets Directive.

The CPI includes the main legal provisions regarding invention patents, utility models (with a lower inventive rank than patents), registered designs and trademarks and now also includes the legal framework regarding the protection of trade secrets and know-how applicable in Portugal.

According to the CPI, any inventions may be the subject matter of patent protection, provided that they are new, inventive and have industrial application. It is further established that, if the above requirements are met, patent protection may be granted either for a process or a product, in any field of technology. The CPI expressly excludes from patent protection, amongst other matters, simple discoveries, scientific theories and mathematical methods. This means that software is subject to protection by copyright and not a patent, unless the software in question is part of a process subject to patent protection *per se* (so-called computer-implemented inventions).

As concerns the duration of the indicated rights, Portuguese patents enjoy protection for 20 years as of the application date, and utility models are registered for a maximum period of 10 years as of the application date. Following these periods, inventions will enter the public domain and may be used freely by any person.

Trade secrets are now regulated in the CPI. Under the new legal framework, trade secrets benefit, with some adaptations, from the civil enforcement procedures and measures provided for industrial property rights, and there are specific rules of preservation of confidentiality of trade secrets in the course of legal proceedings.

The CPI also sets forth other industrial property rights which, depending on the purpose, may also be relevant for FinTech businesses, such as trademarks. In order for a certain commercial symbol to become a trademark, it must be distinctive and capable of

being graphically represented. Trademark registrations have a duration of 10 years as of the application date and may be indefinitely renewed for identical periods of time.

On the other hand, the Portuguese Code of Copyright and Related Rights (“*Código do Direito de Autor e Direitos Conexos*”, the “CDADC”) is applicable to intellectual creations in the literary, scientific and artistic fields which are original and exteriorised in some way. Copyright covers both moral and patrimonial rights of the authors and shall be recognised independently of registration, filing or any other formality. Copyright exists from the moment the work is created. As a general rule, patrimonial rights shall lapse 70 years after the death of the author of the work, even in the case of works disclosed or published posthumously.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

The CPI specifically establishes that in order to be protected, an industrial property right (i.e. patents, utility models, designs and trademarks) must be registered either at a national, European or international level. Protection is granted generally on a first-to-file basis. The registration process is different depending on the industrial property right in question.

For patents and utility models, the ownership rules are as follows:

- i. General rule: the right to the patent shall belong to the inventor or his successors in title. If two or more persons have made an invention, any of them may apply for a patent on behalf of all the parties.
- ii. Special rules: if an invention was made during the performance of an employment contract in which inventive activity is provided for, the right to the patent belongs to the company. In this case, if the inventive activity is not especially remunerated, the inventor is entitled to remuneration in accordance with the importance of the invention. Also, if an invention is part of the employee’s activity, the company has a pre-emptive right to the patent in return for remuneration in accordance with the relevance and importance of the invention; it may also assume ownership or reserve the right to its exclusive exploitation, the acquisition of the patent or the ability to apply for or acquire a foreign patent.

For copyrights and related rights, the ownership rules are as follows:

- i. General rule: copyright shall belong to the intellectual creator of the work.
- ii. Special rules:
 - a) ownership of copyright in a work carried out on commission or on behalf of another person, either in fulfilment of official duties or under an employment contract, shall be determined in accordance with the relevant agreement. In the absence of any agreement, it shall be deemed that ownership of copyright in a work carried out on behalf of another person belongs to the intellectual creator. However, where the name of the creator is not mentioned in the work or is not shown in the customary place, it shall be deemed that the copyright remains the property of the person or entity on whose behalf the work is carried out; and
 - b) in the event of joint co-authors, either: (1) all co-authors have equal exploitation rights, unless otherwise stipulated; or (2) where a work of joint authorship is disclosed or published solely in the name of one or several of the authors, in the absence of any explicit indication by the remaining authors regarding some part of the work, it shall be presumed that the authors not mentioned have assigned their rights to the author or authors in whose name the work has been disclosed or published.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

Under Portuguese rules, industrial property rights (i.e. patents, utility models, designs, trademarks, trade secrets) are locally applicable rights, only enjoying protection in the country in which they were registered. For trademarks, the European Community and international registration systems allow the possibility of including a large number of countries within the scope of the trademark protection: the former to the 28 Member States of the EU; and the latter to the countries that form the Madrid Union.

As for patents, filing a European or international patent application allows the extension of protection of an invention to a large number of countries: a European patent is valid in the countries that are signatories to the Munich Convention; and an international patent is valid in the countries that are signatories to the Patent Cooperation Treaty.

Apart from registered rights, protection is also granted to specific, unregistered rights, including: (a) well-known and reputed trademarks and tradenames, which are protected from unauthorised use by third parties that might take unfair advantage of their reputation or affect their distinctive character (in accordance with article 6 *bis* of the Paris Convention for the Protection of Industrial Property); (b) non-registered European Union designs (if they have already been marketed in the European Union), which are protected for a period of three years following the date on which the design was first made available to the public within the territory of the European Union (following which the protection cannot be extended); and (c) know-how and business information (trade secrets) now benefit, under the new rules of the CPI, of a specific enforcement framework (similar to the one applicable to the registered industrial property rights) which facilitates its protection.

As concerns copyright and related rights, given the fact that they do not require registration to be valid and only depend on their exteriorisation, there is no formal recognition procedure. The Portuguese rules apply to Portuguese authors, but also to nationals of third countries who reside in Portugal. Also, works by foreign authors, or authors with a foreign country as their country of origin, shall enjoy the protection granted by Portuguese law, subject to reciprocity, and with the exception of any international convention to the contrary of which the Portuguese State may be bound. Additionally, works published for the first time in Portugal and where Portugal is the country of origin of the author of unpublished works shall enjoy protection under the CDADC.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

Exploitation of industrial property rights can occur either directly by their owner or through a full or partial licence granted to third parties. Licence contracts must be drawn up in writing and unless otherwise expressly stipulated, the licence shall be understood to be non-exclusive. Also, in order for a licence to have *erga omnes* effects it must be registered at the National Institute of Industrial Property (otherwise it will only have *inter partes* effects).

As regards copyright and related rights, the CDADC grants the author an exclusive right to enjoy and use his/her work, either in whole or in part, including, in particular, the right to disclose, publish and exploit it economically in any direct or indirect form within the limitations of the law. The powers related to the

administration of copyright may be exercised by the owner of the copyright himself or through his/her duly authorised representative (which are generally national or foreign associations specifically established for the administration of a large amount of owners of copyright). As in other jurisdictions, exploitation rights are limited by a number of exceptions that allow the general public, or certain beneficiaries, to make specific, free use of the work without requiring permission from the author. In such cases, the author will not receive any remuneration, unless equitable compensation of some kind is deemed to be appropriate.

Acknowledgments

The authors would like to acknowledge the assistance of their colleagues Joana Mota (*Principal Associate*) and Luís Alves Dias (*Senior Associate*) in the preparation of this chapter.

Joana Mota joined Uría Menéndez as a Junior Associate in February 2012 and became a Principal Associate in 2018. Joana focuses her

practice on the acquisition, protection and maintenance of national and international IP rights and has represented parties in related litigation proceedings. She has also advised companies on personal data protection issues. Joana has a postgraduate qualification in IP law, taught by the Portuguese Association of Intellectual Property Law in conjunction with the Faculty of Law of the Universidade de Lisboa. She also has an advanced qualification in data protection law from the Universidade de Lisboa.

Luís Alves Dias is a Senior Associate in the Lisbon office of Uría Menéndez-Proença de Carvalho, having joined the firm in December 2015. His professional practice is mainly focused on providing legal advice to domestic and international clients regarding banking and finance law, FinTech and insurance law in both the regulatory and the purely transactional strands. Luís is a founding associate of the Portuguese FinTech and InsurTech Association (“AFIP”), co-coordinator of the RegTech Working Group of AFIP and co-founder of the Lisbon chapter of Legal Hackers.



Pedro Ferreira Malaquias

Uría Menéndez – Proença de Carvalho
Praça Marquês de Pombal, 12
1250-162 Lisboa
Portugal

Tel: +351 21030 8600
Email: ferreira.malaquias@uria.com
URL: www.uria.com

Pedro Ferreira Malaquias (*Partner*) joined Uría Menéndez in 2004 when Vasconcelos, F. Sá Carneiro, Fontes & Associados – one of the most prestigious Portuguese law firms – integrated with Uría Menéndez and has been a Partner of the firm since then. He currently heads the Finance Department in Portugal and is responsible for the areas of banking and insurance.

Pedro focuses on banking, restructuring and insurance law and has over 20 years of experience in:

Banking: advice on all legal aspects related to retail and investment banks, including loans, credit facilities, guarantees, commercial paper and structured finance.

Securities: advice on diverse areas of securities law, including financial intermediation, markets, settlement procedures, cross-border services, venture capital, and securities and bond issues. Legal advice on products such as repos, securities lending, derivative and transactions.

Restructurings: advice on corporate and debt restructuring transactions across various sectors.

Insurance: negotiation of insurance contracts on project finance and structured finance transactions, due diligences within the insurance field, advice on financial products and regulatory and supervision issues.

Since 1998, Pedro has worked as a legal consultant for the Portuguese Banking Association, and acts as their representative on the Legal Committee and on the Retail’s Committee of the European Banking Federation.



Hélder Frias

Uría Menéndez – Proença de Carvalho
Praça Marquês de Pombal, 12
1250-162 Lisboa
Portugal

Tel: +351 21030 8600
Email: helder.frias@uria.com
URL: www.uria.com

Hélder Frias joined the firm in 2006 and is a *Counsel* of the Banking, Finance and Insurance department. From September 2010 to August 2011, he was based in our London office.

Hélder has over 12 years of experience advising Portuguese and foreign clients on M&A transactions of financial institutions, bank assurance alliances and insurance portfolio transfers, as well as on other regulatory matters related to these markets, including the intermediation activity.

Hélder frequently advises on regulatory and supervisory aspects of financial and insurance activities (including banking and financial intermediation services and payment services), such as lending, creation of security, factoring, sale and purchase of receivables, money laundering, venture capital and financial products and investment and retail banking and insurance instruments (capital redemption transactions and unit-linked life insurance agreements).



Uría Menéndez is the leading law firm in the Ibero-American market. We have almost 600 lawyers working in 14 different offices located in the most important financial centres in Europe, the Americas and Asia.

Uría Menéndez lawyers’ extensive experience and comprehensive knowledge of their clients’ industries allow the firm to offer added-value advice in all areas of business and find innovative technical solutions to the most complex legal issues. In addition, through its network of best friends in Europe, Uría Menéndez is able to create cross-firm teams with the leading firms from France (Bredin Prat), Germany (Hengeler Mueller), Italy (BonelliErede), the Netherlands (De Brauw Blackstone Westbroek) and the United Kingdom (Slaughter and May). Uría Menéndez is also a member of renowned international associations such as Lex Mundi.

Furthermore, in January 2015, after more than 20 years working in the region, the firm took a ground-breaking step in creating the first Latin-American integration between leading local firms (Philippi in Chile, and Prietocarrizosa in Colombia): Philippi, Prietocarrizosa & Uría (“PPU”), the first major Ibero-American firm. After an excellent first year, in January 2016 the firm integrated two Peruvian firms, Estudio Ferrero Abogados and Delmar Ugarte, becoming Philippi Prietocarrizosa Ferrero DU & Uría. The opening of a Peru office consolidates PPU’s position and confirms its status as a leading firm in the Pacific Alliance (Chile, Colombia, Mexico and Peru) as it is fast becoming a preeminent firm in Latin America.

Russia

Maxim Mezentsev



Nikita Iovenko



QUORUS GmbH

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

The representatives of Russian business, as well as Russian state authorities, have recently been paying a lot of attention to the stable and rapid development of the fintech sector. Furthermore, at the beginning of 2018, the Central Bank of Russia (hereinafter – the Central Bank) published a document stating the main directions of fintech development in Russia for the years 2018–2020. According to the position of the Central Bank, the following sectors deserve primary attention:

- big data and information analysis;
- artificial intelligence;
- robotisation;
- biometrics;
- distributed ledgers (as well as blockchain technology); and
- cloud technologies.

Russia currently occupies one of the leading positions in the world with respect to the level of fintech involvement in people's lives. The most popular services are related to payments and money transfers, while the volume of such operations increased by 47% in the year 2016. Such a quick growth is caused by the development of banking (Tinkoff Bank, Alfa Bank) and non-banking (QIWI wallet, Yandex Money) platforms. Moreover, services like Master Card PayPass, Visa PayWave, Apple Pay and Samsung Pay have also developed very fast in Russia – contactless technologies and NFC may be used nowadays for payment almost everywhere.

The Russian fintech market now has several innovation projects using the newest technologies in different areas. Some examples of the most successful Russian fintech startups and companies are, among others: VisionLabs; Telegram; Waves Platform; Tinkoff Bank; and Rocket Bank. A big impact on the development of the fintech sector in Russia is made by the largest national technological company, Yandex.

Furthermore, according to the statistics provided by the Central Bank, the level of fintech involvement is the highest in the following fields:

- payments and money transfers (online payments, online money transfers, P2P currency exchange, B2B payments and transfers, cloud cash registers and smart terminals);
- financing (P2P consumer crediting, P2P business crediting, and crowdfunding); and

- capital management (robo-advising, programs and applications on financial planning, social trading, algorithmic exchange trading, and special purpose savings, etc.).

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

Due to the fact that fintech development has accelerated just over the last few years, there are many aspects that are still not regulated by Russian law. This is why we are unable to state that some types of fintech business are prohibited. Of course, there are several general limitations, related to anti-money laundering and terrorism financing. For example, according to the position of the Russian authorities, transactions related to cryptocurrency may be suspected as being used for covering operations aimed at money laundering and terrorism financing. For this particular reason, and due to the fact that the status of cryptocurrency is not still defined in any legal acts, the authorities warn citizens against their participation in such risky operations.

In Russia, it would be more correct to say that many types of fintech still remain unregulated (cryptocurrency, blockchain technology, crowdfunding, P2P crediting, etc.). Furthermore, according to the draft laws elaborated jointly by the Ministry of Finance and the Central Bank, cryptocurrency or tokens will not be recognised as a lawful means of payment in Russia (will not be ranked *pari passu* with fiat currency – the rouble).

As mentioned above, the position of the authorities allows us to state that the use of cryptocurrency as a legal means of payment for ordinary goods will not be widely allowed (as far as we know, some countries have already allowed the use of cryptocurrency for common payments).

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

Russian legislation covering the issues related to the funding of companies, namely the Federal Law dated February 2, 1998 No. 14-FZ “On Limited Liability Companies” and the Federal Law dated December 26, 1995 No. 208-FZ “On Joint-Stock Companies”, prescribe both types of funding – debt and equity.

Equity funding may be performed in the following forms:

- use of the company's net income; and
- issue and offering of shares.

The opportunities of debt funding are the following:

- credits and loans received from banks and other financial institutions;
- issue of bonds;
- funds borrowed from other companies or private persons; and
- budgetary funding.

Furthermore, according to the abovementioned laws, the shareholders of the companies (LLC as well as JSC) are authorised to make gratuitous contributions aimed at financing the current activities of the company. Such contributions do not increase the amount of the company's charter capital and the nominal value of the shares (but do increase the company's net assets value).

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

Russian fintech businesses may enjoy incentive schemes prescribed by law aimed at the stimulation and facilitation of foreign and national investments. For example, special clusters and technological centres created in different regions of the country (one of the most known is Skolkovo) provide startups and small/medium-sized businesses in the sphere of fintech with special tax exemptions or privileges. The government is also entitled to offer grants for the development of projects.

Furthermore, according to the Federal Law dated July 9, 1999 No. 160-FZ "On foreign investments in the Russian Federation", some basic guarantees are provided to foreign investors, including, but not limited to:

- legal protection of the investor's activity in Russia;
- right to freely dispose of the income which is received in Russia; and
- guarantee from a negative change of the legislation.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

First of all, it should be noted that, according to the applicable legislation, there are two different forms of joint-stock companies in Russia: non-public and public ones. A non-public company may receive the status of a public company if it takes a decision to make an IPO and list its securities on a stock exchange.

An IPO in Russia may be structured in one of the following ways:

- additional issue of securities and its use for IPO – primary placement;
- public offer of shares that are already issued and owned by its shareholders – secondary placement; or
- a combination of the two previous options.

The IPOs on the Russian equity market usually include both primary and secondary placements.

To access the exchange and be admitted for public offering, a company should comply with the basic listing requirements:

- compliance of the securities with the obligatory rules of the Russian legislation, namely with the requirements of the Federal Law dated April 22, 1996 No. 39-FZ "On Securities Market", as well as the absence of factors that may impede the listing procedure;
- disclosure of all necessary information about the issuer and the securities to the Central Bank of Russia (financial markets regulator);

- acceptance of the securities for servicing by the settlement depository; and
- registration of the securities prospectus (a document containing all information about the issuer and listed securities) with the Central Bank.

The shares of foreign companies may be admitted for initial placement at a Russian exchange on the basis of a decision of the Central Bank of Russia. It should be further noted that, according to the listing rules adopted by the Moscow Exchange (MOEX), there are several additional requirements with respect to foreign securities in order to be admitted for listing on MOEX:

- the securities should have an international securities identification number (ISIN) and a Classification of Financial Instruments (CFI) code, assigned by one of the national numbering agencies which is a member of the Association of National Numbering Agencies (ANNA);
- the issuer of the securities: (a) is established in a country – a member of the OECD, a member or observer of FATF, a member of MONEYVAL, or the Single Economic Area; or (b) is established in a country with which the Central Bank of Russia has an effective agreement on cooperation; or (c) has already issued securities that are listed on an approved exchange (the list of such exchanges is prepared and updated by the Central Bank); and
- the rights to the foreign securities are recorded by a Russian depository on a special account.

Once the abovementioned requirements are met by the issuer, the securities are approved for listings.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

The case of **Tinkoff Bank**, who provides to its clients a full line of banking products and executes all operations online without any single branch, is a good example of fintech development in the Russian banking sector. The IPO of Tinkoff Bank took place in 2013 and gained around USD 1,087 billion.

In October 2017, the Russian companies group QIWI bought two fintech companies – Rocket Bank and Tochka Bank – that previously pertained to the Russian group Otkritie Holding. These virtual banks, as well as Tinkoff Bank, provide their clients with online banking services.

Furthermore, two companies, originating from Russia, made their exits via ICO. Since it is still impossible to make a lawful ICO in Russia, these offerings were performed in foreign jurisdictions.

- Pavel Durov, the founder and creator of the popular messenger **Telegram**, published at the end of the year 2017 information about his intentions to launch the project "Telegram Open Network" (a new distributed ledger based on blockchain technology) as well as new tokens – Gram. The first round of Telegram's preliminary ICO made between the major shareholders of the company took place in January 2018 and has already gained USD 850 million. On March 30, 2018, the company announced the results of the second stage ICO – a further USD 850 million was raised. Ninety-four investors participated in this investment stage.
- **Waves Platform** – an open-source blockchain platform created by the Russian physicist and businessman Alexander Ivanov. This platform allows its users to launch their own cryptocurrency tokens on the basis of the smart contracts technology. According to the estimations of CoinmarketCap, the market capitalisation of Waves as of February 7, 2019 is more than USD 258 million. The company launched the ICO in 2016 and gained more than BTC 30,000.

Generally speaking, the year 2018 was not very fruitful in terms of IPOs, and fintech companies have not been excluded from this tendency. Experts suppose that such behaviour of the market players may be because of the sanctions policy against Russia and the absence of solid legal framework in the sphere of fintech.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

As was previously stated in question 1.2 above, Russian legislation does not cover the majority of issues related to the sphere of fintech. The legislation concerning cryptocurrencies and cryptoassets will be analysed in the following question below.

On the subject of P2P financing and crowdfunding, a new project law concerning the crowdfunding market (also submitted to Parliament) should be mentioned. This project is more oriented towards the regulation of crowdinvesting and scarcely covers the issues related to ordinary crowdfunding. For example, the draft states in art. 1 that it does not cover the issues relating to donations. Moreover, the law is planned to limit the maximum amount of investments of a non-qualified investor or individual entrepreneur in one project, as well as the overall amount of investments that a project may raise by sums, indicated by the Central Bank (nowadays these amounts are expected to be RUB 1.4 million (\approx USD 21,200; hereinafter, the applied exchange rate of RUB to USD is relevant as of February 7, 2019) and RUB 2 billion (\approx USD 30.3 million), respectively). The first reading of this draft was completed in May 2018 and the second one should take place at the beginning of 2019.

Apart from P2P financing and crowdfunding, the laws regulate the activity of microfinance organisations dealing with microfinancing. According to the Federal Law dated July 2, 2010 No. 151-FZ “On microfinance activity and microfinance companies”, such companies shall receive a special licence and be included on the register. The amount of the microloans that may be provided to entities and individuals is limited to RUB 3 million (\approx USD 45,510) and RUB 500,000 (\approx USD 7,585), respectively. Microfinance companies are not entitled to act as professional members of the securities market or traditional banks.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

The main document elaborated in this sphere is the draft law prepared by the Ministry of Finance and the Central Bank, which was submitted to the Parliament (State Duma) on March 20, 2018 and passed the first reading in May 2018. The key elements of this draft, that fall undoubtedly under the general trend of the Russian authorities’ attitude towards these innovations, are the following:

- cryptocurrency and tokens are qualified as a digital financial asset (hereinafter – a DFA). These DFAs may not be used as lawful means of payment. The transactions aimed at the exchange of DFAs to other DFAs, roubles, foreign currency and other property may be performed by a non-qualified investor via a special DFA Exchange Operator (an entity acting according to the applicable laws as a broker, dealer, forex dealer or market operator) only;
- mining is recognised as an activity aimed at creation or receipt (as a reward for transactions validation) of cryptocurrency. This activity is qualified as business activity if the person (miner) exceeds within three months the limits of energy consumption, stipulated by the government; and

- a smart contract is identified as an agreement in electronic form, the execution of rights and obligations under which is performed by way of automatic electronic transactions in the distributed ledgers, accomplished in the order and under circumstances stipulated in such contract.

Concerning the ICO, the idea of the authorities is to make the procedure similar to IPO. For this reason, at the first stage of issue the issuers of tokens should publish, on the Internet, their investing memorandum and a public offer (a document containing the terms of tokens issue, the issuer, depositary, price, date when the agreements with investors will be concluded, information about the procedure of electronic wallets opening, etc.). During the second stage of the issue the contracts, as well as smart contracts, aimed at tokens transfer to the purchasers are concluded. Non-qualified investors are entitled to purchase tokens from one issue for a maximum sum identified by the Central Bank (this amount is currently planned to be limited to RUB 50,000 \approx USD 758).

It should be further mentioned that in the beginning of September 2018, a great number of modifications were proposed to the first draft of the mentioned law and the basic concepts were substantially altered. For example, the definition of cryptocurrency was completely eliminated from the draft, and financial transactions involving cryptocurrencies were no longer governed by this law (it only covered the sale/purchase and exchange of tokens), etc. These modifications provoked a wave of criticism and scepticism from the part of the Presidential Council for Codification and Development of Civil Legislation. The second hearing of this draft should have taken place in autumn 2018, but due to these disputes the Council issued a recommendation listing all the discrepancies, and suggested returning this draft back to the first hearing once enhanced.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

As was previously mentioned, Russian authorities are encouraged by the development of new technologies, but at the same time try to establish the rules of the game and regulate this sphere for the avoidance of gaps in the law and shadow schemes. The document stating the main directions of fintech development in Russia for the years 2018–2020 published by the Central Bank (its description was provided in question 1.1) represents another example of the authorities’ interest towards fintech.

Furthermore, in the year 2009 Skolkovo Innovation Center (so-called “Russian Silicon Valley”) was created. The main purpose of this high technology business area is the development of science and technologies, including fintech. A special IT cluster is dedicated to the development of information security, information transfer and storage, robotisation, etc.

Besides that, the Russian Government, State Duma and the Ministry of Economic Development and Trade are currently discussing the possibility of launching a new regulatory “sandbox” project. The idea of the authorities is to allow the use of cryptocurrencies for payment purposes in some pilot regions (currently, Kaliningrad and Tatarstan regions are being discussed). It is planned to give some fintech companies dealing with distributed ledgers, including blockchain, artificial intelligence, quantum or neurotechnologies, the possibility to use cryptocurrencies for the purposes of fundraising as well as buying and selling assets.

Another interesting pilot project may be launched in Udmurtia region. The region’s government is currently considering the issue of

tokenised bonds and their listing on the Byelorussian crypto exchange Currency.com. Such placement will be aimed at fundraising and the attraction of additional investment into the region.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

A foreign company providing fintech services and interested in attracting Russian clients should remember that some Russian laws have the so-called imperative provisions that may not be altered or avoided by an agreement of the parties. Such provisions may appear in different fields, such as personal data protection (see also question 4.2), consumer rights protection (the consumer of different goods and services is basically qualified as a weaker party to a contract and has, consequently, several rights aimed at protection of his interests). Furthermore, foreign fintech companies should comply with the mandatory requirements regarding the IPO and ICO (see questions 2.3 and 3.1, respectively).

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

Legal regulation in the field of the collection/use/transmission of personal data is based on the Constitution of the Russian Federation (in particular, cl. 1 art. 24, which prohibits the collection, storage, use and dissemination of information on a person's private life without his/her consent) and international treaties such as the Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data dated January 1, 1981 No. 108 (hereinafter – Personal Data Protection Convention).

The primary national Law is the Federal Law dated July 27, 2006 No. 152-FZ “On personal data” (hereinafter – Personal Data Law).

There are some other federal laws defining cases and peculiarities of processing of personal data, such as the Federal Law dated July 27, 2006 No. 149-FZ “On information, information technologies and the protection of information”. The Labour Code of the Russian Federation (hereinafter – the Labour Code) contains a separate section devoted to the protection of the personal data of the employees.

There are a number of subordinate acts, e.g.:

- the Government Decree dated November 1, 2012 No. 1119 “On approval of the requirements for the protection of personal data during their processing in personal data information systems”;
- the Presidential Decree “On approval of the list of the confidential information”;
- the Order of the Federal Service for Supervision in the sphere of communication, information technologies and mass communications (Roskomnadzor) dated September 5, 2013 No. 996 “On approval of the requirements for the depersonalization of personal data”; and
- the Order of Roskomnadzor dated March 15, 2013 No. 274 “On approval of the list of foreign states which are not parties to the Convention and which provide adequate protection of the rights of subjects of personal data” (Roskomnadzor Order No. 274).

As for fintech businesses, there are no special legal acts, so general principals of personal data protection are applicable.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

Generally, Russian legislation permits cross-border transfer of personal data (s. art. 12 of the Personal Data Law). However, at the same time, the list of countries to which personal data may be transferred is limited by two criteria. It should be either countries which are parties to the Personal Data Protection Convention or countries which provide adequate protection of the rights of personal data subjects according to Roskomnadzor Order No. 274.

The cross-border transfer of personal data may be prohibited or restricted for the purposes of protecting the foundations of the constitutional order of the Russian Federation, morality, health, rights and legitimate interests of citizens, to ensure the state's defence and its security.

As to the transfer of personal data on the territory of foreign states which do not provide adequate protection, it may be carried out only in the following cases:

- there is written consent of the personal data subject to the cross-border transfer of personal data;
- it is stipulated in the international treaties of the Russian Federation;
- it is provided by the federal laws and necessary for the purposes of protection of the foundations of the constitutional order of the Russian Federation, ensuring national defence and safety of the state, and also the steady and safe functioning of transport infrastructure, protection of interests of the personality, and protection of society and the state in the field of transport infrastructure from acts of illegal intervention;
- it is required for the performance of the agreement's obligations, to which the personal data subject is a party; and
- it is required for the protection of life, health and other vital interests of the personal data subject, or other persons if it is impossible to obtain consent – in writing – of the personal data subject.

The requirements of the Personal Data Law apply to the Russian legal entities, as well as to the branches and representative offices of foreign legal entities engaged in activities of personal data processing on the territory of the Russian Federation. But it is worth mentioning that, according to latest amendments to the Personal Data Law, the operator is obliged to ensure the recording, systematisation, accumulation, storage, clarification (updating, changing) and extraction of personal data of Russian citizens using databases located only on the territory of the Russian Federation, even if the personal data was received through the Internet.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

Administrative liability: According to the Federal Law dated February 7, 2017 No. 13-FZ “On amendments to the Code of Administrative Offences of the Russian Federation”, the responsibility for violation in this sphere increased and there are now seven types of offence instead of one. Examples of administrative offences are: processing of personal data in cases not prescribed by law; processing of personal data without written consent of the personal data subject to the processing of his personal data in cases where such consent must be obtained; and others (art. 13.11). The usual penalties for administrative offences in this sphere are fines (up to RUB 75,000 ≈ USD 1,137).

Failure to comply with the data privacy laws also results in the following sanctions:

Criminal liability: The Criminal Code of the Russian Federation contains a number of criminal offences, for example: illegal collection or dissemination of information on the private life of a person, constituting his or her personal or family secrets without his or her consent; or dissemination of this information in a public speech, publicly displayed work or mass media (cl. 1 art. 137). The most common penalties for criminal offences in this sphere are: fines; compulsory community service; imprisonment for a maximum term of five years; and others.

Disciplinary and material liability: According to the Labour Code, the employer (or officers) bear(s) disciplinary and material liability for breach of data privacy laws while processing the personal data of employees (art. 90). The employer is entitled to terminate the employment agreement with an employee in the case where the latter illegally disclosed the personal data of another employee.

Civil law liability: In any case, the person who breaches the data privacy law bears responsibility under civil legislation. Moreover, according to cl. 2 art. 24 of the Personal Data Law, it is possible to compensate moral damage irrespective of compensation for property damage and losses.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

The Russian legislation in the sphere of cyber security and cyber defence is continuously evolving. Among the main documents that may apply to fintech businesses, it is worth mentioning the following:

- The Federal Law dated July 27, 2006 No. 149-FZ “On information, information technologies and information protection”, stipulating the main methods of information protection, orders an obligation of the information holder to utilise constant control of the level of information security, prevent unauthorised access to information and prevent negative impact on the technical means of information processing (e.g. servers, hard discs, etc.).
- Furthermore, the new Federal Law dated July 26, 2017 No. 187-FZ “On safety of critical information infrastructure of the Russian Federation”, adopted at the end of 2017, assumes the creation of a state system of detection, prevention and elimination of the consequences of attacks on information resources of the country.
- The Criminal and Administrative Codes of the Russian Federation contain several offences in the field of computer information, e.g.: the unlawful access to computer information protected by law; the use and distribution of fraudulent computer programs; the undue influence on the critical information infrastructure of the Russian Federation; and non-performance of duties by the news aggregator owner, etc. The most common penalties for such offences in this sphere are fines, compulsory community service or imprisonment.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

The results of a report submitted in 2013 by Russia, as a member of the Financial Action Task Force (FATF), led to the removal of the country from the permanent monitoring list until a new round of mutual evaluations.

Moreover, Russia is a party of several multilateral and bilateral agreements aimed at automatic information exchange, including the Convention on Mutual Administrative Assistance in Tax Matters. In September 2018, Russia started the automatic tax information exchange according to the OECD system.

The main national law in this sphere is the Federal Law dated August 7, 2001 No. 115-FZ “On anti-money laundering and anti-terrorism financing”, stipulating the obligation of financial institutions (including credit organisations, insurance companies, professional participants of the securities market, etc.) to work out the rules of internal supervision and compulsory control of suspicious transactions (usually exceeding or equal to the amount of RUB 600,000 ≈ USD 9,100), taking into account the recommendations and directions of the Central Bank and the orders of the Federal Service for Financial Monitoring.

Furthermore, the law stipulates the obligation of a company to provide banks and tax authorities with relevant information about its beneficial owners (according to the law, a shareholder owning directly or indirectly at least 25% of the company’s shares is qualified as its beneficial owner).

The Criminal and Administrative Codes of the Russian Federation contain a number of offences in this field, e.g. the laundering of money and other property acquired by illegal means, facilitating terrorist activities, the failure to comply with the requirements of the money laundering regulations, etc. The most common penalties for such offences in this sphere are fines, compulsory community service or limitation of freedom.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

In addition to the regulatory regimes already specified above, fintech businesses shall definitely comply with the requirements concerning:

- establishment and registration of a new Russian-based company;
- registration of a foreign company’s Russian branch office;
- taxation of companies; and
- import-substitution and localisation rules.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

In relation to hiring employees, a written employment contract is required. The labour relations arise between an employee and an employer on the basis of such contract. Labour relations between the employer and the employee may appear before signing the labour agreement in case the employee was actually admitted to work at the request of the employer. In this case, the conclusion of the employment contract in writing is required no later than three working days from the date of the actual admission (art. 67 of the Labour Code).

There are some restrictions related to the age of the employee. The conclusion of a contract with a person under the age of 16 is possible if there is no damage to health, study and moral development. In such cases, the consent of one of the parents (guardians), as well as the consent of the guardianship authorities, is obligatory.

Any discrimination of the candidate by the conclusion or termination of an employment contract in connection with the gender, race, skin colour, nationality, language, origin, status (property, family, social and official), age, place of residence of the candidate, and with respect to women for reasons related to pregnancy or the presence of children, is forbidden.

There are different grounds for dismissal of the employee: on the initiative of the employee; by agreement of the parties; due to staff reduction; or due to violation of labour duties, etc. Notification of the dismissal of the employee shall be made in writing (e.g. three days prior to dismissal in case of the employer's initiative).

Employers are not entitled to dismiss certain categories of employees: pregnant women; women with a child under the age of three or single women raising a child under the age of 14; a parent who is the sole breadwinner of a disabled child under the age of 18; and an employee in the period of his temporary incapacity for work, etc.

It should be noted that the Russian labour law is very employee-friendly. An employee may be dismissed only in the case of strong reasons, e.g. because of an absence from the workplace for more than four hours during the working day or appearance of the worker in an intoxicated condition.

5.2 What, if any, mandatory employment benefits must be provided to staff?

An employee is to be granted with a minimum salary (Statutory Minimum Wage Index) amounting to RUB 11,280 ≈ USD 171 (starting from January 1, 2019). However, each territorial subject has the right to establish its own rate, e.g. in Moscow it is equal to RUB 18,781 ≈ USD 285 (starting from January 1, 2019).

The key mandatory employment benefits of an employee are the following:

- in case of official business trips: the preservation of the place of work (position) and average earnings, as well as reimbursement of expenses associated with such trips;
- in case of moving to another locality due to the change of the workplace: reimbursement of all expenses for moving and settlement in a new place;
- in case of combining work with education: additional study leave with the preservation of average earnings;
- in case of staff reduction or liquidation of the organisation: severance in the amount of one average monthly salary and a possibility to require two additional monthly salaries while looking for a new job;
- maternity and paternity leave (up to three years);
- paid annual leave (not less than 28 calendar days); moreover, according to the Federal Law dated November 11, 2018 No. 360-FZ, employees who have three or more children under the age of 12 shall be granted annual paid leave at their discretion at a convenient time for them;
- reduced working time for disabled persons (not more than 35 hours per week with full payment for work); and
- allowance for temporary incapacity for work (illness).

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

According to cl. 1 art. 13 of the Federal Law dated July 25, 2002 No. 115-FZ "On the legal status of foreign citizens in the Russian

Federation", foreigners enjoy the right to freely dispose of their abilities to work, and choose the kind of activity and profession on the territory of the Russian Federation.

Foreigners have the right to enter into labour relations if they have reached the age of 18 (cl. 3 art. 327.1 of the Labour Code).

There are some requirements for employers. The first thing which an employer shall control is the status of a foreigner. There are three statuses of foreigners which are in place in Russia:

- **Temporarily staying foreigners** who work in Russia based on a visa and a work permit.
- **Temporarily residing foreigners** who work in Russia based on a temporary residence permit.
- **Permanently residing foreigners** who work in Russia based on a resident permit.

Most foreigners work in Russia on both a visa and a work permit. A work permit should be executed only for foreigners from visa countries. Foreigners from visa-free countries (e.g. Moldova, Uzbekistan) shall obtain a patent. A work permit may be divided into two categories: for ordinary workers; and for highly qualified specialists (HQs). A highly qualified specialist is a foreign citizen who has experience, skills or achievements in a particular field of activity. Such workers have some privileges over others: a work permit is valid for three years (for ordinary workers this is usually for a year); they do not have to pass an exam in the Russian language, Russian history and the basics of Russian legislation; and they have the right to primary health care and specialised medical care on the basis of the medical insurance policy, etc. Highly-qualified specialists participating in the "Skolkovo" project after entering Russia have the right to obtain a work visa for up to three years in the case of successful employment.

According to art. 16 of the Federal Law dated September 28, 2010 No. 244-FZ "On Skolkovo innovation center", legal entities involved in the implementation of the Skolkovo project which employ foreigners to carry out labour activities do not have to obtain permission for recruitment of such employees. Moreover, invitations to enter the Russian Federation for labour purposes, as well as work permits to foreigners, are issued without taking into account the quotas established by the government of the Russian Federation (not only foreign workers themselves, but also adult members of families of highly qualified specialists).

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

According to art. 2 of the Federal Law dated August 23, 1996 No. 127-FZ "Concerning science and State scientific and technical policy", an innovation means a new or significantly improved product (product or service) or process, a new method of sales or a new method of organisation in business practice, workplace organisation or external relations.

According to art. 1350 of the Civil Code of the Russian Federation (hereinafter – the Civil Code), an invention means a technical solution in any field relating to a product or a method, including the use of a product or a method for a certain purpose.

On the basis of these definitions, we may assert that innovations and inventions are the results of intellectual activity which are currently governed by the Civil Code provisions.

The protection of intellectual rights (in particular, rights to the patent for the innovation or invention) is mainly exercised through

the courts. There is a specialised court for intellectual property rights in Russia (created in 2013) which considers disputes related to the protection of intellectual rights.

But in some cases, the legislator also provides the possibility of extrajudicial protection with a further possibility of appealing against the decision of the administrative body to the courts.

The following bodies administratively consider disputes related to the protection of intellectual property rights:

- Federal service for intellectual property (Rospatent); and
- Federal Executive authorities (the Ministry of Defence, the Ministry of Internal Affairs and others) empowered by the government of the Russian Federation to consider applications for the grant of a patent for inventions that contain data constituting a state secret.

Types of liabilities prescribed by law:

- civil (recognition of the right, restoring the situation that existed before the violation of law, the suppression of acts infringing the intellectual property rights or creating a threat of its violation, compensation for moral harm, and publication of the court's decision on the violation) (arts 1251–1252 of the Civil Code);
- administrative (imposition of a fine and forfeiture of counterfeit copies in case of import, sale and unlawful use of counterfeit works); and
- criminal (imposition of a fine, community service, imprisonment in case of piracy, import, sale and unlawful use of counterfeit works, and unlawful use of industrial property, if the mentioned actions led to a material loss).

Since 2017, pre-court dispute resolution is mandatory in some cases. According to the provisions of the Civil Code, if the rightholder and the infringer of an exclusive right are legal entities and (or) individual entrepreneurs, and the dispute is under the jurisdiction of the state arbitrazh court, the rightholder shall file a pretrial claim before filing a lawsuit for damages or compensation.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

The emergence, exercise and protection of the ownership of IP depend on the item of intellectual property. For example, for the emergence, exercise and protection of copyright, no registration or any other formalities are required.

For other items of intellectual rights, creation and expression in an objective form is not enough: for the rights to arise and be realised and protected, it is necessary to perform a number of formalities prescribed by law.

For example, the exclusive right to an invention, even if it is actively used by the author himself, is not subject to protection, and the object of “industrial property” is not protected until the author (or a person authorised by him) receives a special document – a patent, following certain actions (filing an application, performance of the expert's examination, payment of duties, state registration and receipt of the patent).

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

The Civil Code is the primary legislation for intellectual property rights, but there is a sufficient number of international treaties to which Russia has joined.

Generally, the enforcement and protection of IP rights in Russia are performed according to the documents of title issued by Rospatent. At the same time, some international treaties stipulate a special regime on IP rights protection. For example, Russia is a member of the Paris Convention for the Protection of Industrial Property (1883), Patent Cooperation Treaty (1970) and the Madrid Agreement Concerning the International Registration of Marks (1981). Pursuant to the respective provision of the mentioned treaties, the enforcement of the IP rights protected under these conventional regimes may be done in Russia without the receipt of local patents (the so-called convention priority rule is applied).

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

IP is usually exploited by means of:

- assignment – a comprehensive transfer of the exclusive rights from the rightholder to the other person or entity;
- licensing – granting of the intellectual property for temporary use; or
- franchising – one party possessing a certain set of exclusive rights, having a well-established business reputation and certain experience in the commercial sphere of activity, transfers the set of rights (trademark, know-how, firm name, etc.) to the other party for use in its business activity.

These agreements must be in writing and they are subject to state registration.

According to the Civil Code, no gratuitous assignment of the exclusive right between commercial organisations is allowed. The payment of a remuneration under these agreements may be provided in the form of fixed one-time or periodic payments, interest payments on income (revenue) or in any other form.

Acknowledgment

The authors of this chapter are pleased to acknowledge **Evgeny Zhilin** for his individual contribution and expertise on the matter.

Evgeny Zhilin is our Partner in the Zurich office. His area of expertise focuses on international law (public and private), corporate law, contract law, commercial law, investment legislation, real estate and natural resources law, land law, civil law, litigation and arbitration, and legal due diligence.

Evgeny is the Advisor to the President of the Federal Chamber of Lawyers of the Russian Federation. EMEA Legal Experts recognises him as an expert in corporate law and M&A; *Best Lawyers* qualified him as an expert in trade law; and *IFLR 1000* points him out as a Notable Practitioner. In March 2018, Evgeny was ranked as a leading specialist in the sphere of corporate & M&A transactions and international dispute resolution by the *Kommersant* rating.

**Maxim Mezentsev**

QUORUS GmbH
123112 Presnenskaya nab., 6, bld. 2
Imperia Tower, office 4526
Moscow
Russia

Tel: +7 495 540 60 23
Email: mezentsev@quorus.ch
URL: www.quorus.ch

Maxim is a Senior Associate and Head of QUORUS's Moscow office. Corporate law and M&A, contract law, legal regulation of foreign investments, competition and antitrust, international arbitration, and capital markets are among Maxim's main areas of expertise.

Maxim advises Russian and foreign clients on the matters of contract and corporate law, including the matters of creation, reorganisation and dissolution of legal entities, accreditation of subsidiaries and representative offices of foreign legal entities.

In March 2018, Maxim was ranked as a leading specialist in the sphere of commercial law in the *Kommersant* rating.

Maxim is fluent in Russian, English and German.

**Nikita Iovenko**

QUORUS GmbH
123112 Presnenskaya nab., 6, bld. 2
Imperia Tower, office 4526
Moscow
Russia

Tel: +7 495 540 60 23
Email: iovenko@quorus.ch
URL: www.quorus.ch

Nikita is an Associate in QUORUS's Moscow office. His areas of expertise include, *inter alia*, corporate law and M&A, contract law, laws and regulations in the sphere of fintech, legal regulation of foreign investments, capital markets, civil law, international public and private law.

Nikita performs complex legal support of Russian and foreign clients of the firm, as well as providing assistance to their business activity in Russia and participating in due diligence projects.

Nikita is fluent in Russian, English, French and Spanish.

QUORUS

QUORUS GmbH is a Swiss-Russian management and consultancy firm with an exclusive operational focus on Swiss/European and Russian/Eurasian cross-border activities. QUORUS's aim is to act as a centre of competence and excellence as well as a hub for cross-border Swiss/European-Russian/Eurasian projects, thus it fulfils a dual role in that it advises, sustains and accompanies projects originating in Russia/Eurasia aiming towards Switzerland/Europe, as well as in the opposite direction.

Focusing on holistic, exclusive, tailor-made specialist service solutions based on expertise in Russian, Swiss and EU law, banking, asset-management, and further fields, depending on clients' needs, QUORUS's unique business model provides for targeted partnerships with specialists in Russia, Eurasia, Switzerland, Europe and beyond.

In March 2018, QUORUS was ranked as the leading law firm in Commercial Law and Foreign Trade, Corporate and M&A, International Arbitration, and Pharmaceuticals in the *Kommersant* rating (annual Russian rating of law firms and lawyers).

In December 2018, a famous annual Russian law firms rating – PRAVO 300 – ranked our firm's Commercial and Foreign Trade practice as Tier 1, and the practices of International Arbitration and Corporate/M&A were ranked in Tier 3. The firm also has the status of Recognised Firm according to the *IFLR 1000* international rating.

Singapore

Andrea Chee



Law Zhi Tian



AEI Legal LLC

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Singapore is a leading destination for fintech businesses. It offers a compelling mix of a strongly supportive government, a well-established financial sector, excellent physical and digital infrastructure, a large pool of IT specialists, and a vibrant ecosystem of investors and advisers. It is also seen as a clear starting point for companies looking to expand into Southeast Asia.

Active fintech businesses in Singapore include but are not limited to businesses involved in remittances and money transfers, lending, wealth management, blockchain and cryptocurrency, crowdfunding and investment, and payments.

Fintech firms based in ASEAN saw a record high of US\$458 million in investments between January and October 2018, with US\$222 million going to fintechs in Singapore alone.

In 2018, Singapore hosted 43% of all fintech firms in ASEAN, a 6% increase from 2017. Aiding this upward trend are government-accredited incubators and multiple innovation labs in Singapore run by established players including PayPal, Mastercard, Visa, DBS, HSBC, Citi, IBM, Microsoft and Oracle.

The Singapore government recently opened its interbank instant fund transfer system (**FAST**) to non-banks, allowing consumers to top up e-wallets from any bank account. Singapore also launched a “first of its kind globally” national QR code standard, SGQR, which combined the QR codes of multiple electronic payments solutions to address the fragmented e-payment landscape. The Monetary Authority of Singapore (**MAS**) issued e-payments user protection guidelines to deal with, *inter alia*, the liability for losses arising from unauthorised transactions.

Notable fintech trends include the rise of non-financial tech players in the fintech space – for instance, Singapore-based Grab began as a ride-hailing startup, but after launching its digital payment platform GrabPay, expanded into credit services. Singapore continues to be a leader for blockchain-based startups. The rise of artificial intelligence and big data, coupled with some high-profile data breach incidents, has resulted in increased awareness and emphasis on data protection and privacy.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

There are no specific prohibitions or restrictions on fintech businesses.

With respect to initial coin offerings (**ICOs**), in contrast to the outright bans declared by some regulators in other parts of Asia, the MAS has stated that digital tokens will be regulated if they exhibit the features of capital market products regulated under Singapore legislation.

Intermediaries providing services in connection with ICOs may also be subject to regulation.

Fintech firms remain subject to the laws of Singapore generally. For example, websites and financial transactions relating to prohibited remote gambling activities may be blocked under the Remote Gambling Act.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

Singapore has a thriving investment scene.

There are a number of prominent angel investors, including Facebook’s co-founder Eduardo Saverin, and various angel networks.

Early-stage venture capitalist (**VC**) firms are also very active in Singapore, including Golden Gate Ventures, Sequoia and Rakuten. Singapore’s Temasek has also begun making investments in early-stage companies.

Singapore is one of the world’s financial centres, with numerous financial institutions available to provide loans and financing. There are also crowdfunding platforms specifically targeting startups, such as FundedHere and Fundnel.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

Numerous incentives are available to Singapore start-ups. In particular, fintechs can avail themselves of the US\$225 million

Financial Sector Technology and Innovation (**FSTI**) scheme, which offers funding for up to 50–70% of a company's qualifying costs, capped at S\$200,000, to promote experimentation.

Other incentives available to startups include:

- Startup SG, a platform run by Enterprise Singapore, which provides funds, mentorship, and grants to startups, facilitates employment passes, and provides support to accelerators and incubators.
- The Capabilities Development Grant, which helps to defray up to 70% of qualifying project costs (e.g. equipment and software costs) in areas such as product development and market access.
- The Inland Revenue Authority of Singapore (**IRAS**) offers tax exemptions to startups. From 2020, qualifying startups may enjoy a 75% exemption on the first S\$100,000 of chargeable income and a further 50% exemption on the next S\$100,000 of chargeable income.

There are also multiple incentives for investors. In addition to having one of the lowest corporate tax rates in the world, Singapore offers tax holidays and concessions, grants and other favourable conditions. For example:

- Angel investors are encouraged to invest in startups with the Angel Investors Tax Deduction Scheme which offers tax deductions for at least S\$100,000 of qualifying investment in a qualifying startup.
- Funds may be tax-exempt, whether onshore or offshore.
- The MAS has a Financial Sector Incentive (**FSI**) Scheme for licensed financial institutions, from fund managers to capital market players. Income derived by FSI award holders from qualifying activities are subject to income tax at concessionary rates.

In 2018, the MAS announced a number of initiatives to enhance private markets financing channels, including a programme to place up to US\$5 billion with private equity and infrastructure fund managers.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

The Singapore Exchange (**SGX**) has two boards, the Main Board and the Catalist Board.

There are no quantitative criteria for companies seeking to list on the Catalist Board, a sponsor-supervised listing platform. A Catalist issuer is required to appoint a qualified sponsor to assess its suitability for listing and to advise on the IPO, and must maintain a sponsor after the IPO.

A Main Board issuer must satisfy one of the following quantitative criteria:

- Minimum consolidated pre-tax profit (based on full-year consolidated audited accounts) of at least S\$30 million for the latest financial year, and an operating track record of at least three years.
- Profitable in the latest financial year (pre-tax profit based on the latest full-year consolidated audited accounts), an operating track record of at least three years, and a market capitalisation of not less than S\$150 million based on the issue price and post-invitation issued share capital.
- Operating revenue (actual or *pro forma*) in the latest completed financial year, a market capitalisation of not less than S\$300 million based on the issue price and post-invitation issued share capital. Real estate investment trusts and business trusts which have met the S\$300 million market capitalisation rule can apply even if they do not have historical financial information, if they are able to demonstrate that they will generate operating revenue immediately upon listing.

There are also other requirements in respect of shareholding spread and distribution, financial position and liquidity, and directors and management. For example, SGX will require a director with no prior experience as a director of an issuer listed on SGX to undergo appropriate training. The character and integrity of the directors, management and controlling shareholders will be relevant factors for consideration. The board must have independent directors.

A Life Science company which is unable to meet the Main Board's quantitative criteria may still be able to list on SGX if, *inter alia*, it has raised funds from institutional or accredited investors not less than six months prior to the date of the listing application, will have a market capitalisation of at least S\$300 million, can demonstrate a three-year record of laboratory research and development (**R&D**) operations, and has enough working capital for at least 18 months after listing.

A Mineral Oil and Gas (**MOG**) company which is unable to meet the Main Board's quantitative criteria may still be able to list on SGX if it will have a market capitalisation of at least S\$300 million and has disclosed a plan, substantiated by the opinion of an independent qualified person, to advance to production with capital expenditure for each milestone.

Significantly, in 2018, SGX approved a landmark change to its listing rules and allowed dual-class share (**DCS**) structures for issuers seeking a primary listing on the SGX Main Board. Multiple-voting shares may carry up to 10 votes per share. DCS issuers must meet SGX's Main Board criteria, and satisfy SGX as to their suitability to list as a DCS structure.

In January 2019, the S\$75 million Grant for Equity Market Singapore was launched to defray the costs of listing on SGX and support research initiatives.

- Technology companies, including fintech, consumer tech, on-demand services, gaming services and peripheral manufacturers, with a market capitalisation of at least S\$300 million, may receive up to 70% of the funds for their listing expenses, capped at S\$1 million.
- Companies in high-growth sectors, such as digital, healthcare, advanced manufacturing, logistics, urban solutions, infrastructure and hub services, with a market capitalisation of at least S\$300 million, may receive up to 20% of the funds for their listing expenses, capped at S\$500,000.
- Other eligible companies may receive up to 20% of the funds for their listing expenses, capped at S\$200,000.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

In 2018, global fintech group Ayondo, which offers B2B and B2C clients social trading and brokerage services, was listed on the SGX Catalist board, joining 74 other technology companies listed on the SGX.

In 2018, 71 deals were struck for fintech companies in Singapore. Notable deals included:

- P2P lending platform Funding Societies, which raised US\$25 million in its oversubscribed Series B funding round led by Softbank;
- blockchain startup Terra, which raised US\$32 million during its seed round;
- insurtech company Singapore Life, which raised US\$52 million from British billionaire Michael Spencer; and
- cloud-computing company Deskera, which raised US\$60 million and launched a B2B commerce platform for SMEs.

Singapore-based Grab has reached “decacorn” status. A ride-hailing firm which launched its own digital payment platform GrabPay and expanded into credit services, it was valued at over US\$10 billion in its most recent funding round in 2018.

Singapore-based Carousell, a mobile classifieds app, launched its e-wallet Caroupay, and raised US\$85 million in 2018 with a valuation of over US\$500 million.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

Singapore has a supportive regulatory environment for businesses.

The primary regulator for most fintech businesses is the MAS.

Fintech businesses may fall within the regulatory ambit of one or more of the following regulatory regimes:

- the Banking Act;
- the Business Trusts Act;
- the Companies Act;
- the Financial Advisers Act;
- the Finance Companies Act;
- the Insurance Act;
- the Securities and Futures Act;
- the Trust Companies Act;
- the Moneylenders Act;
- the Commodity Trading Act; and
- the Payment Services Act (PSA) (which will replace the Payment Systems (Oversight) Act and the Money-Changing and Remittance Businesses Act).

The new PSA is intended to provide a more conducive environment for innovation in payment services, whilst ensuring that risks across the payments value chain are mitigated. Regulated payment services include money transfers, electronic money issuance and digital payment tokens.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

The MAS has stated that ICOs and digital tokens will be regulated if they exhibit the features of capital market products regulated under Singapore legislation; for example, if a token confers on its holder a legal or beneficial interest, or evidences indebtedness. If the token constitutes a capital market product, amongst other things, a prospectus may have to be prepared and registered in connection with the offering.

Intermediaries facilitating an ICO or offering advice may also be subject to regulation. They may be required to have a capital markets licence or financial adviser’s licence or be otherwise exempted.

Cryptocurrency and cryptoasset companies must comply with anti-money laundering and counter-financing of terrorism requirements. These stipulations include conducting enhanced due diligence if certain risks are identified. In appropriate cases, companies may even be obliged to report suspicious transactions to the Suspicious Transaction Reporting Office of the Singapore Police Force’s Commercial Affairs Department, under the Terrorism (Suppression of Financing) Act.

Companies dealing with cryptocurrencies should also take note of the new Payment Services Act – an exemption or licence may be required under the new legislation. Licences include:

- a money-changing licence for money-changing services;
- a Major Payment Institution (MPI) licence for payment services where (i) the monthly average of the total value of all payment transactions over a calendar year exceeds S\$3 million, or (ii) where the monthly average of the total value of all payment transactions over a calendar year for two or more licensable activities exceeds S\$6 million. A MPI licensee must maintain a minimum paid-up capital of S\$250,000; and
- a Standard Payment Institution licence for payment services where the thresholds for the MPI licence are not met.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

The Singapore government and the MAS are highly supportive of fintech innovation.

The Singapore Fintech Festival, organised by the MAS, is reportedly one of the largest gatherings of the global fintech community, attracting leaders from central banks and regulatory agencies, financial institutions, VC firms and fintech companies. In 2018, there were over 40,000 participants from over 100 countries.

As of February 2019, the MAS had signed 29 cooperation agreements with international counterparts to foster closer cooperation, including China, Hong Kong, Japan, Korea, India, Australia, Switzerland, the US and the UK, as well as several members of ASEAN.

The FSTI scheme, which has committed US\$225 million of funding targeted at, *inter alia*, fintech firms, is an initiative of MAS.

The MAS has had a dedicated Fintech and Innovation Group since 2015 to formulate regulatory policy and develop strategies to facilitate the use of technology and innovation in the finance sector, as well as its own FinTech Innovation Lab.

The MAS was one of the first regulators in the world to introduce a regulatory sandbox for fintech companies. Within the sandbox, the MAS may relax specific legal and regulatory requirements.

In 2018, the MAS proposed a Sandbox Express with fast-track approvals available within 21 days. This route envisages providing quicker clearance for companies conducting activities viewed as lower risk or falling within specific pre-defined sandboxes, such as insurance broking, being a recognised market operator, and providing remittance services. The MAS has proposed to assess these applications based on the technological innovativeness of the financial service and the applicant’s key stakeholders.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

Overseas fintech businesses which actively target the Singapore market by offering their products or services in Singapore will remain subject to Singapore laws with extra-territorial provisions, such as the Securities and Futures Act and the Financial Advisers Act, and may require licences or exemptions.

However, it should not be illegal for an overseas fintech business to serve a person in Singapore pursuant to an unsolicited enquiry.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

The Personal Data Protection Act 2012 (PDPA) regulates the collection, use and disclosure of personal data by organisations.

Key obligations include:

- notifying individuals of the purpose for which their data is being collected, used and/or disclosed and obtaining their informed consent for such purpose;
- allowing individuals to access and request correction of their personal data; and
- implementing reasonable security measures to ensure the data is secure from unauthorised access, modification, use and disclosure.

Fintech businesses that deal with consumers should have data protection policies and practices to meet the requirements under the PDPA.

In particular, in 2018, the Personal Data Protection Commission (PDPC) issued advisory guidelines regarding NRIC and other national identification numbers. NRIC refers to the Singapore National Registration Identification Card, a permanent and irreplaceable identifier assigned by the Singapore government to Singapore citizens and permanent residents. Organisations are generally not allowed to collect NRIC numbers, birth certificate numbers, foreign identification numbers, work permit numbers and passport numbers, unless it is necessary to precisely verify an individual's identity to a high degree of fidelity, or otherwise required by law.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

Singapore's PDPA applies to foreign organisations which undertake activities relating to the collection, use and disclosure of personal data in Singapore.

Before transferring personal data outside Singapore, the transferring organisation must take appropriate steps to ensure, *inter alia*, that the recipient organisation is bound by legally enforceable obligations to provide a standard of protection comparable to the PDPA standard.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

The PDPC may investigate complaints, issue directions to organisations to ensure compliance with the PDPA or to rectify issues, and may impose a penalty of up to S\$1 million.

Section 32 of the PDPA also provides that individuals may commence a private action in the courts to seek relief, including by way of an injunction, declaration, damages, or such other relief as the court thinks fit.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

The Computer Misuse and Cybersecurity Act penalises various

cybersecurity offences, including hacking, denial-of-service attacks, phishing, identity theft or fraud, malware infections and electronic theft.

The new Cybersecurity Act 2018 provides, *inter alia*, for the designation of certain computer or computer systems which deliver essential services (including banking and payment services) as Critical Information Infrastructure (CII). CII owners may be required to establish mechanisms and processes to detect cybersecurity threats, conduct annual risk assessments, and participate in cybersecurity exercises if directed. CII owners must notify the Cyber Security Agency of Singapore in the event of a cybersecurity incident.

The Penal Code, Copyright Act, Strategic Goods (Control) Act and the PDPA also contain provisions which may apply to cybersecurity breaches.

Fintech businesses should also note that the MAS has issued guidelines and notices regarding technology risk management, including requiring the implementation of controls to protect customer information from unauthorised access or disclosure.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

Singapore is a member of the Financial Action Task Force and has a strong framework for anti-money laundering and countering the financing of terrorism (AML/CFT).

The Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA) criminalises money laundering in Singapore. The CDSA makes it mandatory for a person to lodge a suspicious transaction report if he or she knows or has reasonable grounds to suspect that any property represents the proceeds of, or was or is intended to be used in connection with, any act that may constitute drug dealing or criminal conduct, and failure to do so constitutes a criminal offence.

Fintech businesses should also comply with relevant AML/CFT notices which the MAS may issue from time to time. For example, fintech businesses are required to conduct customer due diligence for new clients and to monitor for unusual transactions or dealings.

Singapore is also a member of the United Nations (UN) and gives effect to the sanctions under the UN Security Council Resolutions, via regulations issued pursuant to the UN Act. All persons in Singapore must comply with the UN Regulations, including not dealing with UN-designated individuals and entities. Breach of the regulations could subject an individual to a fine not exceeding S\$500,000 and jail for up to 10 years or both, or in any other case, to a fine not exceeding S\$1 million.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

A business must comply with the requirements of the Accounting and Corporate Regulatory Authority (ACRA) and the relevant legislation; for example, the Companies Act, in order to establish a legal entity in Singapore.

Businesses that deal with consumers must comply with, *inter alia*, the Consumer Protection (Fair Trading) Act, which protects consumers against unfair business practices, and the Unfair Contract Terms Act, which protects consumers by limiting the extent to which civil liability can be avoided via contract.

The Competition Act prohibits the prevention, restriction or distortion of competition within Singapore.

The Employment Act and the Employment Claims Act provides certain protections for certain employees and facilitates the resolution of employment disputes.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

Singapore's new Employment Act (EA) and Employment Claims Act are expected to come into effect on 1 April 2019.

The "core provisions" of the EA will now extend to all professionals, managers, executives and technicians (PMETs) without any salary cap, in addition to all workmen and non-workmen. These provisions include:

- a minimum of seven to 14 days of annual leave (depending on the length of service);
- salary payment to be made within seven days after the end of the salary period;
- paid sick leave of 14 days per year and up to 60 days if hospitalisation is required (including full reimbursement for medical consultation fees);
- 11 gazetted public holidays;
- a requirement that employers maintain proper employment records, issue key employment terms in writing, and itemised pay slips to employees; and
- recourse for wrong dismissals.

Independent contractors who are not employees are not protected under the EA.

In Singapore, employers are generally free to negotiate the terms of employment.

The Tripartite Guidelines on Fair Employment Practices (TAFEP) state, *inter alia*, that recruitment should not be based on discriminatory criteria such as age, race, religion and gender. Employers who do not abide by the TAFEP may have their work pass privileges curtailed.

Employers can agree with employees on the notice period for termination. If it is not contractually agreed, the EA stipulates a minimum notice period, ranging between one day if the length of employment is less than 26 weeks, to four weeks if the length of employment is five years or more. Payment may be made *in lieu* of notice. An employee may be dismissed without notice for misconduct inconsistent with the express or implied terms of service, after due inquiry.

The Retirement and Re-employment Act prohibits employers from dismissing employees below the age of 62 due to their age. The minimum retirement age is 62.

In relation to employees who are not Singapore citizens, employers must ensure that such employees fulfil their tax obligations upon termination of employment or in the event he/she plans to leave Singapore for more than three months. Employers must notify IRAS in advance and seek tax clearance, withhold tax and complete tax filings.

5.2 What, if any, mandatory employment benefits must be provided to staff?

In addition to the "core provisions" of the EA mentioned above, the EA also stipulates, in relation to workmen earning a basic monthly

salary of up to S\$4,500 and non-workmen earning a basic monthly salary of up to S\$2,500, fixed work hours and overtime pay.

The Child Development Co-Savings Act states that if the stipulated eligibility criteria are met, an employee is entitled to 16 weeks of maternity leave, two weeks of paternity leave, six days of childcare leave and adoption leave.

In relation to employees who are Singapore citizens or Singapore permanent residents, both employers and employees are required to make contributions each month to the employee's Central Provident Fund (CPF) account. CPF is a mandatory employment-based savings plan. The employer is required to deduct from the employee's salary in respect of the employee's contribution, and contribute monies directly to the employee's CPF account.

Employers are also required to pay a Skill Development Fund levy, which ranges between S\$2–S\$11.25 per month per employee.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

Generally, foreigners are required to have a valid work pass to work in Singapore, regardless of the length of employment.

Singapore offers a particular work pass, the EntrePass, for serial entrepreneurs, high-calibre innovators and experienced investors who want to operate a business in Singapore. Fintech business entrepreneurs may be able to utilise the EntrePass.

In addition, Startup SG facilitates employment passes for startups.

For fintech businesses, the most relevant work passes are likely to be the Employment Pass, which is intended for professionals, managers and executives earning a monthly salary of at least S\$3,600, or the S-Pass, which is intended for skilled staff earning a monthly salary of at least S\$2,300. Work permits are intended for semi-skilled employees. The Singapore Ministry of Manpower imposes quotas on the number of work passes which a company may apply for.

In addition, under the Fair Consideration Framework, job vacancies must be first advertised to Singaporeans on the Jobs Bank, a Singapore government portal, for at least 14 calendar days before an application for a work pass may be made in respect of that position. This requirement may be waived if the position has a fixed monthly salary of at least S\$15,000, the company has less than 10 employees, the employment term is less than one month, or the position is to be filled by an "intra-corporate transferee". Under the World Trade Organisation (WTO) General Agreement on Trade in Services, an intra-corporate transferee is a person holding a senior position in an organisation or possessing an advanced level of expertise.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Singapore's intellectual property (IP) regime is consistently ranked as one of the best in the world. Singapore is ranked third in the world and top in Asia for having the best IP protection in the World Economic Forum's Global Competitiveness Report 2018.

Intellectual property rights are protected in Singapore via legislation, such as the Copyright Act, Registered Designs Act, Patents Act, and the Trade Marks Act, and under the common law, such as the laws of contract and confidentiality.

Original works of authorship, including software code and app content, are protected by copyright. Singapore's Copyright Act expressly recognises computer programs as literary works – the typical protection term is the creator's lifespan plus 70 years. No formalities are required for copyright.

The external appearance of an article or non-physical product may be registered and protected under the Registered Designs Act. Applications may be filed with the Registry of Designs in the Intellectual Property Office of Singapore (IPOS) or under the Hague Agreement Concerning the International Registration of Industrial Designs, administered by the World Intellectual Property Organisation (WIPO).

An invention of a product, process, or technical improvement to existing technology may be protected by a patent. Applications may be filed with the Registry of Patents in IPOS, or under the Patent Cooperation Treaty administered by WIPO.

Business names and logos may be protected as trade marks under the Trade Marks Act or Singapore's common law. Applications may be filed with the Registry of Trade Marks in IPOS, or under the Madrid Protocol administered by WIPO. Singapore is also a party to the Nice Agreement Concerning the International Classification of Goods and Services for the Purposes of the Registration of Marks. Trade mark protection is typically granted for a term of 10 years from the registration date and may be renewed.

A design, trade mark, or patent application which is filed in Singapore can claim a right of priority against applications in other countries which are parties to the Paris Convention for the Protection of Industrial Property (**Paris Convention**), administered by WIPO or members of the WTO, and *vice versa*.

Trade secrets, know-how and research and development may be protected by contract, e.g. via confidentiality or non-disclosure agreements, and by the common law duty of confidentiality.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

As a general rule, under Singapore law, intellectual property rights created in the course of employment will be held by the employer. It is common in Singapore for employees to acknowledge this position in employment contracts or in proprietary information and inventions agreements.

Outside of employment:

- copyright typically subsists in the creator, and can be licensed, transferred or assigned;
- for designs, the owner is typically the creator, unless the design was created pursuant to a commission, in which case the owner is the commissioning party;
- for patents, the owner is typically the inventor, unless the patent is required to be granted to another person by virtue of any statute, rule of law, treaty, international convention or enforceable term of any agreement entered into with the inventor prior to the creation of the invention; and
- for trade marks, the owner is usually the successful applicant, subject to challenges by other parties.

Fintech businesses may wish to note in particular a new proposed amendment to Singapore's copyright law, providing an exception allowing users to copy lawfully accessed data for data analysis and mining, facilitating the use of AI and big data to generate insights.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

To enforce IP rights in Singapore, one may rely on Singapore law, registrations with IPOS, or international treaties and multi-jurisdictional rights.

A copyright claim can be brought by a creator who is a citizen or resident of Singapore, a member country of the Berne Convention, or a member country of the WTO.

A design, trade mark, or patent application which is filed in Singapore can claim a right of priority against applications in other countries which are parties to the Paris Convention or members of the WTO, and *vice versa*.

Singapore has an IP court, established in 2002, with specialist practitioners to resolve IP disputes.

WIPO has had a Singapore office since 2010 to, *inter alia*, promote arbitration and mediation for IP disputes.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

IP rights can be licensed, assigned or used as security under Singapore law.

Typically, IP rights may be licensed or assigned. A licence permits the licensee to use the IP rights for certain specified purposes, whilst the licensor retains ownership. An assignment involves the full or partial transfer of ownership to the assignee.

It would be prudent for a licence or assignment to be made in writing and signed by the parties. The requirements differ depending on the type of IP and the terms of the agreement. For example, the Trade Marks Act expressly states that a trade mark licence is not effective unless it is in writing and signed by or on behalf of the grantor, and the Registered Designs Rules imposes a similar requirement implicitly by stating that the signature of the licence grantor is required for records; although the Patents Act does not have an express requirement for the form of licence.

Licences and assignments of registrable IP rights are also registrable transactions. An unregistered licence for a registered design, patent or trade mark may be ineffective against a person acquiring a conflicting interest. The Patents Act and Registered Designs Act impose limits on the rights to damages or account of profits for infringement occurring between the date of the licence and the date of registration of the licence.

The Civil Law Act stipulates that the agreement should be in writing and signed if it is not to be performed within one year of the date of the agreement.

A charge created over a company's IP rights should be registered with ACRA within 30 days of creation.



Andrea Chee

AEI Legal LLC
1 Phillip Street
Royal One Philip #05-01
Singapore 048692

Tel: +65 9795 4673
Email: andrea.chee@aeilegal.com
URL: www.aeilegal.com

Andrea has over 16 years of experience as a lawyer in Singapore and Hong Kong.

Before founding AEI Legal, Andrea was a partner at one of Singapore's leading law firms, leading a team in its corporate finance division. Prior to that she worked in the Hong Kong offices of a Magic Circle law firm.

Her practice focuses on cross-border and domestic mergers and acquisitions (M&A), equity capital markets (ECM) and technology, media and telecommunications (TMT) law.

Andrea has been recommended in *The Legal 500 Asia Pacific* (2015), the *JFLR 1000* (2016) and *The Legal 500 Asia Pacific* (2017).



Law Zhi Tian

AEI Legal LLC
1 Phillip Street
Royal One Philip #05-01
Singapore 048692

Tel: +65 9069 5321
Email: law.zhitian@aeilegal.com
URL: www.aeilegal.com

Zhi Tian's main areas of practice are cross-border and domestic mergers and acquisitions (M&A), equity capital markets (ECM), and technology, media and telecommunications (TMT) law.

She regularly advises clients regarding regulatory and compliance issues including in relation to fintech, data protection and privacy. Zhi Tian has been involved in cross-border M&A transactions, and in early and growth stage investments.

Prior to joining the firm, she trained in dispute resolution in a reputable firm involved in commercial and civil litigation matters.



A boutique corporate law firm of choice, AEI Legal was founded by a team from one of Singapore's leading law firms, and has through high standards and effective advice won mandates from a wide swathe of clients including multinational corporations, listed issuers, family offices and startups.

AEI Legal's practice areas include fintech, data protection and privacy, mergers and acquisitions, startups, venture capital, family offices, equity capital markets and IPOs, and regulatory and compliance advisory.

AEI Legal was a finalist in the "Rising Law Firm" and "Transactional Boutique Law Firm of the Year" categories of the 2019 SE Asia Law Awards.

Slovenia

Schoenherr

Jurij Lampič



1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

In Slovenia, standalone fintech businesses predominately cluster in the alternative (electronic) payments sub-sector, offering services such as mobile payments, mobile wallets and virtual credit cards. There seems to be early stage activity in other fields as well (peer-to-peer lending and insurance tech).

Established businesses have been essential drivers of innovation in the field since at least 2001, which marked the introduction of Moneta, a homegrown mobile payment solution developed by leading local software vendors and operated until recently as a joint venture of Telekom Slovenije, national telecoms operator, and Nova KBM, a leading bank. Slovenian banks have offered internet banking since the late '90s and now almost uniformly offer mobile banking as well. They continue to expand their online offerings, exploring, *inter alia*, online lending and e-banking chatbots. Petrol, the national energy company, recently entered into strategic partnership with mBills to jointly offer the eponymous mobile wallet service. Halcom, a local software developer, offers e-banking and e-certification solutions providing infrastructure for the operation of fintechs and traditional banks.

Slovenia also hosts a lively cryptocurrency business community, with a number of firms plausibly qualifying as fintechs. Among these, Bitstamp, one of the oldest cryptoassets exchanges, has been a runaway success (it was founded in Slovenia in 2011 but has since relocated to Luxembourg). Examples of other fintech-oriented locally founded cryptobusinesses include ICONOMI (formerly Cashila; (crypto)asset management), Bitnik (Bitcoin ATMs) and Hiveterminal (blockchain-based invoice financing).

While not necessarily fintech business *per se*, online crowdinvesting platform Conda has entered the Slovenian market and tailored its offering to comply with local laws.

In the public sector, innovation can be observed in the field of financial regtech. The Financial Administration of the Republic of Slovenia (*Finančna uprava Republike Slovenije*), the tax authority, has long enabled submissions of (personal) income statements as well as other tax-related tasks to be performed online, and has recently launched a mobile app version of their eDavki portal. The Administration has also developed a mobile app to crowdsource

enforcement of VAT rules, incentivising consumers with cash prizes to scan QR codes on invoices they receive through the app.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

There are no statutory bans or restrictions specifically targeting fintech activity (including cryptocurrency businesses) in Slovenia. Depending on their nature, fintech services may be subject to restrictions or (licensing) requirements under sectoral and/or general legislation (see in particular question 3.1 below). Several regulators have issued guidance and recommendations in respect of cryptocurrency activities (see question 3.2 below).

While not a ban *per se*, the Slovenian Payment Services Act (see question 3.1 below) somewhat limited the use of fiduciary bank accounts for businesses holding client funds (which will be necessary for effective operation of many fintech use cases). Rules have now been amended such that entities termed “central counterparties” will be allowed to open such accounts.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

Startups, SMEs and similar types of businesses (including fintechs) may take advantage of all common forms of funding, with key local sources listed below:

- **equity** (capital injections) or **quasi-equity** (convertible/subordinated loans) **financing** is typically offered to qualifying businesses by venture capital firms, business angel groups (e.g. *Poslovni angeli Slovenije*), various startup accelerators and the Slovene Enterprise Fund (*Slovenski podjetniški sklad*; see question 2.2 below);
- **debt financing** from commercial lenders is generally harder to obtain by early stage businesses; the market gap is filled by SID Banka, a Slovenian state-owned import-export bank, which offers debt financing to qualifying SMEs. In addition, the Slovene Enterprise Fund offers microloans (up to EUR 25,000) and loan guarantees, which may in turn facilitate access to (traditional) bank loans; and
- **non-refundable grants and subsidies** offered by the Slovene Enterprise Fund or – on an *ad hoc* basis – other government agencies or entities.

Slovenian startups have also made use of international and regional crowdfunding platforms, such as Kickstarter, Indiegogo and Conda, which offer various funding models ranging from supporters' contributions in exchange for early product delivery to subordinated loans.

Finally, many blockchain-oriented companies were able, in particular in 2017 and 2018, to take advantage of a regulatory arbitrage opportunity enabled by initial coin offerings ("ICO"). As of 2019, this funding model is notably less prevalent compared to previous years due to regulatory uncertainty, general cooling of blockchain-related enthusiasm and less volatile markets in cryptoassets.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

Investment incentive schemes are mainly targeted at facilitating access to finance for startups and SMEs. Key such instruments are grants and debt financing provided by the Slovene Enterprise Fund under the recently adopted Investment Promotion Act to companies qualifying as either "high added value companies" (companies with added value per employee over 50% over the Slovenian average, among other conditions), or "innovative startup companies" (companies marketing an innovative product or service or a high-potential business model, as defined by the Act). The Act mandates the establishment of a public register of such companies, which is available at <https://podjetniskisklad.si/sl/register/register-podjetij-z-visoko-dodano-vrednostjo> and <https://podjetniskisklad.si/sl/register/register-inovativnih-zagonskih-podjetij>.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

A company wishing to launch an IPO and list on a Slovenian organised market will need to follow two key sets of rules:

- *capital markets regulations and general corporate law*, with the key requirement being the publication of a prospectus approved by the Securities Market Agency; the mandatory substance of a prospectus is prescribed by the Market in Financial Instruments Act (implementing the Prospectus Directive) and (delegated) EU legislation; and
- *rules of the organised market/trading venue*, such as the Ljubljana Stock Exchange (LJSE), containing further listing requirements; the LJSE generally offers two main types of public listing – Prime Market and Standard/Entry Market – with differing requirements in terms of liquidity, disclosure, governance, management structure, business prospects, financial requirements and adequate distribution of the share capital among investors.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

Bitstamp, one of the oldest cryptoassets exchanges, was acquired by NXMH, the Belgium-based arm of the South Korean tech investment holding NXC, in 2018. One of Bitstamp's founders retained a 10% stake post-exit and remains the CEO.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

Fintech as such does not attract specific regulation in Slovenia. Depending on the business model, the following statutes (of general application) may apply to a fintech firm or its offering (by way of summary):

- the Payment Services, Services of Issuing Electronic Money and Payment Systems Act (implementing, *inter alia*, the Payment Services Directive 2 and the E-Money Directive) ("Payment Services Act"), which regulates payment services, issuance of electronic money and licensing of payment institutions and electronic money issuers;
- the Market in Financial Instruments Act (implementing, *inter alia*, the MiFID II and Prospectus Directive – soon to be replaced by the Prospectus Regulation), which regulates the provision of investment services, (initial) public offerings of securities and licensing of brokers and investment firms;
- the Banking Act (implementing, *inter alia*, the Capital Requirements Directive IV), which regulates credit institutions and their licensing; note that financial services as defined under the Banking Act (including B2B lending) do not require a licence if not performed by a bank and unless qualifying as a licensed activity under different sectoral legislation;
- the Consumer Protection Act, which regulates distance marketing of financial services and other aspects of consumer protection; and the Consumer Credit Act (implementing, *inter alia*, the Consumer Credit Directive), which regulates licensing of (non-bank) consumer credit providers and conduct of businesses in respect of consumer lending;
- the Insurance Act (implementing, *inter alia*, the Insurance Distribution Directive), regulating licensing of insurance companies, insurance distribution and conduct of business in offering of insurance products;
- the Investment Funds and Management Companies Act (implementing, *inter alia*, the UCITS IV Directive) and Alternative Investment Fund Managers Act (implementing, *inter alia*, the Alternative Investment Fund Managers Directive);
- the Prevention of Money Laundering and Terrorist Financing Act (implementing, *inter alia*, the Fourth AML Directive – see also question 4.5 below) ("AML Act"); and
- rules of general application such as the mandatory provisions of the Code of Obligations and Companies Act, Employment Relationship Act (see questions 5.1 to 5.3 below), General Data Protection Regulation ("GDPR") and the accompanying Personal Data Protection Act (see questions 4.1 to 4.3 below), e-privacy legislation, tax legislation, etc.

As with most cases of technology entering regulated sectors, the key legal challenge lies in mapping the fintech service's business model onto the existing regulatory regime.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

No, save for a reference to entities issuing and managing virtual currencies in the AML Act (see question 4.5 below).

However, several national regulators have followed EU bodies in issuing non-binding guidance or recommendations addressing common legal considerations in respect of cryptocurrencies:

- the Bank of Slovenia (*Banka Slovenije*) published "*Questions and answers on virtual currencies*", expressing its view on

the legal nature thereof (virtual currencies are neither legal tender, foreign currencies nor electronic money in the sense of the E-Money Directive, but no legal obstacles exist for them to be used as means of exchange) and warned users and businesses active in the field of the risks involved (available in English at <https://www.bsi.si/en/media/1180/pogosta-vprasanja-in-odgovori-o-virtualnih-valutah>);

- the Securities Market Agency (*Agencija za trg vrednostnih papirjev*) published a position paper on raising of capital utilising blockchain, in which it summarises views of the Agency on the legal nature of ICOs after soliciting input from several industry and academic stakeholders; the Agency indicates that the “security token”/“utility token” distinction may be relevant to future regulation of the field (available in Slovene at https://www.a-tvp.si/Documents/Naslovnica/Povstercki/Staliska_ATVP_ICO.pdf);
- the Slovenian Financial Stability Board (*Odbor za finančno stabilnost*), a macroprudential body, issued a warning on risks associated with cryptocurrencies and ICOs, aimed primarily at consumers (available in Slovene at https://www.a-tvp.si/Documents/Naslovnica/Opozorila_ICO/OFS_izjava_za_javnost_glede_virtualnih_valut.docx);
- the Financial Administration of the Republic of Slovenia (*Finančna uprava Republike Slovenije*), the tax authority, published guidance on the perspective of tax treatment of mining and trading cryptocurrencies in relation to personal income tax, corporate income tax, value-added tax and financial services tax (available in Slovene at http://www.fu.gov.si/fileadmin/Internet/Davki_in_druge_dajatve/Podrocja/Dohodnina/Drugi_dohodki/Opis/Davcna_obravnavna_poslovanja_z_virtualnimi_valutami_po_ZDoh-2_ZDDPO-2_ZDDV-1_in_ZDFS.docx); and
- the Office for Money Laundering Prevention (*Urad Republike Slovenije za preprečevanje pranja denarja*), the AML watchdog, published (i) a warning to the addressees (including natural persons exercising their professional activities) engaged in “trading” or “issuing” Bitcoin to observe AML legislation and pay special attention to Bitcoin transactions (available in Slovene at http://www.uppd.gov.si/fileadmin/uppd.gov.si/pageuploads/dokumenti/Bitcoj_n_obvestilo.pdf), and (ii) guidance on performing the KYC procedure/source of funds identification in cases where a client claims to have obtained the funds through cryptocurrency trading (available in Slovene at http://www.uppd.gov.si/fileadmin/uppd.gov.si/pageuploads/mnenjaZPPDFT/usmeritve_virtualne_valute_izvor_sredstev_objava_10.04.2018.docx.pdf).

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

The Slovenian government is keen to improve the local business and legal environment for startups and SMEs, with a particular focus on facilitating the adoption of blockchain technology. In 2017, the Ministry for Economic Development and Technology – in consultation with industry stakeholders – developed an action plan titled “Slovenia – the land of innovative startups”, identifying key legal and administrative obstacles to the growth of startups and SMEs (including the uncertainties regarding fiduciary accounts (see question 1.2 above) and language barriers (see question 3.4 below)) and defining steps for the mitigation of such obstacles (the “**Startups Action Plan**”). In addition, in 2018 the Ministry published a similar document in respect of accelerating the implementation of blockchain technology and drafting cryptocurrency regulation (the

“**Blockchain Action Plan**”). Policy proposals from both documents are currently in various stages of consideration, with some of them already seeing implementation (see, e.g., question 5.3 below regarding the foreign workers regime). While the Blockchain Action Plan mentions the regulatory sandbox approach, this option is not currently available in Slovenia.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

Regulated EU and EEA-based fintech businesses operating in regulated sectors may benefit from a passporting regime under statutes on payment services, e-money issuance, banking services, investment services, UCITS/AIF management and insurance services (by way of example), enabling direct provision of services on the basis of free movement of services. Such providers shall remain subject to direct supervision of their local regulator and will be able to operate compliantly in Slovenia by – for the most part – following the regulatory regime of their home Member State. In some cases, *Slovenian* laws specifically oblige passported service providers to comply with certain Slovenian rules, such as those on banking secrecy (as regulated by the Slovenian Banking Act), consumer protection, data protection and AML – fields which are largely harmonised on the EU level.

Service providers based in third countries will need to establish a local branch in order to operate in Slovenia, which applies to regulated as well as non-regulated businesses (under general corporate law).

In terms of hurdles, a degree of ambiguity is sometimes present with respect to language requirements in consumer communication. Under a broad interpretation of consumer protection legislation and provisions on public use of the Slovene language, all business (with no specific carve-outs for cross-border provision of services) with Slovenian consumers should be conducted in the Slovene language. Startups Action Plan mentions additional hurdles of a general nature, such as a physical presence requirement for transactions requiring notarisation, which is considered an impediment to foreign investment.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

Collection, processing, transmission and other aspects of personal data protection are primarily regulated by (i) the General Data Protection Regulation (“**GDPR**” – in force throughout the EU since 25 May 2018), and (ii) the Personal Data Protection Act. The latter covers subject matter not regulated by the GDPR, such as protection of the personal data of employees and video surveillance and is currently being amended to align it with GDPR (in particular with respect to sanctions provisions).

The following aspects of the data protection regime as regulated by the GDPR may be of particular relevance to fintech businesses (by way of example): (i) rules on automated decision-making, including

profiling (e.g. with respect to algorithmic creditworthiness assessments); (ii) conditions for consent; (iii) rules on international transfers of data (see also question 4.2 below); (iv) rights of data subjects (e.g. right to erasure and data portability); and, tying to the previous point; (v) the concept of “privacy by design and by default”.

In addition, fintechs may be – depending on their business model and regulated entity status – subject to statutory secrecy obligations (applicable to client data in general), such as banking or insurance secrecy, and an equivalent duty obliging payment system providers. Of particular relevance to fintech, the Payment Services Directive 2 eases access to consumer banking data for alternative payment services providers (the so-called “open banking” concept), while simultaneously giving banking clients more control over their data.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

Yes, the GDPR applies extraterritorially to any entity processing personal data of data subjects residing in the EU, regardless of whether the entity itself (a processor or a controller) is located within the EU.

The GDPR allows for a free flow of personal data of EU residents within the EU but restricts transfers of data to third countries. In summary, the transfer of personal data outside of the EU is allowed subject to: (i) an adequacy decision of the European Commission in respect of a third country (designating data protection regimes of third countries “adequate” for the purposes of data transfer); or, in the absence of an adequacy decision (ii) “appropriate safeguards” for the transfer being in place, such as the use of binding corporate rules (facilitating intra-group transfers), the use of standard data protection clauses adopted by the European Commission (for transfers to third country-based unrelated entities), and in certain specific situations (which include the presence of the individual’s consent, necessity of the transfer for the performance of the contract or public interest).

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

As of March 2019, the sanctions regime remains contained in the Personal Data Protection Act which is not yet aligned with the GDPR in this respect, and thus envisages administrative penalties of up to EUR 12,500. Note that an amendment to the Act, currently in the legislative pipeline, will significantly increase the penalties, bringing them as high as 4% of the total worldwide annual turnover of the preceding financial year in respect of the infringing undertaking (in line with the GDPR).

Apart from administrative sanctions, breaching entities or individuals may face civil liability and – for particularly grave infringements – criminal liability (e.g. under the criminal offence of misuse of personal data).

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

Fintechs, including payment services providers, may – again depending on their business model and regulated entity status – fall under the remit of any (or several) of the following cyber security/cyber resilience regimes:

- (i) the Information Security Act (implementing, *inter alia*, the NIS Directive), under which an “essential service operator”

may be subject to enhanced cybersecurity obligations; the Act lists banking and financial market infrastructure as sectors potentially falling under the remit of the “essential service” designation;

- (ii) sectoral regulation (see question 3.1 above), to the extent addressing operational conduct and risk management of regulated entities; a substantial body of EU hard and soft law exists in the area and covers payment systems providers as well; and
- (iii) obligations to maintain cyber security measures are also implicit in data protection and data privacy legislation; e.g., in the GDPR’s obligations for controllers and processors to implement “appropriate technical and organisational measures to ensure a level of security appropriate to the risk”.

The regimes listed above may apply in parallel to an individual entity. A Slovenian-specific aspect to note is the comparable strictness of the local privacy regime (enshrined in the Constitution and continuously reaffirmed by case law), which may restrict the use of certain customary cyber security-related measures, especially related to internal security – by way of illustration, comprehensive monitoring of employees’ online activities and communication at work designed to identify internal security risks may fall foul of employees’ rights to privacy.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

Due to the nature of their services, most fintech businesses will likely be subject to the AML Act (implementing the Fourth AML Directive), which imposes, *inter alia*, know-your-customer, monitoring and reporting obligations. Certain exemptions apply, including with respect to *de minimis* transactions and occasional transacting. Notably, the AML Act lists entities “issuing and managing” virtual currencies (specifically listing crypto exchanges operating as fiat on-ramps) as obliged entities thereunder. Severe cases of money laundering may be criminally prosecuted.

AML regulation globally is a fast-moving regulatory field and is set to change in the near future, with (i) additional (national and EU) regulatory guidance targeted at cryptocurrency transactions and businesses, (ii) the implementation of the Fifth AML Directive (EU Member States have until 10 January 2020 to implement its provisions; the Directive provides for a more comprehensive AML regime regarding virtual currencies), and (iii) a European Parliament roadmap on tackling of financial crime, tax evasion and tax avoidance (published on 26 March 2019), envisaging among other wide-ranging proposals a plan for an EU AML watchdog, European financial police force and EU financial intelligence unit.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

In addition to the regulatory regime outlined in other sections of this chapter, fintechs – as with any online business – may need to comply with local legislation implementing the E-Privacy Directive (soon to be replaced by the E-Privacy Regulation) and Directive 2000/31/EC (governing, *inter alia*, the provision of “information society services”), e.g. with respect to cookies, online (direct) marketing and liability of service providers.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

Key labour legislation provisions on hiring pertain to (i) the mandatory publication of a vacancy (for private sector employers as well), with certain exemptions, (ii) non-discrimination (e.g. a prohibition on advertising a vacancy as suitable for one gender only, unless the gender is a “material and decisive” requirement for the particular work), and (iii) limitations on fixed-term contracts (and chaining thereof) for permanent positions.

Dismissals are subject to relatively detailed procedural and substantive regulation (sometimes perceived as inflexible by the employers), with a closed set of eligible causes for termination: incompetence; redundancy (“business reasons”); breach of employment duties; disability; an unsuccessfully completed trial period; and additional extraordinary reasons (enabling fast-track termination – e.g. failure to show up at work for a certain period or severe breaches of employment duties). A terminated employee must be served with a carefully reasoned termination notice, upon which he or she is eligible for a notice period and (potentially) a severance pay-out. Certain categories of employees enjoy additional protection from termination. Special procedural rules exist in respect of handling mass redundancies.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Key mandatory employment benefits are as follows (by way of summary): 20 days of paid annual leave (with additional days accruing with years of service); paid maternity/paternity leave; paid sick leave; annual vacation top-up payment (“regres”); and (capped) reimbursements of commute and food costs incurred on working days.

In addition, employers are obliged to partially contribute towards employees’ social insurance payments (in respect of health, pension, social security and unemployment insurance). Additional employee protection rules apply, such as working hours limits, overtime, limits on the work of minors and a minimum wage.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

EU, EEA and Swiss citizens have unrestricted access to the Slovenian labour market on the basis of free movement of services.

In order to work or to be self-employed in Slovenia, individuals from countries not listed in the previous paragraph need to:

- obtain a so-called single work and residence permit (*enotno dovoljenje za bivanje in delo*); or
- qualify as one of several special categories of foreign nationals as set out in the Employment, Self-employment and Work of Foreigners Act, such as holders of a Slovenian temporary residence permit, holders of permanent residence permits, persons under international protection or asylum seekers.

The regime is considered relatively cumbersome and has been recognised as such in the Startups Action Plan. This has recently prompted a slight relaxation of conditions for hiring of foreigners by “high added value companies” and “innovative startup companies” (see question 2.2 above). Other than that, no special hiring routes are available to fintech companies.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Slovenian legislation provides for an internationally comparable regime of intellectual and industrial property protection provided by way of:

- copyright (for “individual intellectual creations in fields of literature, science and art, expressed in any form”, which includes software/code) and related rights, such as rights of creators of databases, publishers and film producers; and
- patents, designs (“models”), trademarks and certain additional sub-types (industrial property rights).

In addition, a company name (a “firm”) is protected from imitation by general corporate law, as well as by rules on unfair competition practices; the latter also prohibit unauthorised use of a brand or other signage of a company. Registered domain names (using the country-code top-level domain “.si”) can be safeguarded via a dispute resolution procedure administered by the registrar.

Local legislation is heavily influenced by EU rules and international treaties. Recent adoption of the EU Copyright Directive may have significant implications on the online (business) landscape in the EU and locally.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Copyright of the author generally arises by operation of law with the creation of a protected work, with no registration being required. Copyright remains valid for 70 years following the author’s death.

Industrial property rights take effect with registration, with several routes available in this respect (by way of example):

- national registrations at the Slovenian Intellectual Property Office;
- EU registrations at the EU Intellectual Property Office (for EU trademarks and designs) and European Patent Office (for EU patents); and
- international registration mechanisms administered by the World Intellectual Property Organization (WIPO).

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

Slovenia is a party to all significant international treaties on intellectual and industrial property, including the Berne Convention, WIPO Copyright Treaty (concerning copyright on software) and the TRIPS Agreement, and is a member of the European Union (see question 6.2 above regarding EU-wide protection mechanisms). This means that intellectual and industrial property rights of non-domestic origin will be enforceable in Slovenia in many typical cases.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

Intellectual property rights can generally be monetised through self-exploitation (e.g. manufacturing of a product by an inventor who obtained the patent therefor), licensing to third parties (in all standard modalities, e.g. exclusive/non-exclusive, worldwide/territorially limited, perpetual/for a set time period) and collateralisation (e.g. a pledge on a trademark or domain name). Examples of restrictions on monetisation and licensing include (i) non-transferability of the “moral” component of a copyright (e.g. right of attribution of authorship), (ii) compulsory licensing of a patent to the state in case of a prevailing public interest, and (iii) various statutory licences (including for use in a classroom or by the media and reproduction for private use).

An additional important feature of the regime is the automatic exclusive transfer of monetary components of a copyright on works created in the course of employment from the employee (the author) to the employer (this is the default regime – parties may agree otherwise). The rights in turn transfer back to the employee after a period of 10 years by operation of law, but the employer may re-acquire them by providing compensation; the 10-year limitation does not apply to databases and software, which remain with the employer in perpetuity in the absence of the agreement to the contrary. Note that this form of compulsory licence applies within *employment* relationships and will generally not be triggered in respect of contractors, necessitating the use of contractual copyright transfer provisions.



Jurij Lampič

Schoenherr
Tomšičeva ulica 3
SI-1000 Ljubljana
Slovenia

Tel: +386 1 200 09 80
Email: j.lampic@schoenherr.eu
URL: www.schoenherr.si

Jurij Lampič is a senior associate at Schoenherr Slovenia where he focuses on Banking & Finance and Corporate/M&A matters. He has extensive transactional experience in secondary debt market deals and has supported or advised clients in several domestic and cross-border transactions. Jurij is also regularly engaged in financing and restructuring projects, as well as in M&A, where he was a part of transaction teams in several high-profile Slovenian deals. He also advises on financial regulatory matters, especially in the field of capital markets regulation. Jurij is a member of Schoenherr's cross-jurisdictional technology & digitalisation group and has a particular interest in smart contracts and law/code intersection. Jurij holds a law degree from the University of Ljubljana's Faculty of Law and an MSc from the University of Oxford's Master in Law and Finance (MLF) programme, and passed the Slovenian Bar Exam in March 2018.

schönherr

Schoenherr Slovenia is a branch of the international law firm Schoenherr – Attorneys at Law, based in Vienna, Austria, which was one of the first foreign firms to enter the Slovenian market in 2001. Since then, our firm has developed into one of the leading law firms on the Slovenian market. Our team is comprised of around 20 lawyers, all experienced and focused on at least one of Schoenherr's practice areas. In addition to the firm in Ljubljana, the Schoenherr – Attorneys at Law firm has offices in 13 other locations/countries in CEE, as well as desks covering five further markets in the Balkans. We offer foreign and domestic investors the complete range of transaction support, including advice on large-scale privatisations, private equity investments, real estate acquisitions, financial debt restructurings and project finance, as well as non-transactional work such as competition advice, regulatory matters, employment and litigation.

South Africa



Angela Itzikowitz



Ina Meiring

ENSafrica

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

South Africa has witnessed an increase in fintech businesses over the last two years or so, and it is noticeable that a number of these businesses have attracted significant investment and funding from local and foreign investors alike.

The majority of fintech start-ups provide payments and money transfer services, with the rest of the market roughly divided between: trading, investment and crowdfunding; blockchain and Bitcoin; and lending, financing and retail banking services.

In the payment space, there is Karr, which, in partnership with Nedbank, launched a mobile payment app that facilitates parents paying for *ad hoc* events such as school shows, trivia nights, field trips, sports events and fundraisers while on the go – including auto-reminders for events.

Prospra is a mobile savings wallet for low-income South Africans that makes it easy to save small amounts infrequently using prepaid vouchers.

Akiba Digital is a gamified mobile app making it easier and more rewarding to set, manage and meet savings goals.

2019 will see the launch of three new digital banks, namely TymeBank, Bank Zero and Discovery Bank. TymeBank styles itself as the first digital-only bank. It does not have any banking branches and relies solely on digital means (mobile app and website) and kiosks housed predominantly in retail stores.

Discovery has launched what they term “the world’s first behavioural bank”, a fully functional digital bank that can be joined by anyone with a smartphone.

Bank Zero is a new app-driven bank, which is accessible to all customers and individuals with a smartphone. Bank Zero also offers its services through an app without a customer having to visit a branch.

Sureswipe is a card payment acceptance organisation that offers independent retailers and service providers an easy and accessible way to accept card payments and consolidate payment channels, simplifying the administrative burden of such providers as a result.

TransferWise is a money transfer system allowing private individuals and businesses to send money abroad at lower costs without any hidden charges.

Yoco is a highly successful fintech company in South Africa in the mobile payment service provider industry, targeting small to medium companies which require the portability of a card reader. In the past two years of operation, Yoco has raised US\$7 million.

As regards insurance, the Fo-Sho insurance product relies on policy holders forming groups with similar risk profiles to create savings pools to reduce the cost of risk financing and to mitigate excess payments in the event of a claim. The app gives the consumer the power to obtain insurance quickly, comfortably, and on their own terms in a very short space of time.

Self-labelled as the “Uber of insurance”, Riovic directly connects to risk managers and risk underwriters and allows private investors to accept a stream of certain cash flows in exchange for an uncertain future liability.

In the security and regulation fintech sphere, Bokio automates accounting and serves as a decision-making platform for small businesses – automatically handling invoicing, payroll and accounting.

With regard to payment and verification, the online verification system ThisIsMe allows individuals, businesses, regulators and financial institutions to link into Home Affairs and major banks.

In the property and investment space, KapitalWise – a cost-effective micro-investment platform for financial institutions – delivers personal investing literacy and predictive analytics to retail users of financial institutions.

In the Energy and Agriculture fintech industry, The Sun Exchange is a market place where consumers can buy into commercial solar projects at the scale of one cell at a time, using blockchain and smart contracts to facilitate transactions.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

The Banks Act, 1990 regulates the “business of a bank”, which is defined as the taking of deposits from the general public as a regular feature of its (the entity’s) business. Subject to certain exemptions, any person (natural or juristic) taking money from the public (which includes corporates) and who undertakes that the monies will be repaid on demand or otherwise, conditionally or unconditionally, and with or without interest, must register as a bank in terms of the Banks Act.

Similarly, peer-to-peer or market-place lenders are regulated by the National Credit Act, 2005 (“NCA”), which, subject to certain limited exemptions, obliges all lenders to register as credit providers, regardless of the quantum of the loan or the number of loans the lender has granted. The NCA is also prescriptive as to the

fees, interest and other charges that may be levied by a lender. Loan participations or sub-participants by non-banks may also fall foul of banking regulation, and be treated as deposits, even though these loan participations are often styled and drafted as a sale of rights or economic interests rather than a loan to the funder.

Virtual currencies, such as Bitcoin and other cryptocurrencies, are not currently regarded as legal tender. Bitcoin exchanges may, however, have to be licensed in due course. In terms of a consultation paper issued by the South African Reserve Bank dated 16 January 2019, exchanges and persons who keep crypto assets in safe custody will have to register with the Prudential Authority or the Financial Sector Conduct Authority (“FSCA”).

A person giving advice or rendering intermediary services, in respect of financial products, must register as a financial services provider under the Financial Advisory and Intermediary Services Act, 2002 (“FAIS”), and this is also true of the entity or person behind the “robo” adviser. Bitcoin and crypto assets are not currently regarded as financial products and are therefore not regulated by the FAIS Act.

Crowdfunding is not currently regulated under South African law. Going forward, crowdfunders may find themselves falling foul of the Banks Act, 1990 where the funding is by way of debt, and there is an obligation to repay or to register as an exchange under the Financial Markets Act, 2012 where the funding is by way of equity. The Financial Intelligence Centre Act 38 of 2001 (“FICA”) places Anti-Money Laundering (“AML”) obligations, including registration, customer due diligence, reporting and recordkeeping requirements on accountable institutions, in Schedule 1 of FICA.

As fintech poses increased risks of money laundering, going forward cryptocurrency exchanges and crypto assets service providers will be included as accountable institutions and, as such, will be obliged to comply with customer due diligence and all other obligations imposed on accountable institutions.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

Traditional loans are still commonplace, and peer-to-peer lending and crowdfunding appear to be on the rise, despite the regulatory hurdles referred to above.

Royal Fields Finance, a majority black-owned company, provides specialised short-term funding to SMEs and start-up ventures, without requiring risk capital contributions.

Government grant funding and soft loans by private companies to employment equity compliant fintechs are other avenues for raising capital.

Venture capital and private equity firms investing in fintech are also on the rise. A comprehensive list of venture capital and private equity firms is available on the website of the South African Venture Capital and Private Equity Association.

See also question 2.2 below.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

The Black Business Supplier Development Programme provides grant funding that encourages black businesses to grow by acquiring

assets and operational capacity, and provides a maximum investment of R1 million to a 51% black-owned entity, with 50% black management.

The Technology and Human Resources for Industry Programme, a project between the Department of Trade and Industry and the National Research Foundation, was implemented to improve South Africa’s technical skills and competitive edge through the development of technology. This grant, with a fund capacity of R150 million, is primarily aimed at engineering graduates and developing SMEs into large companies.

The CEO Initiative – under the auspices of the Minister of Finance to avert a ratings downgrade and foster inclusive economic growth – has announced a key milestone in establishing the R1.5 billion private sector fund to stimulate entrepreneurship and support the growth of SMEs.

The Incubation Support Programme is a grant aimed at assisting entities in developing incubator programmes and thereby creating employment within the communities, in turn strengthening the economy. The programme is aimed at encouraging partnerships between the private sector, SMEs and the Government in order to create sustainable growth within the economy.

The Section 12J Venture Capital Company (“VCC”) tax regime is a tax incentive that allows investors who invest in accredited Venture Capital companies, that then invest in small businesses, to make a tax deduction of 100% in the year that the investment was made. Although the underlying investments can include fintech offerings, there have been very few investments in tech start-ups to date, but with fintech on the rise, the Section 12J tax regime represents a major incentive for investment into fintech businesses.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

The Johannesburg Stock Exchange (“JSE”) is licensed as an exchange under the Financial Markets Act, 2012 and serves as South Africa’s premier exchange.

The principal requirements for a JSE Main Board listing include: subscribed capital of at least R50 million; not less than 25 million equity shares in issue, and 20% of each class of equity securities must be held by the public to ensure reasonable liquidity; and a satisfactory audited profit history for the preceding three financial years, where the last report must show an audited profit of at least R15 million before taxation and after taking account of the headline earnings adjustment on a pre-tax basis.

In addition, the company must be carrying on as its main activity, either by itself or through one or more of its subsidiaries, an independent business – supported by its historic revenue earning history – which gives it control over a majority of its assets, and must have done so for a prescribed period.

The JSE requires the appointment of a sponsor to list on the main board, whose responsibilities include advising the directors of their responsibilities and obligations, satisfying itself that the company is suitable to list, and liaising between the JSE and the company.

The JSE furthermore requires an accredited independent accountant to report in the prospectus or pre-listing statement on, amongst other things, the profits and financial position of the company over the preceding three years.

The JSE may, in exceptional circumstances, list companies that do not comply with these requirements.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

We are not aware of any notable exits in the fintech industry for 2019, but the ICO industry has slowed considerably.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

See question 1.2 above and section 4 below.

Money laundering in South Africa is regulated by FICA and the Prevention of Organised Crime Act, 1998 (“POCA”) and the regulations promulgated thereunder. The latter sets out the money-laundering offences, while the former (for the most part) provides the administrative framework for regulating anti-money laundering. FICA was recently amended by the FICA Amendment Act, which introduced a risk-based approach to client due diligence. “Accountable institutions”, as defined in FICA, include banks, insurers, money remitters, investment advisers and the like. Accountable institutions are subject to onerous compliance obligations, including identifying and verifying customers and record-keeping as well as registering with the Financial Intelligence Centre (“FIC”). Fintech companies that do not fall within the definition (of an accountable institution) are exempt from these obligations, and the monitoring and screening of transactions becomes increasingly difficult where transactions are conducted cross-border using financial technology. It is interesting to note in passing that mobile phone operators are not accountable institutions for purposes of FICA.

The SARB and the FIC have recommended that cryptocurrency asset service providers should comply with FICA. Among other things, this would require South African cryptocurrency asset providers to do the following:

- Register with the FIC as accountable institutions, conduct due diligence of clients and keep records. This also includes monitoring transactions and compiling and filing reports on any unusual or suspicious crypto transactions, and reporting cash transactions of R24,999 and above (see the proposed amendment to this threshold discussed in question 3.2 below).
- Adopt a risk-based approach to customer due diligence.
- Ensure complete compliance with FICA or risk facing remedial action, which would include administrative sanctions.

The National Payment System Act, 1998 regulates the provision of payment services, including clearing settlement, payment processing, and the like. Subject to limited exceptions, only registered banks are allowed to clear and settle payment instructions between banks within the national payment system. The Payment Association of South Africa has been appointed by the South African Reserve Bank (“SARB”) as the payment system management body which organises, manages, oversees and regulates, in relation to its members, all matters affecting payment instructions.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

Not as of yet.

The SARB, together with other financial services regulators (the FIC, the FSCA and National Treasury), are embarking on a process of “limited” or “lite” regulation of cryptocurrencies or crypto assets.

In January 2019, the SARB released a consultation paper outlining its proposals for the way forward and inviting members of the public and industry stakeholders to send their comments.

Once public and stakeholder comments have been collated, the SARB plans to issue a policy paper for release in the second quarter of this year.

The SARB is aware of the risk of fraudulent activities, such as money laundering, terrorist-financing activities, the circumvention of exchange controls, and the masking of illicit financial flows, particularly from the anonymity of dealing in crypto assets.

With regards to the regulation of anti-money laundering, the SARB proposes that crypto asset service providers be required to:

- register with the FIC (as accountable institutions);
- conduct customer due diligence, including ongoing monitoring;
- keep records, and
- file reports on suspicious and unusual transactions, cash transactions of R24,999.99 and above, and (if aware) any property that it either possesses or controls that may be linked to terrorist activity or terrorist organisations. The FIC, however, has released a consultation paper relating to the amendment of regulations in respect of cash threshold reporting and aggregation.

It is proposed that the cash threshold amount of R24,999.99 be increased to R49,999.99. The obligation to report information concerning cash transactions will therefore arise when a transaction is concluded with a client by means of which the cash paid or received totals is R50,000.00 and above.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

Financial markets are tightly regulated in South Africa, and while such regulation is necessary to protect consumers and the sector from systemic risk, it does create high and sometimes insurmountable barriers to entry for fintech innovators. While the regulators are open to discussion with these innovators, and are giving serious thought to the regulatory challenges posed by fintech, they have been slow to adapt regulations to embrace fintech. Unlike other jurisdictions, such as Singapore and the United Kingdom, neither the SARB nor the FSCA (previously the FSB) have to date created regulatory sandboxes for these companies.

The SARB is exploring cryptocurrencies and blockchain and is interested in innovations that may stem from its development; and, recently, a number of South African banks have pushed ahead with plans to test blockchain applications in a partnership that has drawn support from the SARB and the FSCA.

On 31 January 2019, the SARB released a media statement where it confirmed that it is joining the Global Financial Innovation Network (“GFIN”) as a member. This is part of SARB’s journey to support responsible financial innovation for the benefit of all South Africans. Joining GFIN will provide the SARB with the opportunity to share and gain insights from its fellow regulations on experiences in enabling innovation.

The GFIN will pilot the hosting of cross-border trials by financial entities through the regulatory sandboxes of those members who

have chosen to participate in the pilot. Although the SARB supports this initiative, it has elected not to partake in the pilot in order to first focus on the appropriateness and feasibility of a SARB regulatory sandbox. The SARB will first put in place a process that is fair and open for South African firms, and ensure that consumer protection is in place for citizens who are clients of those companies participating in the trials.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

See question 1.2 above and section 4 below.

A foreign company offering fintech products and services is required to register as an external company in terms of the Companies Act, 2008 within 20 business days after it first begins conducting business within the Republic.

Direct marketing to customers in South Africa is stringently regulated in terms of the Consumer Protection Act, 2008 (“CPA”) and the Protection of Personal Information Act, 2013 (“POPI”).

South Africa still has a system of exchange control and, subject to exemptions, persons wishing to remit money cross-border would have to apply for permission from the SARB or entities authorised to deal in foreign exchange.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

POPI has been signed into law, but has not yet come into full force. Certain provisions relating to the establishment of the Regulator and the issuing of regulations under POPI, however, came into force on 11 April 2014.

The effective date of the remainder of the provisions under POPI will not be prior to the Information Regulator becoming operational, which may only be in the first few months of 2019.

The Regulations relating to the Protection of Personal Information, 2018 (“the Regulations”) were published under GN R1383 on 14 December 2018. The Regulations are highly administrative in nature and do not necessarily assist organisations in interpreting POPI to ensure compliance. As a result, the Regulations do not substantially alter that which needs to be complied with. Although the Regulations are final, the Regulations will only commence on a date to be determined by the Regulator by proclamation in the Government Gazette. The commencement date of the Regulations will be aligned with the POPI commencement date.

A responsible party (defined in POPI as “a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information”) is given a one-year transitional period after the commencement of the Act to comply with the provisions of POPI. This period may be extended by the Minister of Justice by an additional period which may not exceed three years.

POPI applies to the automated or non-automated processing of personal information entered into a record in any form (provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof) by or for a responsible party who or which is domiciled in South Africa, or not domiciled in South Africa, unless the processing relates only to the forwarding of personal information through South Africa.

Fintech businesses will undoubtedly constitute responsible parties and will have to comply with the eight conditions for lawful processing of personal information set out in Chapter 3 of POPI when collecting, using, transmitting, or otherwise processing personal information.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

See question 4.1 above.

Section 72 of POPI regulates the transfer of personal information outside South Africa. Consent of the data subject is a sufficient justification for the transfer of such information. The transfer may also be done without the consent of the data subject if, among other things, it is done for the benefit of the data subject, and obtaining the consent of the data subject is not reasonably practicable; and, if it were reasonably practicable, the data subject would be likely to give it.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

The unlawful processing of personal information and the unlawful disclosure of such information to a third party could lead to delictual (tort) liability and damages, as well as a breach of POPI.

A contravention of POPI could also lead to a fine or to imprisonment for a period not exceeding 10 years, or to both such fine and imprisonment. A responsible party who is alleged to have committed an offence in terms of POPI may also be liable to an administrative fine up to the amount of R10 million.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

The current legal framework to combat cybercrime is a hybrid of legislation and the common law. The common law, which develops on a case-by-case basis, has failed to keep up with the nature of cybercrime.

The Cybercrimes Bill is nearing the stages of becoming law, as it was passed by the National Assembly on 27 November 2018. The Cybercrimes Bill seeks to create offences which have a bearing on cybercrime, to criminalise the distribution of data messages which are harmful, and to provide for interim protection orders, among other issues.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

The statutes regulating money laundering are POCA (referred to in question 3.1) and FICA (referred to in question 1.2). The statute regulating the financing of terrorism is the Protection of

Constitutional Democracy against Terrorist and Related Activities Act, 2004. Regulations promulgated under these Acts clarify and amplify the various obligations and provide for certain exemptions. As to money-laundering regulation, POCA (as the main regulation) contains the substantive money laundering provisions, while FICA provides the administrative framework. (See also question 3.1 above.)

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

See question 1.2 above.

In addition, the scope and application of the CPA is extremely wide. It applies to: (a) the promotion of goods (defined to include any game, information, data, software, code or other intangible product written or encoded on any medium or a licence to use any such intangible product) and services; (b) all transactions for the supply of goods and services between suppliers and consumers (unless specifically exempt); and (c) the goods and services themselves once the transaction has been concluded.

The CPA will apply fully to fintech businesses that provide products or services to natural persons or juristic persons with an annual turnover or asset value not exceeding R2 million (at the time the transaction is concluded).

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

Businesses do not encounter any restrictions in relation to the hiring of their staff. The Labour Relations Act 66, 1995 (“LRA”), however, requires dismissals to be both substantively and procedurally fair. Therefore, a dismissal must be effected for a fair reason and in accordance with a fair procedure. The LRA provides for three categories of dismissals: dismissals for misconduct; incapacity (poor work performance, ill health or injury); and dismissals for operational requirements.

5.2 What, if any, mandatory employment benefits must be provided to staff?

There are no mandatory employment benefits that must be provided to staff. Employers grant their employees benefits on a discretionary basis.

The Basic Conditions of Employment Act, 1997 confers certain rights on employees, for example:

- paid annual leave (21 days in an annual leave cycle);
- paid sick leave (six weeks during a 36-month cycle);
- maternity leave (four consecutive months); and
- paid family responsibility leave for child births, child sickness and familial deaths (three days in an annual leave cycle).

The Act also regulates the number of hours worked by employees to 45 hours in any week. This limitation on hours worked, however, only applies to employees earning below the threshold set by the Minister of Labour.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

Any foreign national who is not a permanent resident of South Africa and who wishes to render services in South Africa needs to obtain a work visa in order to do so. In terms of the Immigration Act, 2002, foreign nationals will be allowed to work in South Africa if they have Intra-Company Transfer Work Visas or Critical Skills Work Visas.

Intra-Company Transfer Work Visas allow foreign nationals to be transferred from a business abroad to a local branch, subsidiary or affiliate. Critical Skills Work Visas are granted to candidates who possess special expertise and know-how in relation to a particular industry, which is listed by the Department of Labour. Each of these visas have particular requirements that must be met.

A foreign national is obliged to obtain his/her visa through application to the South African consular office in his/her country of ordinary residence or home country. If there is no consular office, then the foreign national must apply by courier to his/her closest South African foreign mission or to the Department of Home Affairs in South Africa.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

In South Africa, innovations, inventions and other creations of the mind are protected by well-established intellectual property laws. The main pieces of legislation that regulate the creation, ownership, protection and enforcement of intellectual property rights include the Patents Act, 1978, the Designs Act, 1993, the Trade Marks Act, 1993 and the Copyright Act, 1978.

Depending on the nature of the innovation or invention, either one or more of these pieces of legislation may apply when seeking protection over the relevant intellectual property.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Patent – an application for a patent in respect of an invention may be made by the inventor or by any other person acquiring from him the right to apply, or by both such inventor or such other person.

Design – the proprietor of a design is either: (a) the author of the design; (b) where the author of the design executes the work for another person, the other person for whom the work is so executed; (c) where a person, or his employee acting in the course of his employment, makes a design for another person in terms of an agreement, such other person; or (d) where the ownership in the design has passed to any other person, such other person.

Trade Mark – the proprietor of a trade mark is the person who first used the trade mark in respect of goods or services, or the person who first registered the trade mark in respect of goods or services, whichever is the earlier.

Copyright – ownership of copyright in a work vests in the author or, in the case of joint authorship, in the co-authors of the work. However, the following exceptions apply:

- Where a literary or artistic work is made by an author in the course of his employment by the owner of a newspaper, magazine or similar periodical under a contract of employment, and is so made for the purpose of publication in said periodical, the owner of the periodical shall be the owner of the copyright in the work insofar as the copyright relates to publication of the work in said periodical or to reproduction of the work for the purpose of it being so published. In all other respects, however, the author shall be the owner of any copyright subsisting in the work.
- Where a person commissions the taking of a photograph, the painting or drawing of a portrait, the making of a gravure, the making of a cinematograph film or the making of a sound recording and pays or agrees to pay for it in money or money's worth, and the work is made in pursuance of that commission, such person shall be the owner of any copyright subsisting therein.
- Where a work is made in the course of the author's employment by another person under a contract of employment, that other person shall be the owner of any copyright subsisting in the work.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

South Africa has acceded to the Patent Cooperation Treaty, which makes it possible to seek patent protection for an invention simultaneously in each of a number of countries (including in South Africa) by filing an "international" patent application.

The Trade Marks Act affords protection to trade marks that are entitled to protection as well-known trademarks under the Paris Convention on the Protection of Industrial Property of 20 March 1883, as revised or amended from time to time.

The Copyright Act makes provision for the extension of the application of the operation of the Act to other countries by way of publication of a notice in the Government Gazette listing such countries. The last published notice was GN 136/1989 in Government Gazette 1178 dated 3 March 1989.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

Intellectual property rights may be exploited in a number of ways, including through licensing agreements, mergers or sales, joint ventures or collaboration agreements, and the like. Certain anti-competitive rules are prohibited from being included in such commercial agreements relating to the sale or licensing of intellectual property rights, in particular patents.

Acknowledgment

The authors would like to acknowledge Byron Bromham, Candidate Attorney, Banking and Finance, for his assistance during the preparation of this chapter.



Prof. Angela Itzikowitz

ENSafrica
The Marc | Tower 1
129 Rivonia Road
Sandton
South Africa

Tel: +27 83 680 2077
Email: aitzikowitz@ENSafrica.com
URL: www.ENSafrica.com

Professor Angela Itzikowitz is a director in ENSafrica's Banking and Finance department. She specialises in banking and financial market regulation, including finance and regulatory reform, card and related electronic payment instruments, derivatives, loan agreements, collective investment schemes, insurance, and fintech.

She has done a significant amount of work in South African Development Community ("SADC") countries such as Uganda, Kenya and Zambia, including regulatory law reform through capacity building projects. Angela has participated in a number of financial market initiatives in Asia in collaboration with colleagues from Beijing, Shanghai, Hong Kong and India. She also acts for a number of European banks, asset managers and investment advisors.

In addition, she has been recognised as a leading Fintech lawyer, advising banks and start ups.

Angela is recognised as a leading/recommended lawyer by:

- *Chambers Global Guide*: – (Band 1) Banking and Finance: Regulatory.
- *Who's Who* 2017, 2018 – Banking, FinTech (South Africa).
- *Best Lawyers®* 2018, 2017, 2016 – Banking and Finance (South Africa).

Angela is fluent in English, Afrikaans and German and speaks South Sotho and Mandarin.



Ina Meiring

ENSafrica
The Marc | Tower 1
129 Rivonia Road
Sandton
South Africa

Tel: +27 82 452 3450
Email: imeiring@ENSafrica.com
URL: www.ENSafrica.com

Ina Meiring is an executive in ENSafrica's Banking and Finance department. Ina is regarded as one of the top finance regulatory experts in South Africa and her clients include leading local and international financial institutions. Her experience includes advising on banking and financial services regulation and consumer law matters, including: the South African Consumer Protection Act, 2008; the National Credit Act, 2005; and the Protection of Personal Information Act, 2013. Her expertise further includes advising on corporate governance, exchange control, securitisations, payment instruments and payment methods.

Ina is a member of the expert group appointed by the South African Reserve Bank for the review of the National Payment System Act, 1998. She has authored chapters on South African banking regulation for a number of legal publications, and has lectured at the University of Johannesburg and the University of South Africa.



ENSafrica is an independent law firm with over 200 years of experience. The firm has over 600 practitioners in 14 offices on the continent, in Ghana, Mauritius, Namibia, Rwanda, South Africa, Tanzania and Uganda.

Spain

Leticia López-Lapuente



Isabel Aguilar Alonso



Uría Menéndez

1 The Fintech Landscape

- 1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).**

Mirroring the global trend, Spain's financial sector has faced disruptive changes over the last few years due to the entrance of a considerable number of fintech businesses. Although growth has not slowed down during the last year (it was estimated that there were 50 fintech companies in 2013, which have increased to 336 as of January 2019 – source: finnovating.com), a consolidation stage of the fintech business in Spain is expected to occur in the medium term.

Fintechs are present in all financial sectors, providing a wide array of services both to final clients and traditional financial entities. They are particularly active in sectors where intermediation between parties is fundamental, including in lending, FX, brokerage and investment services, such as investment advice and portfolio management. In those sectors, the development of platforms and big data, robotics and artificial intelligence tools represent the most recent trends in innovation (to date, mainly crowd-funding and crowd-lending platforms and robo-advisors). Fintechs are also highly involved in the Spanish payments sector, in which they have played a key role in the recent development of online and mobile payments. So-called third-party providers (“TPPs”) under PSD2 have also emerged in the Spanish market. TPPs mainly focus on offering customers mobile-account information services and personal-finance management solutions; however, their expansion into new, unexpected business areas is predicted in the near future. 2017 and 2018 have seen a growth in fintech business of above 40%.

The insurtech market has also experienced a significant growth, and as of February 2019, there are 185 startups in Spain related to this business. Further disruption is still expected in the insurtech market in the near future.

Although 2017 has been a year of rapid growth for initial coin offerings (“ICOs”) both globally and in Europe, 2018 has experienced a moderate growth in this market. In any case, it is expected that the ICO market will be further developed in Spain in the coming years. Apart from the above, the main disruption in the global financial sector is still expected to result from ledger technologies such as blockchain. Although the use of this type of technology is not yet widespread, it is expected to emerge in Spain in many areas, not limited to cybersecurity and cryptocurrencies.

In brief, the fintech sector is provoking a profound shift in the Spanish financial, investment and insurance sectors, encroaching on the *status quo* of traditional entities. As a natural result of the above, and in response to recent consumer patterns, the traditional model created by financial institutions is being pushed towards introducing new fintech elements into their product portfolio. For this reason, Spanish financial institutions have substantially increased their investment in fintech in 2017 and 2018. Meanwhile, fintech businesses must face significant challenges in connection with the provision of financial services, both regulatory (as detailed in question 3.1) and, in some specific cases, regarding their activity's compatibility with that of the owner of the data required for it to operate.

- 1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?**

The feasibility of setting up and operating a fintech or insurtech business in Spain should be analysed on a case-by-case basis. Although no fintech or insurtech business is prohibited or restricted in Spain *per se*, specific regulatory licences and compliance with regulatory requirements may be applicable in the financial and insurance sectors. However, except as explained in our response to question 3.1, as of the time of writing, there is no specific regulation governing fintech or insurtech companies in Spain.

Regarding cryptocurrency, Spain has not yet regulated this sector as it is awaiting the European Union's regulation of the matter. Therefore, for the moment, cryptocurrencies are not prohibited or restricted in Spain, nor are they recognised as a legal currency. Please refer to question 3.2 for more information.

2 Funding For Fintech

- 2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?**

Spanish law does not impose any restriction on the ability of fintechs to be funded via equity or debt. Nevertheless, at this point in time, most fintechs are financed through equity financing rounds at different stages, supported by an array of investors (private equity and venture capital houses, angel investors, and even specific institutions).

Crowd-funding has also grown as of late as a funding alternative for fintech companies; there are also growing fintech incubators (some financed by financial entities) and accelerators.

Traditional bank financing is also available; although, in practice, fintech companies in early stages of development usually face difficulties in demonstrating the required credit standing reliability based on a reliable business case.

IPOs on the Spanish Stock Exchanges and, particularly, on the Spanish Alternative Stock Exchange (requiring less stringent conditions for IPOs), represent additional, highly efficient financing alternatives for fintech businesses that have achieved a certain level of growth in the market.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

Yes: (i) the Spanish “patent box” regime and the research, development and innovation tax credit potentially applicable to Spanish resident companies engaged in tech/fintech activities, when dealing with advanced registered software; and (ii) the corporate income tax benefits for start-ups (e.g. a 15% rate for the start-up’s first two fiscal years, instead of the general 25% rate) and Spanish-resident venture-capital entities (*entidades de capital riesgo*); along with (iii) tax credits for “business angels” in specific start-ups (under specific conditions) represent the main tax incentive schemes for investment in tech or fintech businesses generally applicable in Spain. Proper structuring is essential for investors in these companies to mitigate any Spanish tax leakage applicable to investments in tech/fintech companies.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

Spanish legislation establishes the principle of freedom to issue and offer securities in Spain; nevertheless, the admission of securities to trading on official Spanish stock exchanges (i.e. a regulated market supervised by the National Securities Market Commission (the “CNMV”)) or on a multilateral trading facility (currently, the Alternative Stock Market, *Mercado Alternativo Bursátil* (“MAB”)), a self-regulated entity that has grown significantly in recent years) is subject to verification of specific eligibility and information requirements.

While distinct requirements apply for an IPO on the official Spanish stock exchanges as opposed to a listing on the MAB, common listing requirements include the following, among others: (i) the issuer must be a public limited company (*sociedad anónima*), or its equivalent under foreign law, validly incorporated and currently existing; (ii) the securities to be listed must meet all applicable legal requirements, and must be freely transferrable, represented in book-entry form, and grant the same rights to all holders in the same position; (iii) admission to trading is conditional upon submitting specific documentation to the appropriate regulator evidencing compliance with the legal framework applicable to the issuer and the securities, the issuer’s audited financial statements and a public offering or listing prospectus or informative document; and (iv) the application for admission to listing must cover all securities of the same class, and a minimum volume and a minimum distribution of the securities among the public are required.

Generally speaking, the MAB provides an alternative for small and medium-sized companies to access capital markets through a less burdensome legal framework. As opposed to the Spanish stock exchanges, the MAB does not require a minimum activity period (i.e., business projections are permitted even if the fintech business

has performed activities for fewer than two years). Also, while the official Spanish stock exchanges require a minimum capitalisation of EUR 6 million, only EUR 2 million is required for an IPO on the MAB. Thus, it may be an attractive, less onerous platform for growing fintech businesses to access capital markets.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

There have been no IPOs of Spanish core fintech companies in Spain. That said, some companies listed on the MAB provide services that are ancillary to the financial industry (e.g. Think Smart, Lleida, and Facephi).

However, both traditional banks and investors keep investing significant and growing amounts in Spanish fintechs. Among the most notable investments are Fintonic (financial aggregator) which has received EUR 25 million in a financing round led by ING Group and the insurer Previsión Sanitaria Nacional, Antai (venture building) which has received EUR 20 million from, among others, Banco Sabadell and Mutua Madrileña, MytripleA (financing for small and medium-sized companies) which has received EUR 15 million mainly from GLI Finance Limited, Peer Transfer (international educational payment tool), which has received EUR 18 million from Bain Capital and SpotCap (alternative financing platform), which received EUR 31.5 million from the private equity house Finstar Financial Group.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

As of today, there is no specific regulatory framework in Spain governing fintechs. This is mainly due to the fact that fintech businesses in Spain cover a vast range of activities.

In general, fintech businesses focused only on developing IT solutions to support the provision of services by financial entities are not currently subject to any financial regulatory regime. However, fintechs that engage in financial activities such as payment services, deposit-taking activities, investment services, payment services and insurance, are subject to the general regulatory regime that applies to any company operating in those sectors.

2018 brought the transposition into Spanish law of PSD 2, which, in broad terms (i) has recognised and established the Spanish regime applicable to the so-called Payment Initiation Services Providers and Account Information Services Providers – recognising for the first time the legal right for these companies to have access to information from traditional banks, (ii) has simplified the authorisation process for small-sized entities and entities operating only in Spain subject to financial regulatory authorisation, and (iii) has strengthened the obligations regarding payments security, including the reinforcement of requirements for online clients’ identification.

Cybersecurity and data protection regimes may also be applicable to certain fintech businesses, as well as other regulatory regimes, as described in section 4.

However, specific legal developments have already arisen in Spain in connection with some particular types of fintech businesses. This is the case for crowd-funding and crowd-lending platforms, which

are subject to Law 5/2015, of April 27, on the promotion of business financing, which, for the first time in Spain, regulates the activities of these platforms.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

As anticipated in question 1.2, Spain has not yet regulated this sector as it is awaiting the European Union's regulation of the matter. Therefore, for the moment, cryptocurrencies are not prohibited or restricted in Spain, nor are they recognised as a legal currency. This notwithstanding, ICOs may already qualify as financial instruments or fall within the scope of financial regulations depending on how they are structured. In this regard, both the European Securities Market Authority (the "ESMA") and the CNMV have issued certain guidelines reminding firms involved in ICOs of their regulatory obligations in connection with the Prospectus Directive, MiFID, the AIFMD and the anti-money laundering legislation. The same rules apply to the cryptoassets.

During the past years, the ESMA has been working with different National Competent Authorities (including the CNMV) in the analysis of the different business models of cryptoassets, the risks and potential benefits that they may introduce, and how they fit within the existing regulatory framework. Based on this work, the ESMA issued advice on ICOs and cryptoassets in January 2019. This report identified gaps in the existing regulatory framework in relation to ICOS and cryptoassets. We would expect further regulation from the EU Institutions on the basis of this advice and with the purpose of addressing the gaps identified by the ESMA.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

Although no active legislative or governmental action has yet been taken other than the approval of the laws for the transposition of PSD 2 in Spain and the regulation of crowd-funding and crowd-lending platforms, Spanish regulators show that they are receptive to the fintech activities. By way of example, the CNMV has created a section on its webpage aimed at establishing an informal communication space with financial entities and promoters of fintech businesses in which the latter may discuss and propose initiatives and be continually informed on legal developments and issues that may affect their projects. The insurance regulator (*Dirección General de Seguros y Reaseguros*) has also communicated to the industry the importance of the challenge that technology represents to the market.

On the other hand, the Spanish Fintech and Insurtech Association (*Asociación Española de Fintech e Insurtech*) is calling for a review of the current regulatory environment to promote the development of fintech businesses in Spain. In particular, the following measures are being proposed:

- (i) the implementation of a "regulatory sandbox", understood as a defined authorisation programme under which entities that meet specific requirements would receive a temporary, limited licence to test the market's reaction to their products and services;
- (ii) advice programmes offered by regulatory authorities to businesses that are ineligible for the regulatory sandbox programme; and
- (iii) certain regulatory amendments seeking to define which activities do not trigger licensing requirements and

establishing a licensing regime that is proportionate to the activities undertaken by fintechs. Among others, the amendments include the request of a longer deadline for the complete down-payment of the minimum capital requirements applicable to be eligible for certain regulatory licences (e.g. investment firms), the simplification of the conditions which are required in order to be authorised as a certain type of regulated entity, as well as various specific amendments to Law 5/2015, of April 27, on the promotion of business financing.

In July 2018, the Ministry of Economy and Business published the Draft Law for the Digital Transformation of the Financial System (the "Draft Bill"), which has been discussed by the Spanish Government in February 2019. The final text of the Draft Bill is not public at the moment. However, it is known that the purposes of such Draft Bill are: (i) ensuring that financial supervisory authorities have adequate instruments to keep performing their supervisory and regulatory functions within the new digital environment; and (ii) facilitating the innovative process in order to achieve better access to financing by productive sectors, more efficient financial services and a greater attraction of talent in a highly competitive international environment. In this line of promotion of digital innovation, the Draft Bill implements a regulatory sandbox in Spain, the terms of which are still unknown until the final text of the Draft Bill is published. The Draft Bill is under discussion and there is no specific deadline within which it will be passed.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

There are no specific regulatory hurdles for fintechs that are established outside Spain. These fintechs face the same entry barriers as those established in Spain, namely, the obstacles resulting from the provision of financial services that trigger licensing requirements. The current legal regime for the authorisation of financial entities, which is established by reference to EU law, does not provide for a simplified procedure for businesses that only provide a limited range of services, as is the case for many fintechs. Hence, as of today, fintechs providing regulated services such as payment or investments services must navigate complex and burdensome procedures in Spain or in their country of establishment before having access to customers.

Also, other requirements under other domestic legislation (e.g. those resulting from Spanish data protection laws) may create burdens on certain fintech businesses or activities that are designed to support the activities of financial companies, as described in section 4.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

Processing of personal data. The processing of personal data by fintech companies established in Spain is subject to certain data protection rules. At EU level, Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the

processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (“**General Data Protection Regulation**” or “**GDPR**”) exists, which has been directly applicable to all Member States of the EU, including Spain, since 25 May 2018. Therefore, the GDPR sets out the main rules that apply to the processing of personal data by fintech companies in Spain, including those regarding transparency of processing, consent and other legal basis for such processing, security duties, rules applicable to data breaches, appointment of data protection officers and other accountability duties. The GDPR aims to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the EU, which helps to homogenise privacy policies and compliance rules for those fintech business acting in other EU jurisdictions in addition to Spain.

That said, at a national level and in addition to GDPR, certain local data protection rules exist in Spain. In particular, a local data protection law was passed in December 2018, i.e. Spanish Basic Law 3/2018 on Data Protection and Digital Rights Guarantees (*Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales*, “**LOPD**”). The LOPD formally repealed the previous national data protection regulations, the content of which was incompatible with the GDPR, and adapted local rules for them to be compatible with the GDPR. The goal of the LOPD is not the implementation or modification of the GDPR, but rather (i) harmonising the Spanish law with the provisions of the GDPR (which in any case has direct applicability in Spain), and (ii) providing specific data protection regulation in different fields that are not expressly covered by the GDPR, or that are covered by the GDPR but in relation to which the Member States are given some competence to enact a more detailed regulation. This means that certain specific types of data processing not specifically regulated in the GDPR (e.g. creditworthiness of shared files) have been provided with more detailed regulation in the Spanish LOPD.

The LOPD also includes some new content, including in particular a new set of rights of citizens in relation to new technologies, known as “digital rights”. This set of new digital rights may impact the business of certain fintech companies since some rights regulate and grant additional privacy safeguards related to the use of technologies, such as digital rights granted to employees regarding the use by employers of IT tools for monitoring purposes in the workplace, use of geolocation systems or CCTV-related processing.

Cookies, ecommerce and direct marketing activities by electronic means. In addition to data protection rules, the processing of personal data for marketing purposes through electronic means and the use of cookies (and similar technologies) are governed at an EU level by a different set of rules, which include (i) Directive 2000/31/EC of the European Parliament and of the Council, of 8 June 2000, on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (“**Ecommerce Directive**”), and (ii) Directive 2002/58/EC of the European Parliament and of the Council, of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (“**E-privacy Directive**”). These EU Directives have been implemented in Spain through national rules. In particular, at a national level, the use of cookies and the processing of personal data for marketing purposes through electronic means are governed in Spain by Law 34/2002 of 11 July on information society services and e-commerce (*Ley 34/2002 de 11 de julio, de servicios de la sociedad de la información y comercio electrónico*). Thus, the use of cookies or the direct marketing activities carried out by fintech businesses established in Spain must meet the requirements of these national rules which, in the majority of cases, replicate without significant changes the rules set out in the relevant EU Directives.

In addition, guidelines and opinions issued by the Spanish Data Protection Authority (*Agencia Española de Protección de Datos*) as well as those issued by the European Data Protection Board, must be taken into account by fintech companies, since they interpret and clarify specific matters in the data protection regulations, whether European or national.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

Extraterritorial scope. The GDPR and LOPD apply to businesses located in Spain, regardless of the corporate form of such business (e.g. company, branch or establishment). Moreover, extraterritorial scope of EU data protection rules set out in article 3 of the GDPR applies in Spain. Thus, non-EU fintech businesses offering goods or services to data subjects in Spain and the monitoring of their behaviour as far as their behaviour takes place within Spain would be subject to GDPR rules. Also, and even though the LOPD does not provide for rules regarding territorial scope, it should be understood that such non-EU businesses would also fall within the scope of the LOPD. These non-EU companies should have to appoint a representative in the EU and this representative may be held liable under data protection rules for the processing carried out by non-EU businesses.

International transfers of personal data. The transfer of personal data from Spain to territories or organisations located outside the EU is subject to the rules regarding international transfers of data set out in the GDPR (articles 44 to 50). The LOPD does not provide additional relevant rules for Spain to those set out in the GDPR. In general terms, international transfers of personal data may be carried out to the extent that the recipient is subject to an adequacy decision by the EU Commission, if appropriate safeguards have been adopted (e.g. Binding Corporate Rules or Model Clauses) or if the transfer falls within one of the derogations listed in article 49 of the GDPR (e.g. explicit consent of data subjects).

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

The sanctioning regime for failing to comply with GDPR and LOPD is set out in the GDPR (i.e. fines up to EUR 20 million, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher). That said, the LOPD provides for more detail when it comes to the classification of severity of infringements. In particular, the LOPD sets out three categories of data protection infringements (minor, serious and very serious infringements). For each of these categories, the LOPD sets out the list of acts or omissions that could fall within such category. The list under each of these three categories is quite detailed.

The LOPD also provides for a statutory period for each category. According to it, administrative liability for minor infringements shall expire within one year, while the expiry for serious infringements is set at two years and at three years for very serious infringements.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

The applicable European regulation concerning this matter is Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common

level of security of network and information systems across the Union (“NIS Directive”), which requires local implementation in each Member State. The NIS Directive provides measures aimed at achieving a high common level of security of network and information systems in the EU so as to improve the functioning of the internal market. In Spain, the NIS Directive has been implemented in 2018 by Royal Decree-Law 12/2018 of 7 September on security of networks and information systems [*Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información* (“RDL 12/2018”)]. As it happens, in the NIS Directive, the RDL 12/2018 mainly (i) regulates and establishes requirements to ensure the security of networks and information systems used for the provision of the essential services and the digital services, and (ii) establishes a system to notify cybersecurity incidents. The RDL 12/2018 has a quite broad scope and it will be subject to a future development by means of ancillary regulations. Also, the RDL determines which are the competent bodies for cybersecurity matters in Spain (such as the Department of State for the Development of Digital Technology (*Secretaría de Estado para el Avance Digital*) of the Ministry of Economy and Business (*Ministerio de Economía y Empresa*) or the INCIBE-CERT). In Spain, the competent authority has, among other functions, powers to impose sanctions.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

In general, fintech businesses providing services that are catalogued as financial, investment or insurance-related services (including payment entities and electronic money institutions, currency exchange services and transfer of funds services) and the related intermediation services are subject to AML and prevention of terrorist financing requirements. The Spanish laws regulating both the prevention of money-laundering and terrorist financing were recently unified. Those regulations impose various obligations, although they primarily relate to the formal identification of the beneficial owner of any legal or natural persons intending to enter business transactions with them, the application of simplified or enhanced due-diligence measures with prospective clients and the potential reporting of various events to the corresponding authorities.

The 5th AML Directive was published in June 2018 and it has included under its scope the providers engaged in exchange services between virtual currencies and fiat currencies. Such Directive must be implemented in Spain by early 2020, so cryptocurrencies will not be subject to the Spanish AML regulations until then.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

Apart from the financial regulatory frameworks already addressed in question 2.1 above, along with data protection and AML regulations, other regulatory regimes may also apply to Spanish fintech businesses. One notable instance is Royal Legislative Decree 1/2007, of 16 November, approving the revised text of the general law on the protection of consumers and users. This regulation establishes guiding principles applicable to relationships with consumers and users (understood as legal or natural persons acting in a context that falls outside entrepreneurial or professional activities) and entrepreneurs. Also of note is Law 34/2002, of 11 July, on services of the information society and electronic commerce, which is of particular importance for online businesses,

as it establishes a regulatory regime for electronic agreements (e.g. the information to be provided to the contracting parties prior to and after the execution of the relevant agreements, the conditions applicable for the validity of electronic agreements, and other obligations applicable to electronic providers). For the financial sector in particular, another notable instance is Spanish Law 22/2007 on the commercialisation by distant means of financial services addressed to consumers, setting out the rules for electronic agreements and electronic marketing communications.

In view of the above and of the highly complex financial regulatory environment to which fintech companies may be subject (see section 3), the growing sector of regtech businesses in Spain should not be ignored (i.e. businesses that, based on big data or blockchain technologies, are creating solutions to facilitate other companies’ regulatory compliance). The regtech roadmap has particularly evolved in 2018, where regtech companies have diversified in different areas, such as risk management, clients’ identification, reporting, big data and cybersecurity.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

Although Spanish employment law is composed of numerous employment provisions, issued by different bodies and with different priorities, the basic legal framework around the hiring and dismissal of staff in Spain is constituted by the Statute of Workers (“SW”) and the Social Security Law.

The SW is the most important law in connection with employment law and contains the basic and general employment law framework for ordinary employees (e.g. employment rights and obligations, types of employment contracts, salary, worktime, dismissals, employee representatives). The SW was approved by a consolidated text passed by Royal Legislative Decree 2/2015 of 23 October. The Social Security Law was approved by a consolidated text passed by Royal Legislative Decree 8/2015 of 23 October and contains the basic regulations governing social security contributions and social security benefits (e.g. retirement, unemployment, disability benefits).

In general, it is necessary to comply with certain requirements from employment and Social Security perspectives before hiring employees in Spain (e.g. registering employees with Social Security, notifying Social Security of the employment, health and safety and work obligations, and registering employment contracts).

On the dismissal side, Spanish law recognises the “stability in employment” principle, implying that the duration of contracts is essentially indefinite (i.e. the SW specifies fixed causes for temporary contracts) and that dismissal can be complicated and expensive for employers. Pursuant to the SW, an employee can only be dismissed: (i) on a disciplinary basis as a result of serious, wilful non-compliance with his/her duties; or (ii) for objective reasons based on the need to eliminate specific positions for economic, technical, production, or organisational reasons. Under Spanish labour law, an employee can only be dismissed under those specified reasons. Therefore, if an employee files a judicial claim with a labour court alleging the dismissal to be unfair and the reasons set out above are not proven or not sufficiently serious, the court will declare the dismissal to be unfair and the employee will be

entitled to a severance payment equivalent to 33 days of salary per year of service, subject to a maximum limit of 24 months of salary. Moreover, it must be noted that some employees receive special protection from the law against dismissal. In this regard, employee representatives may not be dismissed based on the activities carried out in the exercise of their representation and have job retention rights in the event of suspension or termination of the employment relationship due to economic, technological, production, or economic causes. In addition, employees dismissed under certain maternity or paternity-related circumstances are also specially protected against dismissal due to objective grounds.

5.2 What, if any, mandatory employment benefits must be provided to staff?

As previously mentioned, the SW works as the basic legal regulation on all matters related to employment and sets out the minimum conditions that employment contract must respect. Moreover, Spanish law provides that agreements entered into between employers and employees may, when they meet certain requirements regarding content and the representative authority of the negotiating parties, bind all employers and employees – including those not directly represented by the negotiators – within certain economic areas, thus making such collective bargaining agreements (“CBAs”) mandatory. Among other matters, the CBAs regulate matters concerning employment relationships such as salary structure, working hours, overtime, allowances, job description, benefits, prevention of occupational hazards, remuneration, duties, holidays, productivity, or the disciplinary framework. Employment contracts can establish provisions on working conditions, but may only improve on the conditions established in the SW and in the applicable CBA. In sum, mandatory rights conferred on employees by the SW and the applicable CBA cannot be legally waived by the employee.

Since most of employment law, including law made through CBAs, is mandatory, contractual freedom in employment matters is rather narrow. Taking all this into account, the most relevant mandatory provisions on employment are the following ones:

- The SW sets forth an “interprofessional” minimum annual, monthly, or daily salary that is determined annually by the central government, taking into consideration the next year’s forecasts for several financial indexes. For 2019, the interprofessional minimum monthly salary has been set at EUR 900.
- The maximum statutory work schedule is 40 hours of effective work per week, calculated on an annual basis. Workdays of more than nine hours are not permitted, unless a different distribution of the workday is established by collective agreements or, in its absence, by agreements between the employer and the employee representatives. In all cases, a minimum 12-hour break must be provided between the end of one workday and the beginning of the next. Employees are also permitted to a weekly uninterrupted rest period of one-and-a-half days (generally, Saturday afternoons or Monday mornings and all of Sunday).
- Vacation time is regulated in the applicable collective bargaining agreement or individual labour contract. Nevertheless, employees are mandatorily entitled to enjoy at least 30 calendar days per year of vacation. In addition, employees in Spain enjoy 14 days each year as official paid bank holidays.
- Generally speaking, in the event of the birth, adoption, or fostering of a child, employees are entitled to 16 weeks of paid leave. Furthermore, employees who apply for legal

custody of a child under 12 years of age, or a physically or mentally handicapped relative not able to perform a remunerated activity, are entitled to a reduction of between one-eighth and one-half of their working time, in which case the remuneration will be reduced proportionally.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

There is no special route for obtaining permission for individuals who wish to work in fintech businesses. On the one hand, according to EU and domestic regulations, citizens of EU/EEA Member States can exercise the rights of entry and exit, free movement, residence, and work in Spain. Ordinary registration certificates and residency cards may be required. On the other hand, foreign non-EU/EEA citizens must obtain a residence and work authorisation by filing the required documentation with the labour authorities.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

We refer separately to inventions (which generally include innovations) and works.

Inventions are typically the result of research. That result may essentially be protected by patents, utility models or, if such protection is not available or the parties do not wish to request it, inventions can also enjoy a certain degree of protection as “know-how” or a “trade secret”:

- Spanish patents provide protection for the relevant invention for 20 years as of the filing date.
- Utility models protect inventions of lower inventive rank than patents, and are granted for a period of 10 years.
- Once the referred protection periods have expired, the invention will enter the public domain and any person can use it freely.
- Know-how and trade secrets have a value as long as they are kept confidential, as opposed to patents, and therefore it is a matter of contract (confidentiality agreements) and of fact (other protective measures adopted) that the invention remains valuable.

On a separate note, software would not be deemed an invention but would be protected by copyright (*derecho de autor*) from the very moment of its creation. Registration is not necessary for protection of software. The exploitation rights in the work will run for the life of the author and survive 70 years after the author’s actual or declared death.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Again, the rules applicable to the ownership of inventions and of works should be analysed separately. These are the default rules under Spanish law to attribute ownership of inventions:

- (a) Absent other applicable rules, the natural person who creates the invention (i.e. the inventor) is the owner.
- (b) If the inventor is an employee (private or public):
 - (1) in case the invention is a result of his/her work for a company, pursuant to the terms of his/her employment

agreement or to the instructions received from the company, then the owner of the rights to the invention is the company; or

- (2) in case the invention is a result of his/her independent work but used relevant knowledge obtained from a company or the company's facilities, then the company can claim ownership rights to the invention or a right to use the invention, subject to payment of fair compensation.

The rule in connection with works is that the original owner of the rights to the work is the author or co-authors (or, in very specific and limited cases, an individual or a legal private or public entity who leads and coordinates personal contributions and publishes the result under its own name – usually in the case of software). The general rule is that the author is the owner of all moral and exploitation rights to the work. However, there exist specific legal presumptions as well as some important exceptions:

- (a) Regarding copyrightable work created by an employee under his/her employment agreement, Spanish law presumes that, unless otherwise agreed, all exploitation rights in the work have been assigned, on an exclusive basis, to the company for the purposes of its ordinary course of business. This assumption applies in particular, but is not limited to, the creation of software.
- (b) In the event of joint co-authors, either:
- (1) all co-authors have equal exploitation rights, unless otherwise agreed; or
 - (2) the exploitation rights to the work correspond to the (legal or natural) person that assumes responsibility for the creation of the work and publishes it under the person's own name.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

When referring to IP rights (“IPRs”), we refer to trademarks, patents, utility models, designs, know-how and business information (trade secrets).

Under Spanish law, enforceable IPRs are those having effect in Spain. This is the case, for instance, of: (a) domestic rights resulting from domestic applications with the SPTO; (b) community rights (e.g. European Union trademarks and designs); and (c) domestic rights resulting from an international application with regional/international IP offices (e.g. international trademark applications under the scope of the Madrid Agreement).

Apart from registered rights, protection is also granted to specific, unregistered rights, including:

- (a) Well-known and reputed trademarks and tradenames, which are protected from unauthorised use by third parties that might take unfair advantage of their reputation or affect their distinctive character (in accordance with article 6 “bis” of the Paris Convention for the Protection of Industrial Property).
- (b) Non-registered European Union designs (if they have already been marketed in the European Union), which are protected for a period of three years following the date on which the design was first made available to the public (and only from uses resulting from its copy).
- (c) Know-how and business information (trade secrets) may be protected if the requirements set forth in Spanish law on unfair competition and Spanish case law are satisfied.

As regards copyright and related rights, since there is no registry and no formal requirements, the owner is entitled to enforce the right irrespective of any “local” or “national” character. Given the territoriality of this category of rights, the *lex loci protectionis* principle applies. The Spanish Copyright Act is directly applicable not only to Spanish and EU citizens but also to nationals of third countries who are ordinarily residents of Spain, and even from nationals of third countries not ordinarily residents of Spain if their works have been published for the first time in Spain. Nationals of third countries must, in all cases, enjoy the protection available under the international conventions and treaties to which Spain is a party and, should there be none, must be treated in the same way as Spanish authors when Spanish authors are themselves treated in the same way as nationals in the country concerned. In the field of copyright, the main multi-jurisdictional treaty is the Berne Convention for the Protection of Literary and Artistic Works, which has been ratified by Spain and more than 170 countries.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

In general, the holder of an IP right may exploit the right: (i) directly; or (ii) through third parties through a licence. Note that, unless otherwise indicated, licences are understood to be non-exclusive, national, for the whole life of the IPR and must be registered with the appropriate office in order to be enforceable against third parties. In addition, licences for patents must be granted in writing.

Under Spanish law, the exploitation of all IPRs is subject to various limitations (most of which result from Spain being party to specific international treaties on industrial property). Those limitations include, but are not restricted to: (i) the exhaustion of IPRs; and (ii) the permitted uses for patents (e.g. private acts with no commercial purposes and acts carried out for experimental purposes).

With respect to copyright and related rights, the author is granted the power to exploit the work in any form (and especially through reproduction, distribution, public communication and transformation). For some activities, the author only has a right to remuneration (e.g. private copying). Usually, the author is not the one who directly exploits the work, but transfers the right through an assignment to specialised entrepreneurs. Although Spanish law does not create a specific presumption, the transfer of copyright usually involves remuneration in the form of a percentage or royalty in connection with the assignee's income generated from the exploitation of the right. As in other jurisdictions, exploitation rights are limited by a number of exceptions that allow the general public, or certain beneficiaries, to make specific, free use of the work without requiring permission from the author. In such cases, the author will not receive any remuneration, unless equitable compensation of some kind is appropriate.

Acknowledgment

The authors would like to acknowledge the assistance of their colleague Livia Solans Chamorro in the preparation of this chapter. Livia Solans Chamorro is a senior associate in Uría Menéndez's Madrid office. She joined the firm in 2009 as an associate in the Corporate and Commercial area. From 2013 to 2014 she was seconded to the Peruvian law firm Payet, Rey, Cauvi.



Leticia López-Lapuente

Uría Menéndez
Príncipe de Vergara 187
28002, Madrid
Spain

Tel: +34 91 586 0727
Email: leticia.lopez-lapuente@uria.com
URL: www.uria.com

Leticia López-Lapuente is a partner of Uría Menéndez and is based in the Madrid office. She heads the data protection and Internet practice of Spanish law firm Uría Menéndez and leads the LATAM data protection group.

Leticia focuses her practice on data protection, IT and commercial law, especially in the Internet, software, e-commerce and technology sectors. She also advises on privacy law issues. Leticia provides clients operating in these sectors with day-to-day advice on regulatory, corporate and commercial matters, including the drafting and negotiation of contracts, privacy advice (including advice in investigations and sanctioning proceedings), big data and AI, cybersecurity, outsourcing, consumer protection and e-commerce issues, M&A, RFP procedures, dealings with public authorities, etc. She has been involved in major transactions and assisted businesses and investors in these sectors.

She regularly speaks in national and international fora regarding personal data protection and technology, in addition to having written numerous articles on data protection-related matters.



Isabel Aguilar Alonso

Uría Menéndez
Príncipe de Vergara 187
28002, Madrid
Spain

Tel: +34 91 586 0120
Email: isabel.aguilar@uria.com
URL: www.uria.com

Isabel Aguilar Alonso joined the firm in 2008 and is a counsel.

She has more than 10 years of experience advising a wide range of financial entities, including collective investment schemes, payment services firms, investment firms and credit entities, in regulatory and financial matters.

In particular, within the regulatory field, she advises on matters such as authorisations, cross-border provision of services, marketing of products, rules of conduct and transparency, consumers and users, disciplinary proceedings, payment services, e-money and SEPA regulations. Within the financial field, her practice includes fintech projects, financing, securitisations, assignments of receivables and security packages.

URÍA MENÉNDEZ

Uría Menéndez is the leading law firm in the Ibero-American market. We have almost 600 lawyers working in 14 different offices located in the most important financial centres in Europe, the Americas and Asia.

Uría Menéndez lawyers' extensive experience and comprehensive knowledge of their clients' industries allow the firm to offer value-added advice in all areas of business and find innovative technical solutions to the most complex legal issues. In addition, through its network of best friends in Europe, Uría Menéndez is able to create cross-firm teams with the leading firms from France (Bredin Prat), Germany (Hengeler Mueller), Italy (BonelliErede), the Netherlands (De Brauw Blackstone Westbroek) and the United Kingdom (Slaughter and May). Uría Menéndez is also a member of renowned international associations such as Lex Mundi.

Furthermore, in January 2015, after more than 20 years working in the region, the firm took a ground-breaking step creating the first Latin-American integration between leading local firms (Philippi in Chile, and Prietocarrizosa in Colombia): Philippi, Prietocarrizosa & Uría (PPU), the first major Ibero-American firm. After an excellent first year, in January 2016 the firm integrated two Peruvian firms, Estudio Ferrero Abogados and Delmar Ugarte, becoming Philippi Prietocarrizosa Ferrero DU & Uría. The opening of a Peru office consolidates PPU's position and confirms its status as a leading firm in the Pacific Alliance (Chile, Colombia, Mexico and Peru) as it is fast becoming a preeminent firm in Latin America.

Sweden

Anders Bergsten



Martin Pekkari



Mannheimer Swartling

1 The Fintech Landscape

- 1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).**

Stockholm, the capital of Sweden, is ranked as the leading Nordic financial centre, with strengths in such areas as innovation and technology, and with the headquarters of three major Nordic banks and the largest stock exchange. The 2018 Bloomberg Innovation Index underlines Sweden's dominance in innovation, ranking the country second globally. In terms of investment volume, Stockholm is often regarded as being one of Europe's main centres for fintech investments, with the past year's major deal being PayPal's acquisition of Stockholm-based iZettle for USD 2.2 billion. The payments segment is currently the largest of the Swedish fintech industry segments, whereas asset management has (thus far) not been as large, but is growing. Cryptocurrency business initiatives are also on the rise. Peer-to-peer lending and insurance have yet to make a real breakthrough on the Swedish fintech market.

Examples of notable fintech innovations by Swedish companies are, *inter alia*: payment solutions for consumer online purchases; simplified payment procedures for small businesses; digitalised administration of receipts; solutions for more secure payments for online purchases; peer-to-peer lending platforms; solutions for fund investments without intermediaries; automated advice on investments (robo-advisors); and automated processing of insurance claims. In general, a continued notable fintech innovation trend on the Swedish market is thus the creation of different solutions, aimed at making it easier for consumers to manage their private finances, mostly through payment solutions and automated advice. Cryptocurrency, mining and related businesses are also trending.

- 1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?**

In general, there are no types of fintech business that are prohibited *per se* in Sweden. However, several restrictions apply to fintech companies depending on the business and services provided and, as such, the business and services must always be reviewed in light of, primarily, the general regulatory framework on financial services and consumer protection. Authorisation may be required from the

Swedish Financial Supervisory Authority ("SFSA") prior to conducting certain activities in Sweden (see below).

2 Funding For Fintech

- 2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?**

Primarily, local and international venture equity and growth equity, as well as venture debt (e.g., from hedge funds).

- 2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?**

There are no special incentive schemes for investments in fintech businesses in particular.

However, a special tax incentive may, under certain circumstances, apply to individuals who invest in small companies. The incentive is granted in the form of a deduction from capital income equal to 50% of the acquisition cost of the investment, with a maximum of SEK 650,000 per individual in any year. The company may only receive investments qualifying for the tax incentive up to a maximum of SEK 20 million per year.

On 1 January, 2018, new tax rules entered into force for employee stock options granted by start-ups. The purpose is to encourage start-up businesses. A range of requirements are set out in order for the rules to apply, but employees holding stock options that qualify under the rules are subject to capital income tax when the underlying shares are sold, rather than employment income tax when the stock options are exercised. For the employing entity, no social security charges are payable.

Lastly, a special tax relief may, under certain circumstances, be granted to foreign key personnel for a limited time period whereby 25% of income is exempt from income tax for personnel qualifying under these specific rules (Sw. *expertskatte regler*).

- 2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?**

Each exchange has its own listing requirements which must be fulfilled, but there are no specific fintech-related listing

requirements which would apply in connection with an IPO in Sweden. However, if the entity to be listed is a regulated entity licensed with the SFSA, certain restrictions on major shareholders and members of the board and management need to be observed.

In Sweden, there are currently two regulated markets, Nasdaq Stockholm and Nordic Growth Market (“NGM”), where Nasdaq Stockholm clearly is the dominant market. There are currently three Swedish multilateral trading platforms (“MTFs”) that have lighter listing requirements: Nasdaq First North; Nordic MTF; and Spotlight.

The listing requirements vary between the markets, but the dominant market (Nasdaq Stockholm) has principal listing requirements regarding, e.g., the below:

- a prospectus drawn up in Swedish pursuant to the European prospectus regime and approved by the SFSA;
- complete annual accounts and operating history for three years (as a general rule);
- capacity to fulfil the disclosure requirements for a listed entity;
- sufficient profitability or working capital;
- sufficient competence and expertise among the Board and Management;
- shares must be freely negotiable and kept in book-entry form (Euroclear Sweden);
- the entire class of the shares must be listed;
- conditions for sufficient liquidity in the shares must be at hand; and
- legal due diligence by a law firm and vetting process by an Exchange Auditor (if not already listed on another market approved by Nasdaq Stockholm).

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

There have been a number of notable exits in the broader fintech area (including iZettle, Trustly, Cinnober and Klarna), and there are a number of smaller and medium-sized exits under way in the next few years.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

The regulatory landscape varies depending on the type of fintech business in question. However, in general terms the following can be said. Businesses that intend to provide financial services generally have to obtain a licence from, and operate under the supervision of, the SFSA. This applies to, *inter alia*: banks; credit market companies; payment companies; fund management companies; investment funds; consumer credit businesses; issuers of electronic money; and securities companies. Key regulatory frameworks for payments and lending relating to fintech include:

- The Banking and Financing Business Act (2004:297). This Act is the key piece of Swedish legislation governing banking and financing business carried out by banks and credit market companies.
- The Consumer Credit Activities Act (2014:275). This Act applies to companies conducting certain consumer lending businesses but is a significantly less burdensome regime than the Banking and Financing Business Act.

- The Consumer Credit Act (2010:1846). This Act contains far-reaching and mandatory consumer protection rules that all types of companies providing consumer credits must adhere to.
- The Payment Services Act (2010:751), being the Swedish implementation of the EU Directive on Payment Services in the Internal Market (“PSD2”).
- The Electronic Money Act (2011:755), implementing the EU Electronic Money Directive.
- The Certain Financial Operations Act (1996:1006). Certain financial activities that do not require authorisation from the SFSA still require notification to the SFSA under this Act.

The key pieces of legislation for asset management businesses are the following:

- The Securities Business Act (2007:528), implementing the EU Markets in Financial Instruments Directive (“MiFID 2”).
- The Alternative Investment Fund Managers Act (2013:561), implementing the EU Alternative Investment Fund Managers Directive.
- The Securities Funds Act (2004:46), implementing the EU Undertakings for Collective Investment in Transferable Securities Directive (“UCITS”).

In addition, it may be noted that many fintech businesses are subject to the following regulations:

- The Anti-Money Laundering and Terrorism Financing Act (2017:630), implementing Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (“AMLD IV”).
- The Identification of Reportable Financial Accounts due to the FATCA Agreement Act (2015:62) and the Identification of Reportable Financial Accounts in connection with Automatic Information Exchange Act (2015:911), being the Swedish implementations of the US-Swedish FATCA intergovernmental agreement and the OECD’s CRS/EU’s DAC2 legislation, respectively.
- The Supervision of Credit Institutions and Investment Firms Act (2014:968), implementing the EU Directive on Access to the Activity of Credit Institutions and the Prudential Supervision of Credit Institutions and Investment Firms (“CRD IV”) and the EU Regulation on Prudential Requirements for Credit Institutions and Investment Firms (“CRR”).

In addition to the above, the SFSA issues detailed regulations and guidelines that supplement the legislative acts set out above.

In July 2016, the Swedish Government appointed an inquiry to conduct a survey on the market for crowdfunding platforms and, if necessary, to propose new provisions (the “Inquiry”). In March 2018, shortly after the European Commission’s proposal for a regulation on crowdfunding was presented, the Inquiry proposed to introduce regulation on crowdfunding in a new commercial law called the Certain Financial Mediation Activities Act. The Act is to contain provisions on a) authorisation or registration requirements to conduct activities governed by the Act, b) how these activities are to be conducted, and c) supervision and sanctions. It is proposed that the new Act shall apply to any business activity that, in return for compensation, seeks to bring together natural persons or legal entities intending to procure financing from natural persons or legal entities intending to provide financing, if the financing is (i) lending-based crowdfunding, (ii) equity-based crowdfunding, (iii) reward-based crowdfunding, or (iv) donation-based crowdfunding. The proposal was well received by Swedish crowdfunding market actors that have long sought clarification on how existing regulation applies to their business. At the same time, however, some market actors were of the opinion that the implementation of new

regulations had taken too long and advocated for a more agile approach by way of self-regulation measures. The Inquiry proposed that the new Act shall come into force on 1 May 2019 (with certain transitional provisions). However, given the Swedish legislative process and the fact that the European Commission's proposal will probably overlap with the new Swedish Act, implementation is most likely to be postponed. At the moment it is unclear when regulation can be expected and whether it will come from the Swedish legislator, the EU or the market actors themselves.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

There is no regulation specifically directed at cryptocurrencies or cryptoassets.

The SFSA has stated that a company that offers to purchase cryptocurrencies, such as Bitcoin, to its clients from its own holdings, must be registered in accordance with the Certain Financial Operations Act (1996:1006) since the company is providing a means of payment.

The SFSA has not provided any guidance on the treatment of cryptoassets. It is envisaged that a determination of whether the cryptoasset at hand meets the definition of a financial instrument and whether the services or activities provided therewith should be treated as a regulated investment service or activity must be made on a case-by-case basis.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

The Swedish Government has generally been receptive to fintech innovation, but due to the fast-paced development in fintech, it has been difficult for the Swedish legislator to keep up. Upon instruction by the Swedish Government, the SFSA has established a fintech-specific innovation centre with the purpose of creating a designated space where fintech companies can engage in dialogue with the SFSA and receive information on the regulations applicable to their business, thus facilitating fintech companies' regulatory compliance. The innovation centre is not a regulatory sandbox allowing companies to test their innovations in the market under the SFSA's supervision. The SFSA believes that the innovation centre has greater potential to succeed than the establishment of a regulatory sandbox.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

It is generally easier for fintech businesses established within the EEA to conduct cross-border activities into Sweden due to the EU rules on passporting (under which EEA-based businesses may generally conduct operations in Sweden following a simple notification to the SFSA). Non-EEA businesses are generally required to obtain separate authorisations from the SFSA and are, in some cases, even forbidden to conduct cross-border activities into Sweden. In addition, the Swedish consumer protection legislation is extensive and may impose stricter requirements than foreign fintech

businesses are used to. To some extent, this consumer protection legislation also applies to companies conducting business outside Sweden if they are approaching Swedish consumers.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

Yes, through the new Swedish Supplementary Provisions concerning the EU General Data Protection Regulation Act (2018:218) ("DPA") and the Supplementary Provisions concerning the EU General Data Protection Regulation Ordinance (2018:219), both entered into force on May 25, 2018. The DPA supplements the EU's General Data Protection Regulation ("GDPR") (applicable to all EU Member States) and applies to data processing not covered by the GDPR with some exceptions. It should also be noted that the DPA is subsidiary to all other legislation, meaning that if another act contains a specific provision which differs from the DPA, then the other act will prevail.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

Yes, on both accounts. The territorial scope of the GDPR extends to organisations with an establishment in the EU/EEA and organisations established outside the EU/EEA that offer goods or services to data subjects in the EU/EEA, or which monitors data subjects within the EU/EEA. Further, it restricts transfers of data to locations outside the EEA.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

The sanctions and penalties under the GDPR include administrative fines (for undertakings), and damages. The maximum administrative fine that can be imposed for infringements of the GDPR is the greater of €20 million or 4% of an undertaking's worldwide turnover for the preceding fiscal year.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

Yes, the GDPR includes cyber security requirements, and there are regulations imposed by the SFSA which may have cyber security implications. Additionally, fintech businesses may be further affected by the recent implementation of national Swedish legislation based on the NIS Directive (Directive (EU) 2016/1148), as well as by the new Swedish Security Protection Act entering into force in April 2019.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

There are primarily three statutes in Sweden that are relevant: the Anti-Money Laundering and Terrorism Financing Act (2017:630)

(“**AMLA**”); the Penalties for Money Laundering Offences Act (2014:307) (“**PMLA**”); and the Penalties for Financing of Particularly Serious Crimes Act (2002:444) (“**PSCA**”).

The AMLA contains provisions on measures that any party providing certain financial or other services is obliged to take to prevent their operations from being exploited for money laundering or financing of terrorism.

Parties that are subject to the AMLA are obliged to monitor and report matters involving suspicious transactions of money laundering or terrorist financing. The requirements of the examination include customer due diligence and a review of transactions.

The PMLA contains criminal law provisions on money laundering. Provided that the measure is intended to conceal the fact that the money or other property derives from an offence or criminal activity, a person is guilty of a money-laundering offence if he or she transfers, acquires, supplies, converts, stores or takes similar actions with the property. The same applies where a person improperly promotes opportunities for someone to transfer money or other property derived from criminal activity. Moreover, this applies where the person did not realise but had reasonable grounds to believe that the property was derived from criminal activity. Abetment of money laundering offences is also criminalised.

The PSCA contains criminal law provisions on the financing of particularly serious crimes and primarily terrorist crimes. Accordingly, it is a crime to collect, provide or receive money or other property with the intent that the assets shall be used, or in the knowledge that they are intended to be used, to commit particularly serious crimes enumerated in the PSCA. Abetment of such acts is also criminalised.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

There are no general regimes that need mentioning, but, as noted above, additional regulatory requirements may apply depending on the type of fintech business in question.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

Hiring

Under the Swedish Employment Protection Act (1982:80) (“**EPA**”), an employment relationship should generally be permanent. However, it is possible to agree on fixed-term employment for up to two years during a five-year period. The employer must give the employee written information on all significant employment terms and conditions no later than one month after the employment relationship begins. The employment may be probationary for up to six months. If applicable, there can be deviations from the aforesaid in collective bargaining agreements.

The hiring process may not be discriminatory on the basis of gender, transgender identity or expression, ethnicity, religion or other religious belief, disability, sexual orientation, or age.

Dismissals

Except for employees in managerial positions – usually only the managing director and, in larger companies, members of the

executive management team – all employees in Sweden are covered by the EPA. To dismiss a permanently employed employee, the employer needs just cause.

Under the EPA, there are two categories of just cause: (i) personal reasons; and (ii) redundancy. The threshold for dismissing someone due to personal reasons is very high, and is only applicable in exceptional and severe cases of, e.g., negligence, disloyalty, difficulties in working with other employees, or incapability to carry out any relevant work.

In contrast, an employer’s decision to lay off employees due to redundancy cannot, as such, be legally challenged under Swedish law (unless redundancy is just a pretext to dismiss someone based on personal grounds). However, Swedish law limits the employer’s freedom to choose which employees to retain and which employees to let go in a redundancy situation, under the so called last-in-first-out principle.

Union consultations are often required prior to dismissals.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Below is a summary of the most important mandatory employment benefits.

Wages and overtime payment

There is no statutory minimum wage. If the employer is bound by a collective bargaining agreement, it normally provides for minimum wage. The same applies for overtime payment. A collective bargaining agreement may also set forth other employment benefits.

Vacation

Generally, all employees are entitled to a minimum of 25 days’ vacation leave per vacation year (with certain exceptions which may apply during the first year of employment). In order for the leave to be paid, the employee must have earned this during the 12-month period preceding the vacation year unless the employer grants vacation pay in advance.

Parental leave

An employee who becomes a parent is entitled to full or part-time leave until the child is 18 months old (regardless of he/she receiving parental leave benefits from the Social Insurance Agency) and thereafter, and until the child is eight years old (or 12 years old if the child was born in 2014 or later), to the extent the parent has saved parental leave benefits from the Swedish Social Insurance Agency. The parental leave benefits from the Social Insurance Agency amount to 480 full days to be divided by the two parents (90 days are, however, earmarked for each parent). The parent is further entitled to part-time reduction (by up to 25%) of normal working hours until the child is eight years old. No compensation must be paid by the employer during the leave, unless otherwise agreed in the individual employment contract or any applicable collective bargaining agreement.

Sick leave

An employer is obliged to pay sick-pay allowance to an employee who is absent from work due to illness. The employer is required to pay sick pay during the first 14 calendar days of the sickness period (although not for the first day, which is a qualifying day). The sick pay must, as a minimum, be equivalent to 80% of the employee’s salary. After the first 14 calendar days of the sickness period, the employee is entitled to sickness benefits from the social security system and, under many collective agreements (if applicable), a top-up from the employer.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

EU citizens

EU citizens do not need any permit to work in Sweden. Provided that the EU citizens work, there is no time limit for staying in Sweden and they do not need to register with the Swedish Migration Agency. If the employment will last for more than a year, the EU citizen shall register with the Swedish Tax Agency.

Non-EU citizens

Non-EU citizens need a work permit, an EU Blue Card, or, if the non-EU citizen has status as a “long term resident” in another EU Member State, he/she enjoys privileges similar to EU citizens and may work under a temporary residence permit.

For non-EU citizens, importantly the salary and the mandatory insurances must be at least on par with those set by Swedish collective agreements. In addition, the employer must comply with certain requirements with regard to advertising the vacant employment, the offering of employment and trade union involvement.

There are no special routes for obtaining permission for individuals who wish to work for the fintech business.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Innovations and inventions may be protected under Swedish IP legislation, which includes protection for patents, copyrights (including software and neighbouring rights), designs and trademarks, although mainly patents and copyright are used to protect innovations and inventions. Applications for registration of national patents, designs and trademarks are administered by the Swedish Patent and Registration Office (“PRV”), also maintaining the official registers. Copyright works are protected upon their creation and may not be registered in Sweden. Trademarks and designs may also be protected without registration under certain circumstances.

In addition, innovations and inventions, whether patentable or not, may be protected as trade secrets under the Trade Secrets Act (2018:558), which entered into force on July 1, 2018. The Act implements an EU directive on the protection of trade secrets and imposes civil and criminal liability for unauthorised use, disclosure, etc.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Once an IP right is obtained, the owner is entitled to exploit the innovation or invention without infringements from competitors for

as long as the exclusive right is valid. If an infringement occurs, the owner can initiate court proceedings in order for the infringement to cease. The different types of IP rights are valid for different time periods. Patents are normally valid for 20 years. Copyrights, which can include computer software, are valid for 70 years after the death of the creator/author. Design protection is valid for five-year periods and can be renewed for a maximum of 25 consecutive years. Registered trademarks are valid for 10-year periods and can, in principle, be renewed an infinite number of times.

Registering patents, trademarks, and protection for designs requires paying a filing fee to the PRV. In addition, patents are subject to annual fees.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

Sweden has ratified a number of multi-jurisdictional treaties and protocols, which recognise other national rights, or enable the application for national rights in several jurisdictions in one single application. With regards to trademarks, European Union Trade Marks are enforceable in Sweden, as well as international trademark registrations, administered by the World Intellectual Property Organization (“WIPO”) if Sweden is designated. Also, patents registered under the European Patent Convention are enforceable if validated in Sweden, as well as designs registered at the EU Intellectual Property Office (“EUIPO”). Further, Sweden is a party to the Berne Convention for the Protection of Literary and Artistic Works, the Universal Copyright Convention, and the agreement on Trade-Related Aspects of Intellectual Property Rights.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

IP rights can be sold or licensed. A licence agreement gives someone else the right to commercially use the exclusive right, and can contain regulations such as limitations to a geographical area, a time limit or refunding. Further, patents and registered trademarks can be pledged, upon registration.

With regards to copyright, the owner may assign/license its rights in whole, or in part. However, there is a distinction between economic rights and moral rights. As a main rule, the moral right cannot be transferred or licensed, but only waived in relation to specific purposes. Furthermore, a new holder, to which the ownership of the copyright passes, is not allowed to, e.g., alter, assign and license the copyright to any third party unless otherwise agreed. If the intention is that the new holder/licensee of the copyright is to be able to dispose of the copyright in such way, it needs to be stipulated explicitly in the agreement.

It is unclear under Swedish law if trade secrets/know-how can be subject to transfer of ownership, or if it is a mere question of access to and right to use such trade secrets/know-how.

**Anders Bergsten**

Mannheimer Swartling
Norrandsgatan 21
Box 1711
SE-111 87 Stockholm
Sweden

Tel: +46 8 595 061 94
Email: anders.bergsten@msa.se
URL: www.mannheimerswartling.se

Anders Bergsten spends a significant part of his practice on drafting, negotiating and managing commercial agreements, particularly IT, technology and outsourcing contracts, support contracts, cloud service contracts, software development contracts, as well as information sharing and cooperation contracts.

Anders also regularly advises clients in relation to data protection law matters. He is well-versed in EU data protection and cyber security law, e.g. the GDPR and the NIS Directive.

Recent examples of the projects in which Anders has been involved include IT and information sharing projects within the banking and finance industry, promissory note digitalisation projects, as well as several group-wide IT outsourcings and global industrial IoT projects. Anders has also carried out several comprehensive GDPR compliance projects, assessing the use of personal data across entire company groups.

The projects in Anders's practice regularly concern multi-jurisdictional matters with a number of complex technical and legal interfaces in relation to several stakeholders.

**Martin Pekkari**

Mannheimer Swartling
Norrandsgatan 21
Box 1711
SE-111 87 Stockholm
Sweden

Tel: +46 8 595 061 91
Email: martin.pekkari@msa.se
URL: www.mannheimerswartling.se

Martin Pekkari has extensive experience from drafting and negotiating commercial contracts in both a domestic and international environment. Many of the projects for which Martin has been responsible are of a cross-border nature and comprise a number of legal areas. Consequently, he has extensive experience managing and coordinating projects, including projects of a cross-border nature and where lawyers in multiple jurisdictions are involved.

Martin has experience from a number of industry sectors, such as IT and technology, manufacturing industry and infrastructure.

Martin's experience covers a wide range of projects and contract types, such as purchase and sale agreements for goods and services, outsourcing (e.g. IS/IT, BPO, manufacturing and R&D), licensing, technology contracts, development agreements/R&D contracts, support, maintenance and operation agreements, distribution and agency agreements, cooperation agreements/joint ventures, infrastructure agreements and PPP agreements (public private partnership).



**MANNHEIMER
SWARTLING**

Mannheimer Swartling is the leading business law firm in the Nordic region. The firm is a full-service firm with three offices in Sweden and five offices in other countries around the world. Mannheimer Swartling works with many of Sweden's, and the world's, leading major and mid-sized companies and organisations.

Mannheimer Swartling's Corporate Commercial practice, which includes the firm's Technology practice group, has expertise in all major areas related to IT and technology. Members of the group regularly draft, review, negotiate and assist clients in managing IT and technology-related contracts, often with an international scope. Projects handled by the group concern e.g. outsourcings, app development agreements, system procurements, cloud services, operating and hosting agreements, IoT projects, sharing economy questions, personal data issues (including group-wide GDPR compliance projects), telecom regulatory issues, internet and e-commerce, etc.

Mannheimer Swartling also has extensive expertise in all major areas concerning the regulatory framework for the financial services sector. The firm regularly provides strategic regulatory advice on business models and arrangements involving financial services, including the outsourcing of financial services and cloud outsourcing in the financial sector. The firm also regularly advises on other regulatory matters such as licence applications, supervision and sanction-related issues involving the Swedish regulator, management assessments, capital adequacy and distribution issues, etc.

Switzerland

Dr. Daniel Flühmann



Dr. Peter Ch. Hsu



Bär & Karrer

1 The Fintech Landscape

- 1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).**

The Swiss fintech landscape has evolved significantly over the past years and Switzerland continues to be an attractive base for innovators in the financial sector. More than 300 active companies in various sectors form the core of the ecosystem of start-ups and aspiring young fintech businesses that have been founded in the recent past. New start-up projects continue to emerge on a regular basis. However, the scope of fintech in the Swiss market is much broader, with many established financial institutions entering the space in the recent past. As a result, the distinction between fintech and traditional financial services has become increasingly blurred. Furthermore, technology-oriented businesses from outside of the financial sector, including large multinational players, are entering the fintech market in Switzerland as well.

Swiss-based fintech businesses include payment systems, investment and asset management services, crowdfunding and crowdlending platforms, insurance-related businesses (*insurtech*) as well as distribution and information platforms in the area of collective investment schemes. Furthermore, blockchain-based businesses continue to be another key focus area, including but not limited to the areas of cryptocurrencies and decentralised ecosystems. Many blockchain start-ups are based in the so-called “cryptovalley” in the Canton of Zug, which also became known in the recent past as a hub for initial coin offerings (“ICOs”). Six out of the 15 biggest ICOs since 2016 took place in Switzerland. More recently, the focus of attention has shifted towards the nascent market of so-called security token offerings (“STOs”) and, by extension, the legal framework and market infrastructure to support them.

The Swiss fintech industry has formed a number of associations and shared interest groups (e.g. the Swiss Finance + Technology Association, Swiss Fintech Innovations, Swiss Finance Startups, the Crypto Valley Association and the Swiss Blockchain Federation) to promote, together with investors, experts, political representatives and the media, the further development of a strong Swiss fintech sector.

- 1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?**

Switzerland has no specific prohibitions or restrictions in place with respect to fintech. Generally speaking, Swiss financial regulation is technology-neutral and principle-based, which has so far allowed it to cope with technological innovation. That said, fintech operators may be subject to regulation and supervision by the Swiss Financial Market Supervisory Authority FINMA (“FINMA”) or by self-regulatory organisations, depending on the nature and specifics of their business. The relevance and application of Swiss laws on, e.g., anti-money laundering, collective investment schemes, financial market infrastructures, banks, insurance companies, securities dealers and/or data protection has to be assessed in the individual case (see question 3.1). With regard to ICOs in particular, FINMA published a guidance letter in which it emphasised the concept of an individual review of each business case regarding the regulatory impact. It is therefore prudent for fintech start-ups to seek clearance from the regulator before launching their project on the market.

2 Funding For Fintech

- 2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?**

Switzerland has an active start-up scene and various funding opportunities are available for companies at every stage of development. There are seed and venture capital firms for early funding as well as mature debt and equity capital markets for successful companies at a later stage. In addition, there are many financial institutions that have a potential interest in buying an equity stake in fintech companies or in a full integration.

Crowdfunding and crowdlending as alternative sources of funding have shown rapid growth rates in Switzerland, both in terms of the number of platforms and the funds raised. The first crowdfunding platform was founded in 2008 and currently there are over 40 active platforms (compared to only four in 2014). In 2017, apparently CHF 374.5 million was raised via these platforms, which is 192% more than in the previous year (Crowdfunding Monitoring Switzerland 2018).

The legislator has facilitated crowdfunding and crowdlending platforms by way of the introduction of the fintech regulation in Switzerland as follows: a) as of 1 August 2017, the maximum

holding period during which the acceptance of funds for the purpose of settlement of customer transactions does not yet qualify as taking deposits from the public (and therefore do not count towards a potential banking licence requirement) was extended from seven to 60 days; and b) a so-called regulatory sandbox was introduced in the BankO, according to which more than 20 deposits from the public can be accepted on a permanent basis without triggering a banking licence requirement as long as i) the deposits accepted do not exceed CHF 1 million, ii) no interest margin business is conducted, and iii) depositors are informed, before making the deposit, that the person accepting the deposits is not supervised by FINMA and that the deposits are not covered by the Swiss depositor protection scheme (*see* question 3.3 for further details).

Furthermore, a growing number of incubators and accelerators, either exclusively fintech-related (such as the association F10 or Thomson Reuters Labs – The Incubator) or focused on digital innovation in general including fintech (such as Kickstart Accelerator), support and guide fintech start-ups in transforming their ideas into successful ventures.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

There are no specific tax or other incentives for the benefit of the fintech industry in Switzerland. However, depending on the tax domicile of the company and the residence of the shareholders, there are certain tax benefits for start-up companies and tax schemes granting some relief to investors. In addition, again depending on the tax domicile of the company (as tax rates vary between the cantons/municipalities), the ordinary profit tax rate in Switzerland can be as low as 12%. Currently, Switzerland is in the process of introducing via a corporate tax reform various general tax incentives, such as special R&D deduction regimes and also a patent box regime.

In particular, start-ups may benefit from a tax holiday on the cantonal and federal level if their tax domicile is located in a structurally less developed region of Switzerland. Furthermore, if a company sells a stake of at least 10% in an investment which has been held for at least one year prior to the sale of the participation, the realised profit benefits from a participation deduction. In addition, Swiss resident individuals are not taxed on capital gains realised on privately held assets. Dividend payments to companies which hold a participation of at least 10% or with a fair market value of at least CHF 1 million in the dividend paying company also benefit from the participation deduction. Dividend payments to Swiss resident individuals on substantial participations of at least 10% are taxed at a reduced rate.

Switzerland levies annual wealth taxes. In order to lessen the tax burden for start-up investors, start-up companies are often valued at their substance value for wealth tax purposes (*e.g.* in the Canton of Zurich).

In terms of management/employee incentives, Switzerland offers attractive participation schemes, which, if structured as an equity participation, generally aim to obtain a tax exempt capital gain (instead of taxable salary) for the Swiss resident managers upon an exit.

Finally, it is common in Switzerland to discuss the tax consequences of an envisioned structure with the competent tax administration and there is an uncomplicated process of obtaining advance tax rulings.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

The requirements for a listing on the SIX Swiss Exchange (the main Swiss stock exchange) are laid down in its Listing Rules and its Additional Rules and can be divided into (i) requirements regarding the issuer, and (ii) requirements regarding the securities to be listed. Essential criteria include, *e.g.*, (i) that the issuer has existed as a company for at least three years (however, exemptions exist) and has a reported equity capital of at least CHF 2.5 million. Furthermore, (ii) the securities must meet the minimum free float requirements (at least 20% of all of the issuer's outstanding securities in the same category have to be held in public ownership, and the capitalisation of those securities in public ownership has to amount to at least CHF 25 million).

The listing requirements of the BX Swiss (the second regulated Swiss stock exchange) are structured in the same way as those of the SIX Swiss Exchange, but they are less stringent (*e.g.* the issuer must only have existed as a company for at least one year and the share capital and the reported equity must only amount to at least CHF 2 million).

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

There have not been any recent IPOs in Switzerland in the specific area of fintech. However, in 2017, Warburg Pincus acquired 45% of the shares in Avaloq Group AG, a leading Swiss provider of software solutions and business process outsourcing services for the financial industry.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

The Swiss financial regulatory regime does not specifically address fintech. In fact, the recent new regulations addressing certain requirements for fintech companies in Switzerland have also been designed according to the principle of technology neutrality, meaning that business activities with substantially similar characteristics are subject to the same regulatory requirements irrespective of whether they are provided using advanced technology or in a more traditional format (although there is a newly introduced mid-range regulatory licence type that is colloquially referred to as “fintech licence”; *see* further below).

The Swiss legal framework governing the activities of traditional financial services providers and fintech operators consists of a number of federal acts and implementing ordinances as well as circulars and other guidance issued by FINMA. Fintech business models have to be assessed in light of this regulatory framework on a case-by-case basis (*see* question 1.2).

More specifically, based on their (intended) activities, fintech businesses may in particular fall within the scope of the Banking Act (“BA”) (if engaging in activities involving the professional acceptance of deposits from the public or the public solicitation of deposit-taking; *see* question 3.2), the Anti-Money Laundering Act (“AMLA”) (if active as a so-called financial intermediary, *e.g.* in connection with payment instruments, payment systems, individual

portfolio management or lending activities; *see* question 4.5), the Collective Investment Schemes Act (if issuing or managing investment funds or engaging in other activities relating to collective investment schemes), the Financial Market Infrastructure Act (if acting as a financial market infrastructure, *e.g.* a multilateral trading facility), the Stock Exchange Act (if acting as a securities broker-dealer or as a proprietary trader), or the Insurance Supervision Act (if acting as an insurer or insurance intermediary). Moreover, *inter alia*, the Consumer Credit Act (“CCA”), the Data Protection Act (“DPA”) as well as the National Bank Act may apply.

Depending on the specific business model, regulatory requirements may include licence or registration requirements as well as ongoing compliance and reporting obligations, in particular relating to organisation, capital adequacy, liquidity and documentation, as well as general fit-and-proper requirements for key individuals, shareholders and the business as such. Certain types of regulated businesses are prudentially supervised by FINMA on an ongoing basis in a two-tier approach, whereby an audit firm (regulatory auditor) appointed by the supervised entity carries out regulatory audits that will be an important basis for the supervision by FINMA. The individual financial market laws provide for *de minimis* and other exemptions that can potentially be relevant for fintech operators depending on the type and scale of their activities.

FINMA is the integrated supervisory authority for the Swiss financial market, ensuring a consistent approach to the qualification and regulatory treatment of fintech operators and other financial institutions. Furthermore, Switzerland has an established system of industry self-regulation by private organisations such as the Swiss Bankers Association SBA, the Swiss Funds & Asset Management Association SFAMA as well as numerous professional organisations for financial intermediaries. Some of the regulations issued by self-regulatory organisations have been recognised by FINMA as minimum standards (*e.g.* in the area of money laundering prevention).

Two major new financial market laws will come into force on 1 January 2020: the Financial Services Act (“FinSA”) and the Financial Institutions Act (“FinIA”). The FinSA contains cross-sectoral rules for the offering of financial services and the distribution of financial instruments and aims to reflect the principles implemented at EU level by the Markets in Financial Instruments Directives MiFID I/II. It will essentially require financial services providers to adhere to a code of conduct, which includes suitability and appropriateness assessments in case of asset management or investment advisory services. The FinIA will establish a differentiated, risk-based supervisory regime for portfolio managers, managers of collective assets, fund management companies and securities firms. As a result, specific fintech activities such as digital asset management services may become subject to a licence requirement by FINMA under the FinIA (in contrast to the current regime where individual asset managers only require a membership with a self-regulatory organisation for anti-money laundering purposes). In addition, digital financial advice or online investment management may in future be covered by the code of conduct rules of the FinSA.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

As Switzerland pursues a principle-based and technology-neutral approach in its legislation, the Swiss legal framework is, in principle, already suitable for dealing with cryptocurrencies and cryptoassets. At present, there is no regulation in Switzerland that is specifically directed at cryptocurrencies and cryptoassets. However, the Swiss Federal Council has proposed to further

improve the prerequisites for distributed ledger technology and blockchain applications and has identified in particular the following key areas for action:

- **Civil law:** Legal certainty in respect of the transfer of rights by means of decentralised digital ledgers may be improved by amending securities law in the Swiss code of obligations.
- **Insolvency law:** The segregation of crypto-based assets in the event of bankruptcy and the potential segregation of data with no asset value should be clarified by amending the Swiss Debt Enforcement and Bankruptcy Act.
- **Financial market laws:** A new and flexible authorisation category for blockchain-based financial market infrastructures should be introduced; as regards banking legislation, bank insolvency law provisions shall be reconciled with the adjustments in general insolvency law.
- **Anti-money laundering and anti-terrorist financing laws:** The treatment of decentralised trading platforms under the Anti-Money Laundering Act should be specified.

To further the legislative process, the Federal Council has instructed the Federal Department of Finance and the Federal Department of Justice and Police to draw up a preliminary draft for framework legislation and a corresponding explanatory report in the first quarter of 2019.

Previously, in February 2018, FINMA published guidelines that outline how the existing regulatory framework will be applied to the enquiries of ICO organisers. The guidelines address important AML and securities law aspects of digital tokens.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

Key representatives of FINMA have repeatedly expressed their principal openness to apply an innovation-friendly and technology-neutral approach to its regulatory and supervisory activities. FINMA has, *inter alia*, established a dedicated fintech desk to interact with fintech start-ups and has revised several of its circulars, which specify the practice of the regulator under the current legislation, to render them technology-neutral (*e.g.* by refraining from physical written form requirements relating to certain documentations or by enabling video and online identification for client-onboarding purposes). In the context of anti-money laundering, FINMA has also revised its respective ordinance introducing simplified organisational requirements for small fintech companies (*see* question 4.5).

In the same vein, Swiss policymakers have reaffirmed their liberal strategy towards the regulation of new technologies in the fintech sector. The Swiss Federal Minister of Finance stated at a roundtable event at the World Economic Forum that Swiss rules for innovations like blockchain will continue to target “processes, not technologies”, which means that new technologies themselves are not regulated but rather the impacts which they cause are overseen by existing legislation, made to be flexible enough to accommodate innovation. In order to make it easier for fintech start-ups to set up shop and to ease regulatory hurdles, a three-pillar legal reform programme was initiated by Swiss policy makers back in 2016. The three-pillar “light touch” programme included the introduction of a regulatory sandbox concept and the extension of the holding period from seven days to 60 days for third-party deposits, which already took effect on 1 August 2017. The third pillar of the legislative reform package refers to the introduction of a new

licensing category to the Swiss framework for financial market supervision and became effective on 1 January 2019:

- **Maximum holding period for settlement accounts:** The revision of the framework for banking legislation extended the time period for which third party monies accepted on interest-free accounts for the purpose of settlement of customer transactions do not qualify as “deposits from the public” (and therefore do not count towards a potential banking licence requirement) to a maximum of 60 days (instead of only seven days). Crowdfunding platforms in particular, but, *e.g.*, also payment service providers, the business model of which typically requires holding third party funds for a certain period of time, benefit from this broadened exemption. It should be noted that settlement accounts of foreign exchange dealers generally do not fall within the scope of the exception for settlement accounts. In the context of fintech, this may in particular affect cryptocurrency traders, which are subject to the same limitation if their business is conducted in a manner comparable to a traditional foreign exchange dealer.
- **Regulatory sandbox:** The Swiss regulatory sandbox provides an innovation space for fintech but also for other emerging businesses and other undertakings to test their business models. It allows any person, without the prior approval or review by the regulator (*i.e.* no licence requirement), to accept deposits from the public in an amount of up to CHF 1 million, regardless of the number of depositors. This exemption is, however, available only if the deposits are neither interest-bearing nor invested (or alternatively used for the purpose of financing a primarily commercial or industrial activity). As a mitigating measure, the deposit-taker must inform the depositors – before accepting any of their monies – that it is not supervised by FINMA and that the deposits are not covered by the depositor protection regime. As of 1 April 2019, new rules will enter into force explicitly prohibiting the interest margin business while at the same time enabling deposits received under the sandbox to be used for private purposes (*i.e.* not for commercial or industrial purposes).
- **Fintech licence:** Under the new licence category (frequently referred to as the “fintech licence” or “banking licence light”), FINMA may authorise companies that do not carry out traditional banking activities to accept deposits from the public up to a maximum threshold of CHF 100 million as long as the deposits are not invested and no interest is paid on them. Hence, companies that merely accept and hold public deposits up to the threshold amount and do not engage in the commercial banking business with maturity transformation are eligible for the fintech licence. The new licence type will bring a number of alleviations in the areas of minimum capital, capital adequacy and liquidity, governance, risk management, compliance, depositor protection as well as accounting and auditing for fintech companies, which so far had to rely on a fully-fledged banking licence for their commercial activities – with the associated regulatory burden. Irrespective of the reliefs granted, anti-money laundering regulation continues to apply to fintech firms if they qualify as financial intermediaries (the same applies to data protection law (*see* question 4.5)).

In addition, regulation professionalising the crowdlending market has been introduced by extending the scope of the CCA to crowdlending intermediaries as of 1 April 2019. Crowdlending intermediaries are now subject to certain reporting duties and further obligations in connection with the review of the creditworthiness of the borrowers.

The Swiss Federal Council published a draft partial revision of the Insurance Supervision Act for public consultation that ended on 28 February 2019. The draft law foresees the competence of FINMA to

exempt insurance undertakings with innovative business models from insurance supervision if this serves the sustainability of the Swiss financial market and the interests of the insured are safeguarded.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

The Swiss inbound cross-border regulatory regime for financial services is relatively liberal in comparison to international regulation. Many Swiss financial market regulatory laws do not apply to fintech (and other) businesses that are domiciled abroad and serve customers in Switzerland on a pure cross-border basis, *i.e.* without employing persons permanently on the ground in Switzerland (including by frequent travel). Notably, the BA and the AMLA apply only to foreign operators that have established a relevant physical presence in Switzerland, *e.g.* a branch or representative office. That said, cross-border operators that are not regulated in Switzerland should refrain from creating an (inaccurate) appearance of “Swissness”, *e.g.* by using a “.ch” website or referring to Swiss contact numbers or addresses.

However, it should be noted that some areas of Swiss financial regulation are more restrictive with regard to cross-border activities, notably the regulation of collective investment schemes as well as insurance regulation.

Furthermore, as Switzerland is neither a member of the EU nor of the EEA, there is no passporting regime available.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

Swiss data protection law is set forth in the DPA and the implementing Data Protection Ordinance (“DPO”). Swiss data protection law is influenced significantly by EU law, both in terms of content and interpretation.

Fintech firms are subject to the DPA if they process personal data in Switzerland. In this context, the mere storage of personal data on a server in Switzerland is sufficient. Deviating from most foreign data protection laws, the DPA also treats information referring to legal entities as personal data. It is worth mentioning that Swiss data protection law is based on an “opt out” model, meaning that the processing of personal data is not allowed against the express wish of a data subject, but the consent of a data subject is not a requirement for lawful processing (subject to specific rules regarding the processing of particularly sensitive personal data).

A fintech firm processing personal data in Switzerland must do so in accordance with the following data processing principles: good faith, proportionality, purpose limitation, transparency, accuracy, data security, and lawfulness. Furthermore, an obligation to register a data file with the Swiss Data Protection Commissioner (“Commissioner”), prior to any data processing, applies if the controller of a data file regularly processes so-called sensitive personal data (*e.g.* health data or trade union related views and activities) or personality profiles (*i.e.* a collection of data that

permits an assessment of essential characteristics of the personality of an individual), or regularly discloses personal data to third parties (including affiliates). The Commissioner maintains an online register of such data files (www.datareg.admin.ch). Registration is free of charge.

Currently, Swiss data protection law is under revision to adapt the DPA to the changed technological and social conditions and, in particular, to improve the transparency of data processing and strengthen the self-determination of data subjects. Furthermore the revision aims to further align Swiss data protection legislation with the requirements of the General Data Protection Regulation (EU) 2016/679 of the EU, as this is a key element to ensure continued EU recognition of Switzerland as a third country with an adequate level of data protection in order for cross-border data transmission to remain possible in the future. The revised DPA is, however, not expected to enter into force before January 2020.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

The activity of processing of personal data on equipment located in Switzerland is, in principle, within the scope of the DPA (*see* question 4.1). This is particularly relevant for foreign fintech firms that are processing personal data in Switzerland through branch offices or third party service providers.

The DPA prohibits a disclosure (transfer) of personal data to abroad if such a transfer could seriously endanger the personality rights of the data subjects concerned. This might be the case particularly if personal data is intended to be disclosed to a country where the local legislation does not guarantee an adequate protection of personal data. The Commissioner has published a (non-binding) list of countries that provide for an adequate level of data protection. In particular, all EU Member States are deemed to meet the requirement of adequate data protection rules. An important means to secure adequate protection for transfers to other countries is the use of model contracts for the transfer of personal data to third countries issued by the European Commission (EU Model Clauses), adapted to Swiss law requirements, or other contractual clauses explicitly recognised by the Commissioner. Another option is to obtain consent for the transfer from the data subject whose data is being transferred.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

The sanctions pursuant to the current DPA are moderate:

- **Civil law sanctions:** A data subject can file a request for an interim injunction against unlawful data processing. It is also possible to lodge a claim for correction or deletion of data or a prohibition on the disclosure of data to third parties. In addition, a data subject is entitled to compensation for actual damages caused by unlawful processing or other breaches of the DPA.
- **Criminal law sanctions:** The Commissioner is not competent to issue any fines. However, based on article 34 DPA, a competent criminal judge may, upon a complaint, sanction individuals with a fine of up to CHF 10,000 if they have wilfully breached certain information obligations stipulated in the DPA.

The draft revision of the DPA provides for an extension of the catalogue of criminal offences and an increase in the fines to be imposed to up to CHF 250,000 (*see* question 4.1).

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

The topic of cyber security is addressed by a number of legal provisions and initiatives:

- The DPA and the DPO set forth certain general security requirements applicable to the IT infrastructure deployed when processing personal data. Such requirements are accompanied by the Commissioner's guide for technical and organisational measures to be taken when processing personal data. It is to be noted that the current DPA does not require data processors to notify a Swiss authority or the data subject concerned of personal data breaches. However, the draft revision of the DPA provides for such an obligation to notify.
- The Swiss Criminal Code ("SCC") provides for statutory offences which protect IT infrastructure against cybercrime (*i.e.* against the unauthorised obtaining of data, unauthorised access to a data processing system, data corruption, *etc.*).
- The Reporting and Analysis Centre for Information Assurance MELANI supports private computer and internet users as well as providers of critical national infrastructures (such as banks, telecommunication services providers, *etc.*) with regard to risks relating to the use of modern information and communication technologies.
- The Federal Department of Defence, Civil Protection and Sport established a Cyber Defence Campus that commenced operations in January 2019, focusing on early detection and observation of current developments in the cyber-world and on the development of action strategies in this respect.

In 2011, Switzerland ratified the Council of Europe Convention on Cybercrime of 2001 (which entailed certain amendments of the SCC and the Swiss Federal Act on International Mutual Assistance in Criminal Matters of 20 March 1981).

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

The Swiss rules on prevention of money laundering and terrorist financing are set forth in the AMLA, the Anti-Money Laundering Ordinance ("AMLO"), ordinances and circulars of FINMA as well as the rulebooks of recognised self-regulatory organisations. Generally speaking, anti-money laundering ("AML") regulation applies to so-called financial intermediaries (and partially to merchants accepting large sums in cash, *i.e.* more than CHF 100,000, as payment in commercial transactions). On the one hand, certain prudentially regulated entities such as, *e.g.*, banks, securities dealers, fund management companies and life insurance undertakings qualify as financial intermediaries based on their regulatory status (*per se* financial intermediaries). On the other hand, any otherwise unregulated person or entity can qualify as a financial intermediary by virtue of its professional activities. In general, this refers to any person that, on a professional basis, accepts or holds on deposit third party assets or that assists in the investment or transfer of such assets. Many fintech business models include elements that lead to their operators qualifying as financial intermediaries in the meaning of the AMLA. If this is the case and no exemptions are available, the fintech firm is required to join a recognised Swiss AML self-regulatory organisation. In this context, the firm is required to comply with certain duties on an ongoing basis, in particular the duty to verify the identity of customers and the beneficial ownership in the relevant assets as well as documentation, reporting and audit requirements. In a push to eliminate barriers for technology-based

business models, FINMA has introduced a new circular that enables onboarding of customers via digital channels, e.g. by means of video transmission and other forms of online identification. This model has also been replicated in the rulebooks of recognised AML self-regulatory organisations.

The AMLA includes specific criminal provisions sanctioning the violation of duties under AML regulation. In addition, certain offences in the area of corruption and money laundering are set forth in general criminal law, meaning that they apply to fintech (and other) firms regardless of their qualification as a financial intermediary.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

Aside from financial regulation in various areas (see questions 3.1 *et seqq.*) and the data protection regime (see questions 4.1 *et seqq.*), fintech firms have to comply with general corporate and civil law provisions as well as with Swiss competition law on the basis of the Unfair Competition Act. Furthermore, depending on the specific business model, the Telecommunications Act may apply.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

Swiss employment law is based on the principle of freedom of contract and, as a general matter, relatively liberal. Individual employment contracts regulate the rights and obligations of employers and employees. Employment contracts can be concluded on a fixed-term basis (the contract ends on a date agreed from the outset) or on an open-ended basis (the contract ends by notice of termination). In case of an open-ended employment contract, statutory law prescribes that the first month of work is the probation period (but it can be contractually extended up to three months, be shortened, or be eliminated entirely). In case of a fixed-term employment contract, there is no statutory probation period (but it can be agreed). In the probation period, the statutory termination notice is seven days.

Private employment contracts can usually be terminated rather easily and, as a general principle, terminations do not lead to any statutory law obligations to render severance payments. The statutory period of notice is between one and three months, depending on the accrued duration of the employment relationship, but the parties are free to agree on another notice period, as long as the notice period is the same for both parties and amounts to at least one month. Nevertheless, the principle of freedom to terminate the employment contract is limited in two ways. First, there is a protection from unlawful dismissal (*missbräuchliche Kündigung*). A notice of termination is, e.g., unlawful where given because of an attribute pertaining to the person of the other party or because the other party in good faith asserts claims under the employment relationship (retaliation). The party having received the unlawful notification may raise a claim for compensation up to a certain threshold. Furthermore, there are restricted periods during which the parties are not allowed to terminate the employment contract (*Kündigung zur Unzeit*, e.g. during a certain period while the employee through no fault of his or her own is partially or entirely prevented from working by illness or accident, or during the pregnancy of an employee and the 16 weeks following birth).

Furthermore, Swiss employment law, e.g., provides for special rules to be met in cases of mass redundancies.

5.2 What, if any, mandatory employment benefits must be provided to staff?

The employer must pay its employees the agreed or customary salary or the salary fixed by standard employment or collective employment contracts. No statutory minimum salary exists in Switzerland, but for certain professions, collective and standard employment agreements set minimum salaries.

The employer may, and in some cases must, make deductions from the salary. Social insurance premiums are paid either by the employer alone, or by the employer and the employee together with the employer deducting the employee's portion of social insurance premiums from the employee's salary. Further deductions are made for unemployment insurance and non-professional accident insurance. The premiums for mandatory occupational pension schemes are fixed by the relevant institutions and borne collectively by the employers and the employees. Health insurance premiums are, unless otherwise agreed, borne by the employees and handled separately from the employment.

The parties are, in principle, free to determine the regular weekly working time. Typically, for full-time employment, a weekly working time between 40 and 44 hours is agreed upon. Overtime hours must be compensated in principle (by remuneration or leisure time). However, public law provisions limit the maximum working time (to 45 hours or 50 hours per week depending on the nature of the work).

Employers in Switzerland must grant their employees at least four weeks of vacation per year, and in the case of employees under the age of 20, at least five weeks of vacation (excluding public holidays). Part-time employees have a *pro rata* entitlement. During the vacation, the employee is entitled to the continued payment of his or her salary.

If the employee is prevented from working due to personal circumstances for which the employee is not at fault, e.g. illness, accident, legal obligations or public duties, the employer must pay the employee a salary for a limited period of time provided that the employment relationship lasted or was concluded for longer than three months. Furthermore, a female employee is entitled to maternity leave of at least 14 weeks. Paternity leave is currently not granted under Swiss law but may be agreed upon by the parties to the employment contract.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

As a general matter, foreign nationals engaged in any kind of gainful employment in Switzerland must apply for a work permit. An exception to the permit requirement applies to business visits of a duration not exceeding eight days as well as third-country nationals who do not work more than eight days per calendar year in Switzerland. Switzerland has a dualistic system for the admission of foreign workers where, on the one hand, nationals from EU/EFTA states can benefit from the Agreement on the Free Movement of Persons (*Personenfreizügigkeitsabkommen*), while permits for nationals from third countries are subject to nationwide quantitative restrictions (quotas).

EU/EFTA nationals according to the Agreement on the Free Movement of Persons (*Personenfreizügigkeitsabkommen*) have a right to a work permit if they have an employment relationship with an employer in Switzerland. No permit is required for work for a duration of less than 90 days per calendar year (there is only a reporting requirement). The same applies to self-employed service providers and companies based in these countries posting workers to Switzerland if the employees have held a valid EU work permit for at least 12 months prior to their assignment to Switzerland. All EU/EFTA citizens being employed by a company in Switzerland for longer than 90 days per calendar year are required to obtain a permit in the form of either (i) a short-term permit for up to four months of uninterrupted stay or 120 days per year, (ii) a short-term permit for up to one year (the actual period of validity depends on the duration of the limited employment contract; “L-Permit”), (iii) a long-term permit for five years based on an unlimited (or at least one-year) employment contract (“B-Permit”), or (iv) a so-called border-crosser permit if they continue to live outside of Switzerland but commute to their Swiss workplace (“G-Permit”). Self-employment EU/EFTA nationals also requires permission, which may be granted for five years upon establishment of a business or permanent establishment with effective and viable business activities in Switzerland.

In contrast, non-EU/non-EFTA citizens have to apply for either (i) a short-term permit for up to four months/120 days per calendar year, (ii) a short-term permit for up to 12 months based on a limited employment contract (“L-Permit”), or (iii) a long-term permit that is valid for an unlimited period but needs to be renewed annually based on an unlimited employment contract (“B-Permit”). With certain exceptions, work permits for citizens of non-EU/non-EFTA countries are subject to a nationwide quota. Furthermore, such permits are only granted to highly qualified employees (*e.g.* senior management positions, specialists or other qualified personnel). In case the person was not assigned from a foreign company to a Swiss affiliate (intra-group transfer), it must be shown that no appropriate candidate throughout Switzerland and EU/EFTA countries can be found. Non-EU/non-EFTA citizens wishing to start working on a self-employed status must submit an application together with a business plan, proof of financial means and a certificate of registration. The competent authority will review the business plan and assess the relevant market situation.

Special rules apply to persons holding a work permit from one of the EU/EFTA countries for more than one year being employed by an employer with domicile in the EU-/EFTA-area. Such persons can be assigned to Switzerland for up to 90 days per calendar year without meeting the requirements as set forth above.

Switzerland does not have a specific immigration scheme for the fintech sector.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Fintech inventions are predominantly protected either by copyright law or by patent law. Assuming that fintech products are typically based on computer programs – or more broadly software – they are protected by copyrights if they possess an individual character (*i.e.* if they are original). In practice, this criterion relates to the novelty or absence of triviality in comparison to existing computer programs. Copyrights in computer programs cover the source code and object code. However, the underlying ideas and principles as well as

algorithms and formulas used in and for computer programs are not protected. Copyright protection in computer programs expires 50 years after the author deceases. Software that is integral to an invention may further be patented for a period of 20 years. However, computer programs *per se* are excluded from patentability.

In addition, the design of fintech products (*e.g.* if implemented in portables, wearables, *etc.*) may be protected for a maximum period of 25 years by design rights. Fintechs may also seek protection under the Trademark Act and register graphical representations for the distinction of the company’s products or services during a period of 10 years (renewable). Marketable products are further protected by the Unfair Competition Act against technical reproduction processes and exploitation without appropriate effort on the part of the reproducing party. Unlike the laws of EU Member States, Swiss law does not provide for database rights.

The protection of fintech inventions or innovation as trade and business secrets may also be based on statutory or contractual obligations.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

As a general rule, the primary owner of the copyright is the author, *i.e.* the natural person who created the work. Computer programs – or more broadly software – are works as defined by Swiss copyright legislation. The copyright automatically vests in the author and exists informally upon the moment of intellectual creation; registration is not required.

In case a computer program has been created under a contractual employment relationship in the course of fulfilling professional duties and contractual obligations, the employer alone is entitled to exercise the exclusive rights of use. Similar statutory rules apply as regards to designs and inventions (patents). However, unlike the situation regarding computer programs, the acquisition of inventions and designs is subject to the payment of an additional compensation to the employee if they have been created outside the performance of contractual obligations (mandatory claim). Outside employment relationships, the IP rights (copyrights) or the right to apply for IP protection (patents, designs) vest in the person who has created the work, inventions or design.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

In Switzerland, only (Swiss) national IP rights are enforceable. This also applies if an IP right has been applied for via an international application system (*e.g.* WIPO’s international patent system PCT or the international trademark system) or regional application system (*e.g.* patent applications under the European Patent Convention) and if Switzerland was chosen as the designated state in respective applications (the resulting rights are national rights, not multi-jurisdictional rights).

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

IP rights are, as a general matter, exploited/monetised by means of assignment (transfer), licensing, and the granting of security interests. There are slightly different formalities for the various

types of IP rights in respect of assignments and licences. Subject to the assignment of copyrights, an assignment must be in writing and signed by the assignor. The recording of the change of ownership in the relevant IP register is not a requirement for the assignment and transfer to the assignee, but may be advisable since a change of ownership not recorded in the register is not relevant for persons who have acquired IP rights in good faith. The written form is not required for licence agreements in general.

Both the licence agreements and the pledge agreements pertaining to trademarks, patents and designs may be entered in the relevant IP register at the request of one of the contractual parties. As a consequence, they become binding on any rights related to trademarks, patents and designs subsequently acquired.



Dr. Daniel Flühmann

Bär & Karrer
Brandschenkestrasse 90
CH-8027 Zurich
Switzerland

Tel: +41 58 261 50 00
Email: daniel.fluehmann@baerkarrer.ch
URL: www.baerkarrer.ch

Daniel Flühmann is a partner in Bär & Karrer's financial services department and co-head of the fintech practice group. His work focuses on banking, insurance and financial markets laws as well as on the area of collective investment schemes. He advises Swiss and foreign banks and securities dealers as well as insurance companies and other financial services providers on regulatory and contract law matters and in the context of enforcement proceedings. A special focus of Daniel Flühmann's practice lies on fintech, both in the context of advising start-up businesses and more established financial institutions, as well as on blockchain technology and the legal framework of its applications in practice. Furthermore, he advises clients on general corporate and commercial matters as well as on M&A transactions.



Dr. Peter Ch. Hsu

Bär & Karrer
Brandschenkestrasse 90
CH-8027 Zurich
Switzerland

Tel: +41 58 261 50 00
Email: peter.hsu@baerkarrer.ch
URL: www.baerkarrer.ch

Peter Hsu is the key contact of Bär & Karrer for the practice area of banking & insurance. His work focuses on banking, insurance, financing and capital markets. He regularly advises Swiss and foreign financial institutions as well as fintech businesses on M&A, regulatory, corporate and contract law matters. Furthermore, he represents clients in regulatory licensing and in enforcement proceedings. Moreover, he often advises clients on M&A transactions as well as in other industries.

BÄR
& KARRER

Bär & Karrer is a renowned Swiss law firm with more than 150 lawyers in Zurich, Geneva, Lugano and Zug.

Our core business is advising our clients on innovative and complex transactions and representing them in litigation, arbitration and regulatory proceedings. Our clients range from multinational corporations to private individuals in Switzerland and around the world.

Most of our work has an international component. We have broad experience handling cross-border proceedings and transactions. Our extensive network consists of correspondent law firms which are all market leaders in their jurisdictions.

Bär & Karrer was repeatedly awarded Switzerland Law Firm of the Year by the most important international legal ranking agencies in recent years.

- 2018, 2016, 2015 and 2014 Mergermarket European M&A Awards.
- 2018 *IFLR* M&A Deal of the Year.
- 2018 Best in Trusts & Estates by *Euromoney LMG*.
- 2018, 2017 Trophées du Droit Silver.
- 2016, 2013 and 2012 *Chambers* Awards.
- 2016, 2015 and 2014 *The Legal 500* ("most recommended law firm in Switzerland").
- 2016 Trophées du Droit Gold.
- 2015 and 2014 *IFLR* Awards.
- 2015, 2014, 2013, 2011, 2010 The Lawyer European Awards.
- 2015 Citywealth Magic Circle Awards ("Law Firm of the Year – EMEA").
- 2014 Citywealth International Financial Centre Awards.

Taiwan



Robin Chang



K. J. Li

Lee and Li, Attorneys-at-Law

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

The Fintech sector has continued its development in Taiwan. In February 2015, Taiwan's Legislative Yuan passed the Act Governing Electronic Payment Institutions to govern E-payment business in Taiwan ("E-Payment Act"). Also, in April 2015, the Financial Supervisory Commission ("FSC") issued the Rules Governing the Administration of Electronic Payment Business ("E-Payment Rules") and other regulations to regulate the business management of E-payment institutions. The E-Payment Act and E-Payment Rules enable E-payment companies to legally conduct a third-party payment business in Taiwan. In addition to the E-Payment Act and E-Payment Rules, the FSC also issued the Fintech Development Strategy White Paper ("White Paper") in May 2016, and proposed the draft of the Financial Technology Development and Innovative Experimentation Act ("Fintech Innovation Act") on January 12, 2017, which was passed by the Legislative Yuan on December 29, 2017 and officially announced on January 31, 2018. The FSC also approved the Self-Regulation Guidelines Governing Business Cooperation Between Member Banks of Bankers Association of the Republic of China and Peer-to-Peer Lending Platform Operators ("P2P Self-Regulation Guidelines") on December 1, 2017.

According to the White Paper, the FSC highlighted the following key policy directions for fintech in Taiwan: E-payment; blockchain; investment in fintech companies; banking industry (use of tokenisation technology for credit card transactions); securities industry (online services, automated trading mechanisms such as robot-advisory services and consolidated internet sale platform of mutual funds, cloud services, Big Data application); insurance industry (online insurance purchase, investment in fintech innovation and new insurance products, Big Data); virtual and physical branches; identity verification mechanisms; regulatory updates; and risk management. Taiwan's Executive Yuan, the superior of the FSC, issued a press release in June 2017 announcing that the FSC will continue to support the development of fintech.

Under Taiwan law, conducting finance-related activities in Taiwan generally requires a licence from the FSC. However, similar to the "regulatory sandbox" concept raised by the Financial Conduct Authority in UK, the FSC will set up a fintech experiment

mechanism under the Fintech Innovation Act to provide a safe environment for the development and testing of fintech, exempt fintech innovation from the current licensing requirements for financial business and stipulate applicable regulations on fintech experiments. If a financial institution or non-financial institution plans to conduct fintech business in Taiwan, such institution may apply to the FSC for prior approval (the "Fintech Approval") for its financial innovation experiments in accordance with the Fintech Innovation Act. If the permitted innovation experiment has any result and such result passes the FSC's review, the institution may apply for the FSC's approval to conduct that business. According to the FSC's press release on September 18, 2018, the FSC granted its first Fintech Approval to KGI Commercial Bank Co., Ltd. on the same date in respect of its application for experimenting in using telecom mobile identity authentication technology in online credit card business.

Besides this, the FSC has instructed the Bankers Association of the Republic of China ("BAROC") to draft the P2P Self-Regulation Guidelines and the FSC approved such Self-Regulations on December 1, 2017. According to the P2P Self-Regulation Guidelines, the P2P lending platform operators should not act as lenders. However, banks mandated by the P2P lending platform operators may provide services such as running credit checks and providing cash flow, cash custody and credit documents custody services. Also, banks may cooperate with P2P lending platform operators on banks' lending businesses and advertising activities. Accordingly, P2P lending platform operators may provide their P2P lending service together with banks under the Self-Regulations.

Another issue worth noting is that the FSC issued a press release on June 26, 2018 stating its policy for digital-only banks. The FSC further amended the Standards Governing the Establishment of Commercial Banks (the "Bank Establishment Standards") on November 14, 2018 for digital-only banks. A digital-only bank may conduct the same business as conventional commercial banks without setting up any branches, and the minimum paid-in capital required is NT\$10 billion. The FSC schedules to accept applications for digital-only bank licences from November 15, 2018 to February 15, 2019 and expects to issue two digital-only bank licences.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

Please refer to our advice in question 1.1 above. Currently, the FSC does not issue any regulations or rulings to expressly prohibit any

type of fintech business from financial innovation experiments under the Fintech Innovation Act.

In respect of cryptocurrency-based businesses, on December 30, 2013, both Taiwan's Central Bank and the FSC first expressed the Taiwan government's position toward "Bitcoin" by issuing a joint press release. According to the 2013 press release, the two authorities held that Bitcoin should not be considered a "currency", but a highly speculative digital "virtual commodity". In another FSC press release in 2014, the FSC ordered that local banks must not accept Bitcoin or provide services related to Bitcoin (such as exchange Bitcoin for fiat currency). In addition, a report issued by Taiwan's Central Bank on virtual currency in March 2016 and the FSC's press releases in January 2016 both considered Bitcoin to be a virtual commodity issued by private entities to be used and accepted by members of a specific virtual commodity community. However, since Bitcoin is not a legal currency, the FSC in its press release has a clear position that financial institutions are not allowed to accept or exchange Bitcoin and are prohibited from providing cryptocurrency-related services via bank ATMs.

Given the above, in light of the authorities' attitude, Bitcoin is not considered "legal tender", "currency" or a generally accepted "medium of exchange" under the current regulatory regime in Taiwan; instead, Bitcoin is deemed as a digital "virtual commodity". Please note that the Taiwan government's attitude stated in the abovementioned press releases only covers Bitcoin, instead of any types of virtual currencies/cryptocurrencies. But we tend to think that any virtual currencies/cryptocurrencies, if having the same nature and characteristics as Bitcoin, should also be considered as digital "virtual commodities". Further, currently there exists no required licence in Taiwan for (a) operating the services of exchange between virtual currencies or virtual currencies and fiat currencies, or (b) acting as a "money transmitter" and the like in Taiwan.

In addition, although the laws of Taiwan do not explicitly prohibit initial coin offering ("ICO") activities, according to the FSC's further press release issued on June 22, 2018, should an issuer offer tokens in the course of a public sale (i.e., an ICO), and such tokens are deemed as "securities" under the Securities and Exchange Act, which are determined on a case-by-case basis, such offering of tokens would be deemed as offering of securities to the public and a prior registration with the FSC would be required. However, the FSC has not addressed the case in which such tokens are deemed as a type of utility token but not a type of security.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

Aside from IPOs (see further the requirement for an IPO advised in the answer to question 2.3 below), as named in our chapter for the *ICLG to: Fintech 2017*, there are two crowdfunding options in Taiwan: "Gofunding Zone"; and "Go Incubation Board". The Gofunding Zone, which was established for non-equity-based crowdfunding, was terminated on May 10, 2018. Investors, however, may still consider the Go Incubation Board as an equity-based crowdfunding method. The Go Incubation Board provides an equity-based funding alternative to innovative enterprises. Enterprises listed on the Go Incubation Board of Taipei Exchange do not need to conduct an initial public offering. Instead, they are only required to, among other things, report the CPA audited financial statements (in the cases that: (i) the capital exceeds NT\$30 million; or (ii) although the capital is below NT\$30 million, the net income reaches NT\$100 million or the number of

insured labourers exceeds 100) and other material information, and are subject to simplified periodical report requirements.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

According to Articles 23-1 and 23-2 of the Statute for Industrial Innovation, if a venture capital enterprise invests in an innovative enterprise (established for less than three years), while its paid-in capital meets the standard of each year (at least NT\$300 million in the fifth year since incorporation) and the total amount invested in the innovative enterprise reaches 35% of the paid-in capital or NT\$300 million (whichever is lower), or if an individual whose investment in an innovative enterprise reaches NT\$1 million and such individual has held the shares in the innovative enterprise for more than two years, the venture capital enterprise or the individual would be entitled to some tax benefits in accordance with the Statute for Industrial Innovation.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

There are two securities exchanges in Taiwan: Taiwan Stock Exchange; and Taipei Exchange. In addition to the non-listed crowdfunding option, Go Incubation Board, offered by Taipei Exchange as advised in question 2.1 above, the two exchanges' major listing conditions for a Taiwanese company are as follows:

1. Taiwan Stock Exchange.
 - Duration of corporate existence: Three years.
 - Company size: Paid-in capital or net worth reaches NT\$600 million or market capitalisation reaches NT\$1.6 billion.
 - Profitability: The cumulative net income before tax for the most recent three fiscal years reaches NT\$250 million, and the net income before tax for the most recent fiscal year reaches NT\$120 million and the issuer has no accumulated deficits. However, certain newly established companies which meet statutory requirements are exempted from this profitability requirement.
2. Taipei Exchange.
 - Duration of corporate existence: Two years.
 - Company size: Shareholders' equity reaches NT\$100 million.
 - Profitability: The ratio of income before tax to shareholders' equity shall meet one of the following requirements, and the income before tax for the most recent year shall reach NT\$4 million: (i) most recent fiscal year: the ratio shall exceed 4% and there shall be no accumulated deficit; or (ii) the last two fiscal years: the ratio shall exceed 3% in each year or averages 3% over the two years, and the ratio for the most recent year is better. However, certain newly established companies which meet statutory requirements are exempted from this profitability requirement.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

As fintech is a new and developing area in Taiwan, to our knowledge, there has not been any case of notable exits (especially an IPO) by the founders of fintech businesses so far.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

As advised in question 1.1 above, in February 2015, Taiwan's Legislative Yuan passed the E-Payment Act, and the FSC has granted its approval to five E-payment service providers (other than banks) to conduct E-payment business in Taiwan. Also, on December 1, 2017, the FSC approved the P2P Self-Regulation Guidelines of BAROC for P2P lending platform operators and banks to work together for P2P lending services. In addition, the Fintech Innovation Act, announced on January 31, 2018, is another piece of fintech legislation to offer a safe harbour for fintech service providers to experiment with financial technology innovations in Taiwan. As mentioned above, since the announcement of the Fintech Innovation Act, the FSC granted one approval to KGI Bank on September 18, 2018. Moreover, the FSC adopted policies to approve the establishment of digital-only banks and made corresponding amendments to the Bank Establishment Standards, issued on November 14, 2018. The FSC schedules to accept applications for digital-only bank licences from November 15, 2018 to February 15, 2019 and expects to issue two internet-only bank licences.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

Under the newly amended Money Laundering Control Act on November 7, 2018, cryptocurrency platforms and the enterprises that conduct the business of trading cryptocurrency are subject to the requirements under the Money Laundering Control Act, including the adoption of certain KYC and AML measures and reporting suspicious transactions to the Investigation Bureau, MOJ.

Aside from the anti-money laundering rules mentioned above, Taiwan has not promulgated any other laws or regulations specifically dealing with the rise of certain applications of blockchain technology, such as so-called "virtual currencies" or "cryptocurrencies". Taiwan's financial regulators have issued several press releases to announce their positions and attitude towards such developments, as well as to educate and warn the general public in Taiwan.

As advised in the answer to question 1.2, on December 30, 2013, both Taiwan's Central Bank and the FSC first expressed the Taiwan government's position towards Bitcoin by issuing a joint press release. According to the 2013 press release, the two authorities held that Bitcoin should not be considered a "currency", but a highly speculative digital "virtual commodity". In another FSC press release in 2014, the FSC ordered that local banks must not accept Bitcoin or provide services related to Bitcoin (such as exchanging Bitcoin for fiat currency). In addition, a report issued by Taiwan's Central Bank on virtual currency in March 2016 and the FSC's press releases in January 2016 both considered Bitcoin to be a virtual commodity issued by private entities to be used and accepted by members of a specific virtual commodity community. However, since Bitcoin is not a legal currency, the FSC in its press release has a clear position that financial institutions are not allowed to accept or exchange Bitcoin and are prohibited from providing cryptocurrency-related services via bank ATMs.

Given the above, in light of the authorities' attitude, Bitcoin is not considered "legal tender", "currency" or a generally accepted

"medium of exchange" under the current regulatory regime in Taiwan; instead, Bitcoin is deemed as a digital "virtual commodity". Please note that the Taiwan government's attitude stated in the abovementioned press releases only covers Bitcoin, instead of any types of virtual currencies/cryptocurrencies. But we tend to think that any virtual currencies/cryptocurrencies, if having the same nature and characteristics as Bitcoin, should also be considered as digital "virtual commodities". Further, currently there exists no required licence in Taiwan for (a) operating the services of exchange between virtual currencies or virtual currencies and fiat currencies, or (b) acting as a "money transmitter" and the like in Taiwan.

In addition, although the laws of Taiwan do not explicitly prohibit ICO activities, according to the FSC's press release further issued on June 22, 2018, should an issuer offer tokens in the course of a public sale (i.e., an ICO), and such tokens are deemed as securities under the Securities and Exchange Act, which are determined on a case-by-case basis, such offering of tokens would be deemed as offering of securities to the public and a prior registration with the FSC would be required. However, the FSC has not addressed the case in which such tokens are deemed as a type of utility token but not a type of security.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

As advised in the answer to question 1.1 above, under the Fintech Innovation Act, the FSC will set up a Fintech experiment mechanism under the Fintech Innovation Act similar to the "regulatory sandbox" concept to provide a safe environment for the development and testing of fintech, exempt fintech innovation from the current licensing requirements for financial businesses and stipulate applicable regulations on fintech experiments. Both the financial institutions proposing to conduct fintech business and the non-financial institutions proposing to use the information, internet or other technologies to conduct fintech business in Taiwan, may apply to the FSC for the Fintech Approval to conduct financial innovation experiments in accordance with the Fintech Innovation Act. We believe this is a good indication of the Taiwan government's open-minded policy principles for fintech services.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

The Fintech Innovation Act does not stipulate that foreign fintech institutions can apply to the FSC directly for prior approval to conduct financial innovation experiments in accordance with the Fintech Innovation Act. Therefore, legally speaking, a foreign fintech institution may only handle relevant matters in accordance with the Fintech Innovation Act after it establishes a branch or a subsidiary in Taiwan.

In addition, if the foreign fintech institution is an E-payment institution and it proposes to conduct E-payment business in Taiwan, such foreign fintech institution shall establish an E-payment institution in Taiwan and apply for the FSC's prior approval under the E-Payment Act. If it proposes to cooperate with a Taiwanese E-payment institution for the Taiwanese E-payment institution to handle the payment and collection relating to local

fund flow on its behalf, the Taiwanese E-payment institution shall apply for the FSC's prior approval to cooperate with the foreign E-payment institution under Article 14 of the E-Payment Act.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

In Taiwan, the Personal Data Protection Act (the "PDPA") is the general law regulating the collection, processing and use of personal data, and all enterprises in Taiwan, including fintech enterprises, are subject to the PDPA. The main competent authority of the PDPA is the Ministry of Justice ("MOJ") which issues various rulings in accordance with the PDPA. In addition, each government agency may also issue its regulations under the PDPA to regulate the companies under its supervision. For example, the FSC also regulates local banks' compliance with the PDPA. The local regulators' interpretations of the PDPA are not binding upon Taiwan courts, but would usually be consulted as references by Taiwan courts in rendering their judgments.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

Under the PDPA, any non-governmental agencies, which include any natural persons, juristic persons and unincorporated associations other than government agencies, must comply with the PDPA when collecting, processing or using an individual's personal data within Taiwan. The PDPA also provides that any collection, processing or use of personal data of a Taiwanese individual by any non-governmental agency outside Taiwan should comply with the requirements of the PDPA.

In addition, according to a ruling issued by the MOJ on August 26, 2015, the collection, processing or use of an individual's personal data by a foreigner or a foreign company within Taiwan is also subject to the PDPA, regardless of whether such foreign national or entity is registered in Taiwan.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

Where a non-government agency violates the PDPA, the competent authority has the power to impose administrative fines and/or rectification orders on it. In addition, the following major breaches may lead to individual criminal liability of the violator:

- illegal collection, processing or use of personal data with the intent to make unlawful profits for itself or a third party, or with the intent to damage the interests of another, causing injury to another (Article 41 of the PDPA); and
- illegal change or deletion of personal data files or employment of any other illegal means with the intent to make unlawful profits for itself or a third party, or with the intent to damage the interests of another, thereby impeding the accuracy of personal data files and causing injury to another (Article 42 of the PDPA).

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

The Security Control and Procedure Standards for Financial Institutions Handling E-Banking Business are the main regulations governing the security requirements applicable to banks which conduct E-banking business. Also, the Regulations Governing the Standards for Information System and Security Management of Electronic Payment Institutions are the main regulations governing the security requirements applicable to E-payment institutions. In addition, the Security Control and Procedure Standards for Financial Institutions Handling E-Banking Business are the main regulations governing the security requirements applicable to banks which cooperate with P2P lending platforms in respect of P2P business.

The Fintech Innovation Act does not clearly provide that fintech businesses are subject to the security requirements under said regulations. However, since a fintech enterprise must apply with the FSC for prior approval to conduct financial innovation experiments, we believe that the FSC will review the applicant's proposed security measures on a case-by-case basis in order to ensure that such measures can protect the transactions involved and the interests of its customers.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

The Money Laundering Control Act imposes certain AML requirements on financial institutions and certain non-financial institutions (including enterprises and their employees where the business and transaction type make them easily used as a money laundering channel). This includes the adoption of certain KYC and AML measures and the reporting of AML suspicious transactions to the Investigation Bureau, MOJ. The MOJ announced on February 19, 2014 that third-party payment service operators will be subject to the requirements of the Money Laundering Control Act. In addition, under the newly amended Money Laundering Control Act dated November 7, 2018, cryptocurrency platforms and the enterprises that conduct the business of trading cryptocurrency are also subject to the requirements under the Money Laundering Control Act.

In addition, the Counter-terrorism Financing Act in Taiwan also requires institutions regulated by the Money Laundering Control Act to report to the Investigation Bureau, MOJ if they are aware (i) that they hold or manage the properties or property interests of any sanctioned person, or (ii) of the place where the properties or property interests of the sanctioned person are located.

The Fintech Innovation Act does not exempt an applicant from the application of the Money Laundering Control Act and the Counter-terrorism Financing Act. The financial institutions and the non-financial institutions proposing to conduct fintech business therefore shall still comply with the anti-money laundering and counter-terrorism financing laws and regulations issued by the FSC and other relevant government agencies.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

In addition to the Fintech Innovation Act, the FSC can amend the relevant laws and regulations to clearly provide that the relevant financial enterprises follow the Fintech Innovation Act to conduct

financial innovation experiments, which include the Banking Act, Insurance Act, Securities and Exchange Act, Futures Trading Act, E-Payment Act, Act Governing Issuance of Electronic Stored Value Cards, Securities Investment Trust and Consulting Act, Trust Act and Financial Consumer Protection Act. The FSC can also instruct BAROC to amend the P2P Self-Regulation Guidelines.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

The Labor Standards Act (“LSA”) and the relevant regulations govern the major employment requirements in Taiwan.

Employment terms and conditions agreed to by an employer and an employee should be no less favourable than the minimum/mandatory requirements set forth under the LSA and the relevant regulations, otherwise they are null and void and will be superseded by the corresponding provisions prescribed under the LSA. For employment terms and conditions not stated in an employment contract or the employer’s work rules/policies, the legal minimum/mandatory requirements shall apply. For employment terms and conditions provided in an employment contract or the employer’s work rules/policies which are more favourable than the legal requirements, such favourable terms and conditions shall prevail.

As to the termination of the employment contract, an employer should not terminate an employment contract unilaterally unless any of the events specified in Article 11 (layoff with advance notice and severance pay) or Article 12 (dismissal without notice or pay) of the LSA occurs.

In addition, Taiwan’s Legislative Yuan passed the amendments to the LSA on January 31 and November 21, 2018. The key points of the amendments to the LSA include: the removal of the implementation of a five-day work week; increase in the maximum working hours; permitting time off in exchange for overtime pay; reducing the rest time between shifts; allowing the regular leave adjustment for each cycle of seven days; and permitting unused annual leave to be postponed and used in the following year. The amendments have significant impact on employers’ costs and their human resource management.

5.2 What, if any, mandatory employment benefits must be provided to staff?

The main mandatory employment benefits provided under the LSA include salary, overtime pay, breaks, public holidays, annual leave, statutory leave with pay (such as wedding leave, funeral leave, pregnancy check-up leave, etc.), statutory social insurance (including Labour Insurance and National Health Insurance), statutory pension and compensation for occupational hazards.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

According to the Employment and Service Act, no foreigner may work in Taiwan without a work permit from the labour authority,

which should be applied for by his/her employer. In accordance with the regulations governing the employment of foreign employees, the Taiwan branch of a foreign company or a company invested in by foreigners with approval of the Investment Commission, Ministry of Economic Affairs may apply with the Ministry of Labour for the work permits required for employing foreign employees as technicians or managerial officers of the applicant company, provided that the requirements of the employer and the foreign employee set forth in the relevant rules and regulations are met. Therefore, work permits are required before those employees start working in Taiwan.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Innovations and inventions can be protected with intellectual property rights such as patents, copyright or trade secrets in Taiwan in accordance with the Patent Act, Copyright Act and Trade Secret Act. As to patents, an inventor may file an application with Taiwan’s Intellectual Property Office, and the patent right will be obtained and protected under the Patent Act once the application is approved. Local and foreign companies may also register their trademarks in Taiwan with the Intellectual Property Office under the Trademark Act. For copyright and trade secrets, there is no registration or filing requirement for protection under Taiwan law. However, certain requirements under the Copyright Act and the Trade Secret Act must be met in order to qualify as a “protected” copyright or trade secret, such as “originality” and “expression” for a copyright, and “economic valuable” and “adoption of reasonable protection measures” for a trade secret.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

As to patents, if an invention is made by an employee during the course of performing his or her duties under employment, the right to the invention shall be vested in his or her employer and the employer shall pay the employee reasonable remuneration unless otherwise agreed by the parties. If an invention is made by a contractor, the agreement between the parties shall prevail, or such rights shall be vested in the inventor in the absence of such agreement. However, if there is a funding provider, the funding provider may use such invention.

As to trade secrets, if a trade secret is the result of research or development by an employee during the course of performing his or her duties under employment, it shall belong to the employer unless otherwise agreed by the parties. If a trade secret is developed by a contractor, the agreement between the parties shall prevail, or such rights shall be vested in the developer in the absence of such agreement. However, if there is a funding provider, the funding provider may use such invention.

For copyright, if a work is completed by an employee within the scope of employment, such employee is the author of the work but the economic rights to such work shall be enjoyed by the employer unless otherwise agreed by the parties. If a work is developed by a contractor, the contractor who actually makes the work is the author of the work unless otherwise agreed by the parties; the enjoyment of the economic rights arising from the work shall be agreed by the parties, or such rights shall be enjoyed by the contractor in the absence of such agreement. However, the commissioning party may use the work.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

As to patents, as advised in question 6.1 above, an inventor must file an application with Taiwan's Intellectual Property Office, and the patent right will be obtained once the application is approved.

As to trade secrets and copyright, as advised in question 6.1 above, there is no registration or filing requirements for a copyright or a trade secret to be protected under Taiwan law. Trade secrets will be protected under the Trade Secret Act if they satisfy the following constituent elements: (i) they contain information that may be used in the course of production, sales or operations; (ii) they have the nature of secrecy, with economic value; and (iii) they have adopted reasonable protection measures. However, a foreigner's trade secrets will not be protected under the Trade Secret Act if the foreign national's home country has not signed a bilateral trade secrets protection treaty or agreement with Taiwan or if they do not meet the "reciprocity" requirement. Since Taiwan's accession to the

WTO as of January 1, 2002, the trade secrets of natural or juristic persons of WTO members which satisfy the aforementioned constituent elements may likewise enjoy trade secret protection under the reciprocity principle.

For copyright, it subsists upon the completion of a work rather than the registration of the work. A foreigner's works may enjoy copyright protection under the Copyright Act if they meet either the "First Publication" or "Reciprocity" requirement. Since Taiwan's accession to the WTO, the works of natural or juristic persons of WTO members enjoy the same copyright protection under the reciprocity principle.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

In local practice, generally, a patent, copyright or trade secret could be exploited/monetised by way of licensing or transfer to another entity.



Robin Chang

Lee and Li, Attorneys-at-Law
9F, 201 Tun Hua N. Road
Taipei 10508
Taiwan

Tel: +886 2 2183 2208
Email: robinchang@leeandli.com
URL: www.leeandli.com

Robin Chang is a partner at Lee and Li and the head of the firm's banking practice group. His practice focuses on fintech services and regulatory issues, banking, IPO, capital markets, mergers and acquisitions, project financing, financial consumer protection law, personal data protection law, securitisation and antitrust law.

Mr. Chang advises major international commercial banks and investment banks on their operations in Taiwan. He successfully assisted the listing of some foreign companies in Taiwan. He is also involved in many M&A transactions of financial institutions in the Taiwan market.



K. J. Li

Lee and Li, Attorneys-at-Law
9F, 201 Tun Hua N. Road
Taipei 10508
Taiwan

Tel: +886 2 2715 3300 / 2173
Email: lkj@leeandli.com
URL: www.leeandli.com

K. J. Li is a senior attorney in the Banking and Capital Markets Department of Lee and Li. Mr. Li advises financial institutions on regulatory compliance issues, applications and permits, syndicated loans and the drafting and review of relevant transaction documents for relevant businesses. He also has extensive experience in mergers and acquisitions, disposal of non-performing loans by financial institutions, IPOs and drafting bills (such as E-Payment-related regulations and P2P Self-Regulation Guidelines).



As one of the most dedicated legal teams in Taiwan and the largest law firm in Taiwan, we provide a wide range of professional services to fintech service companies, leading domestic and international banks, securities firms, insurance companies and other financial institutions as well as a significant number of corporate clients across different industries. To provide regulatory compliance advice and services to our clients in finance-related industries, we usually work closely with our clients to complete projects in compliance with existing as well as newly issued or amended regulations. Our practice covers fintech services and regulatory issues, syndicated lending, project financing, aircraft financing, ship financing, derivatives, factoring, distressed assets management, consumer banking and regulatory compliance. We have advised on many major transactions such as project finance transactions for power plants, high speed railway and mass rapid transportation systems, the first distressed asset sale, the first merger deal under the Financial Institutions Merger Act, and the establishment of financial holding companies.

Thailand



Dr. Jason Corbett



Don Sornumpol

Silk Legal Co., Ltd.

1 The Fintech Landscape

- 1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).**

Thailand is a comparatively advanced jurisdiction for fintech in relation to many of its peer nations in Southeast Asia and elsewhere in the Asia-Pacific. Banks and other established institutions offer mobile banking, mobile payments, and similar retail applications. Electronic payment methods have become popular and widespread in the country, with one recent estimate predicting Thai users to triple the number of e-payment transactions to 150 *per annum*.

Peer-to-peer lending is an early-stage development in Thailand, with the government recently announcing regulatory legislation in September 2018 that became effective in January 2019. The new legislation grants shared regulatory authority to the Thai Securities and Exchange Commission (SEC) and the nation's central bank, the Bank of Thailand (BOT). Active peer-to-peer lending participants include PeerPower and Beehive Asia.

Fintech applications for remittances are also common, both inbound and outbound. One such offering, DeeMoney, offers currency exchange and international money transfer services by means of their mobile app.

Digital assets and cryptocurrencies are beginning to be regulated by official bodies, a process that has accelerated since the passage of the Royal Decree on Digital Asset Businesses and recent amendments to Thailand's Securities and Exchange Act permitting securities issuance via blockchain technology.

- 1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?**

Under the Royal Decree on Digital Asset Businesses, "digital asset businesses" are not permitted to operate without a licence. "Digital asset businesses" are defined under the Decree as brokers, dealers, or exchanges for digital assets or cryptocurrencies. Additionally, ICO portals, which function as platforms for the consummation of initial coin offerings, fall within the definition. The use of cryptocurrencies to purchase and sell goods, however, is legal. (For more information on the Decree and its provisions, see question 3.1 below.)

Pursuant to the Payment System Act (2017), electronic payment services also may not operate without a Licence to Operate a Designated Payment Service. Depending on the kind of payment service, the requirements for this licence vary significantly, with capital requirements generally of between THB 10 million and THB 100 million.

2 Funding For Fintech

- 2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?**

Seed and early-stage financing are generally available from angel investors, investment clubs, and accelerators and incubators. In 2018, startup funding was led by Omise, 2C2P, and Jitta, with \$45 million, \$18 million, and \$6.5 million in funds raised respectively.

Venture capital is also available from local funds, with Thai VC firms raising over \$300 million in 2017, and also neighbouring countries, with Singapore serving as an important hub of VC financing. Notable firms include Tencent, Singha Ventures, Rakuten Capital, Jungle Ventures, Golden Gate Ventures, Sequoia Capital, Monk's Hill Ventures, and 500 Startups/500 TukTuks.

Equity crowdfunding campaigns and services are an additional method for fundraising; one local application offering crowdfunding campaigns is Asiola. The SEC has offered exemptions from registration requirements for equity crowdfunding up to THB 40 million, with a THB 20 million limit during the first year and a THB 50,000 cap per retail investor.

Large corporate banks also have introduced corporate venture capital as a source of financing; examples are Digital Ventures, by Siam Commercial Bank; and Beacon Capitol, by Kasikorn Bank.

- 2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?**

Thailand's Board of Investment (BOI) offers tax and non-tax incentives to firms in targeted industries, which the government as a matter of policy has chosen to promote. Category 5.9 (Digital Services) of the BOI's promoted industries includes fintech companies. In order to qualify for BOI promotion, a company in this category must hire digital specialists and have capital investment

(excluding the cost of land and working capital) equal to or greater than THB 1 million (approximately £24,000).

Additionally, Category 5.7 of the BOI's promoted industries offers incentives for software companies, which allows fintech enterprises to open back office locations in support of their offshore locations. To qualify for Category 5.7, companies must employ developers or other IT personnel with total salaries of THB 1.5 million annually.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

In order to complete an IPO in Thailand, a company must apply for IPO approval from the SEC as well as listing approval from the Stock Exchange of Thailand (SET).

To be approved for an IPO, a Thai company must appoint a financial advisor who has been qualified by the SEC, conduct a year-long diligence process, legally convert from a private to a public limited company, file an application with a registration statement and draft prospectus for the offering, and either obtain an underwriter's licence or engage a licensed underwriter to distribute shares.

The SET imposes certain quantitative requirements on companies seeking to be listed, as well. These include: thresholds of THB 300 million in paid-up shareholder equity (after giving effect to the IPO); three years of operational history, including one consecutive year with the same management at the time of the IPO; economic performance targets of THB 30 million in profits over the last year prior to the IPO; and a THB 50 million profit over a period of either two or three years prior.

Additional and different criteria are applied to infrastructure firms, holding companies, and foreign companies seeking to list in Thailand. Thailand also maintains a Market for Alternative Investment for smaller issuers.

We anticipate exit strategies for Thailand fintech to continue to be limited *vis-à-vis* traditional companies. Thailand's non-competitive regulatory burdens are likely to keep local IPOs from becoming a viable strategy, as firms are likelier to seek listing on foreign exchanges such as Singapore or Nasdaq.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

There have been no events of this kind within the fintech sector in Thailand. Fintech companies have succeeded in raising seed and early-round financing, but none have reached an exit event as of yet.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

The National Legislative Assembly of Thailand is currently considering the Draft Promotion of Financial Technology Business Bill. Should the Draft Bill be promulgated, it will regulate business that is conducted electronically and is related to the following actors:

1. Financial institutions.
2. Specialised Financial Institutions (SFIs).
3. Businesses supervised by the SEC.

4. Life insurance companies and life insurance brokers.
5. Casualty insurance companies and casualty insurance brokers.
6. Electronic payment businesses.
7. Businesses authorised to operate in a regulatory sandbox.

In the meantime, fintech businesses are regulated under general laws that apply to the above actors. Fintech businesses that are currently regulated under Thai law are:

- Electronic payment services, which are regulated under the Payment Systems Act of 2017.
- Peer-to-peer lending platforms, which are regulated under Section 5 of the Announcement of the Revolutionary Council No. 58.
- Digital asset businesses, which are regulated by the Royal Decree on Digital Asset Businesses of 2018.

As of 2019, the Office of Insurance Commission has proposed the drafts to current legislation governing the insurance industry in order to allow InsurTech businesses to be specifically regulated in Thailand. Guidance is still expected, but Thailand's political cycle is likely to keep this process on hold until the election results are finalised.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

In Thailand, crypto-based assets are specifically regulated by the Royal Decree on Digital Asset Businesses of 2018. The Royal Decree requires that businesses that deal in digital assets, including cryptocurrency, acquire authorisation from the SEC. Accordingly, the SEC has issued a series of subordinate legislation that further regulates crypto-based assets under the Royal Decree – the most significant of which are as follows:

- SEC Notification No. GJ. 10/2561 Re: Exemption of Certain Digital Token Offerings from Provisions Relating to Public Offering of Digital Tokens. issued on 7 June 2018.
 - This notification exempts “utility tokens” from regulation.
- SEC Notification No. GJ. 12/2561 Re: Designation of Additional Digital Tokens. issued on 7 June 2018.
 - This notification subjects to regulation cryptocurrencies issued for the purpose of raising funds from the public, and that specify rights of investors to participate in investment projects and/or rights to acquire goods and/services.
- SEC Notification No. GJ. 15/2561 Re: Public Offering of Digital Tokens.
 - This notification is quite significant since it defines the law in Thailand with regards to how initial coin offerings (ICOs) may be conducted.
- SEC Notification No. GJ. 16/2561 Re: Approval of Service Providers of Digital Token Offering.
 - Thai legislation requires that ICOs be conducted through an approved “ICO portal”, whereby the authorisation of such ICO portals is specified in this notification.
- Notification of the Capital Markets Supervisory Board No. SJ 44/2561, issued on 11 September 2018.
 - This notification initially gave official recognition to seven specified cryptocurrencies as media of exchange for a digital asset business. Pursuant to the subsequent SEC Notification No. SJ 12/2562 (No. 2), issued on 12 February 2019, that was decreased to four cryptocurrencies, *viz.* Bitcoin (BTC), Ethereum (ETH), Ripple (XRP), and Stellar (XLM).

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

Generally, the Thai government is supportive of financial technology as a means to further the "Thailand 4.0" policy. Under the stated policy, Thailand seeks to overcome the "middle income trap" by adopting a new economic model.

The SEC has recently proposed draft amendments to the Securities and Exchange Act of 1992 that will allow it to exempt certain securities business from regulations. Such amendments will allow the SEC to provide a regulatory sandbox for fintech businesses to offer goods and services that utilise new technology or innovations in a limited scope without being subject to normal licensing conditions. The proposed amendments are still subject to approval of the National Legislative Assembly.

On the other hand, the BOT had issued guidelines in late 2016 providing a framework for financial institutions to test goods and services utilising new technology and innovations in a regulatory sandbox for a period of six to 12 months before potentially being offered to the general public. In December 2017, three Thai banks were permitted to offer QR code payment services after such a sandbox trial. According to BOT guidelines, the regulatory sandbox is open to new technology or innovations that are in the field of lending services or payment services, or services that are similar to the aforementioned services. The BOT is also able to allow other types of services in the regulatory sandbox on an *ad hoc* basis.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

Financial service providers that are categorised as "financial institutions" under the Financial Institutions Business Act of 1992 must be authorised and supervised by the BOT. Specific fintech services, such as electronic payment services, have separate licensing requirements. Depending on the situation, a fintech business such as an electronic payment service provider may also be restricted under the Foreign Business Act of 1999, whereby foreign investment is limited to 49% or may be exceeded if an exemption applies, *i.e.* where a foreign company has obtained a licence.

Under current legislation, insurance companies located abroad are absolutely restricted from soliciting new customers in Thailand unless they either do so through a licensed Thai-based insurance company, or through their own licensed branch office in Thailand.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

At the time of writing, the National Legislative Assembly of Thailand has approved the final draft of the Personal Data

Protection Act ("the PDPA"), which would be the general law in this jurisdiction that regulates the collection, use, and transmission of personal data. It is expected that the PDPA will receive Royal Endorsement and become enforceable law before the end of 2019.

In the meantime, financial institutions in Thailand are subject to a separate data protection regime implemented by the Bank of Thailand pursuant to the Financial Institutions Business Act of 2008.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

Yes. The PDPA will have extraterritorial effect if a data controller or data processor based in an overseas jurisdiction offers goods and services to any data owner in Thailand, or if a data controller or data processor monitors activities of any data owners in Thailand. Accordingly, overseas businesses that intend to do business with Thai customers are required to appoint a local representative in Thailand. Furthermore, international transfers of data will be strictly prohibited if the target country does not have an adequate level of data protection regulations. There are exemptions applicable in certain cases, such as where the data owner has provided informed consent, or where such transfer is mandated by law, or in order to fulfil a contractual obligation.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

The PDPA will impose criminal and administrative penalties for any violations. The severity of criminal penalties, depending on the nature of the offence, will range from between six months to one year per violation and/or fines of THB 500,000 to THB 1 million per violation. As for administrative penalties, fines of around THB 1 million to THB 4 million may be imposed depending on the nature of the offence.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

At the time of writing, the National Legislative Assembly of Thailand approved the Draft Cyber Security Act ("Cyber Security Act"). The Cyber Security Act grants government officials a wide range of authority to investigate and prevent possible cyber security threats in the following areas:

- National Security.
- Public services.
- Finance and banking.
- Information technology and communications.
- Transportation and logistics.
- Energy and public utilities.
- Public health.
- Other areas as specified by the Board of National Cyber Security.

The Cyber Security Act was subject to much controversy and public debate in the preceding years due to concerns that it gave authority to government officials to investigate personal data without a court warrant. The revised draft that has been approved by the National Legislative Assembly, however, requires that in urgent circumstances only, government officials must act on probable cause, obtain approval of the Board of National Cyber Security, to inform the courts of the search as soon as possible after it has been conducted.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

Financial institutions are required to keep records of customer identification and transactions pursuant to the Anti-Money Laundering Act of 1999. Furthermore, financial institutions have reporting requirements under the Counter-Financing of Terrorism and Dissemination of Weapons of Mass Destruction Act of 2016. Thailand is party to several international treaties and conventions on fighting financial crimes, such as the UN Convention against Transnational Organized Crime (the Palermo Convention) and the UN Convention against Corruption (the Merida Convention). Thailand is not a member of the FATF but belongs to its sub-organisation, the Asia/Pacific Group on Money Laundering.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

As stated above, the rules and regulations that govern different fintech businesses are scattered about different sources of law in Thailand. Electronic payment service providers are subject specifically to the Payment Systems Act; peer-to-peer lending platforms are subject to their own specific regulatory regime under the BOT; while digital asset businesses are subject to the series of subordinate legislation issued under the Royal Decree.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

The hiring and dismissal of employees in Thailand is governed by the Civil and Commercial Code, as well as the Labour Protection Act of 1998 (LPA). Dismissal may be with or without cause, but employees are entitled to notice of at least one pay period and statutory severance payments. Employment is further subject to general labour laws and regulations.

5.2 What, if any, mandatory employment benefits must be provided to staff?

The Social Security Act of 1990 requires the government, an employer, and an employee to make equal contributions on behalf of the employee for benefits relating to injury, sickness, invalidity, death, maternity, child benefits, old age benefits, and unemployment benefits. The rate of contributions is as prescribed by regulations of the Ministry of Labour.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

According to an order issued by the Royal Thai Police on 30 June 2014, a foreign national may enter Thailand for the purposes of employment if:

- he or she has already obtained a non-immigrant visa from a Royal Thai Embassy or Royal Thai Consulate;
- he or she must be paid a minimum amount of salary, ranging from THB 35,000 to THB 50,000 per month, depending on his/her nationality, as specified by the Royal Thai Police;
- the employer must have a paid-up capital of at least THB 2 million per foreign employee;
- the employer must have filed audited financial statements for the previous two accounting years, whereby such statements must indicate that the employer is engaged in actual business operations and is financially stable;
- the employer must have an actual necessity to employ a foreign national; and
- the employer must not employ foreign nationals in a ratio that exceeds four Thai nationals to one foreign national.

However, to any business promoted by the BOI in accordance with the Investment Promotion Act of 1977, including fintech businesses, the BOI is authorised to grant some relief from these restrictions, such as by lowering the required share capital or Thai-to-foreign worker ratio if the fintech business will hire foreign experts and/or technical specialists. Any such benefits and privileges granted shall be at the discretion of the BOI upon review and approval of the business plan of the fintech company.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

According to the Patent Act of 1979 (Patent Act), the Director-General of the Department of Intellectual Property is authorised to issue patents in order to protect an invention or design. In order to be eligible, an invention must be new, involve an “inventive step” and must be industrially applicable. As for designs, a design is patentable if it is a “new design for industry, including handicrafts”. The owner of a patent is granted various exclusive rights to exploit their patent, such as the right to use or sell the invention, etc. A person who infringes the exclusive patent rights of a patent owner is subject to a fine and/or imprisonment, depending on the nature and severity of the infringement.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Generally, Thai legislation recognises ownership in all manner of IP, including patents, copyright, trademarks, trade secrets, etc. However, with regards to IP rights related to technology specifically, a patent owner in Thailand is granted a patent for a term of 20 years from the date of the application (not the date of issuance). Nevertheless, if any court proceedings delayed the issuance of the patent, then the length of time required to resolve any such proceedings would not be included within the 20-year term. As stated earlier, an owner of a Thai patent is granted exclusive rights to exploit his invention or design; furthermore, the patent owner may freely license or assign his patent to a third-party and receive royalties. A patent owner is also required to pay an annual fee starting from the fifth year of the patent whereby the annual fee adjusts upwards per each year from THB 1,000 to THB 25,000. The patent owner also has the option of paying the entire fee for the full 20-year term at once in the amount of THB 140,000.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

Only local/national rights are enforceable as far as patents are concerned. Nevertheless, claims for damages arising under international IP agreements, such as licensing agreements, or claims related to IP in general, are within the jurisdiction of the Central Intellectual Property and International Trade Court.



Dr. Jason Corbett

Silk Legal Co., Ltd.
RSU Tower, Suite 805
571 Sukhumvit Road (Soi 31)
North Khlongton, Watthana
Bangkok 10110
Thailand

Tel: +66 02 107 2007 ext. 310
Email: jason@silklegal.com
URL: www.silklegal.com/th

Dr. Corbett is the founder and Managing Partner of Silk Legal, a Bangkok-based law firm that advises both foreign and domestic clients. A corporate lawyer by trade, and an entrepreneur at heart, Dr. Corbett has trained in law with a variety of in-house and private practice positions, including one of Canada's largest law firms. He has been involved in several business and start-ups at an executive level in a variety of industries, ranging from law, finance, FMCGs, hospitality, environmental, e-commerce and professional consulting.

Dr. Corbett is truly passionate about his work and is always eager to connect with others: "I enjoy helping to create and sustain businesses with experienced advice, financial support and mentorship".

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

Section 36 of the Patent Act provides that where the patent has been granted in respect to a product, the patent owner shall have the exclusive rights, with regards to the "patented product", to "produce, use, sell, have in possession for sale, offer for sale or import...into the Kingdom". Furthermore, a patent owner is granted the same rights with regards to a product produced by a process where the patent was granted with regards to the process. Furthermore, as stated earlier, the patent owner may grant a licence to exploit his exclusive rights or assign the patent to another person.



Don Sornumpol

Silk Legal Co., Ltd.
RSU Tower, Suite 805
571 Sukhumvit Road (Soi 31)
North Khlongton, Watthana
Bangkok 10110
Thailand

Tel: +66 02 107 2007 ext. 312
Email: don@silklegal.com
URL: www.silklegal.com/th

Don is a lawyer admitted to the New York State Bar who has been practising in Thailand since 2012. His main areas of practice include corporate and commercial transactions, foreign direct investment, investment promotion law, real estate transactions, industrial estate law, factory law, as well as immigration law. His experience includes advising foreign companies and entrepreneurs with establishing businesses under the Thai-U.S. Treaty of Amity, applying for Foreign Business Licences, as well as acquiring land in industrial estates and free-trade zones for the purposes of establishing factories and other industrial-scale operations.



SILK LEGAL

Silk Legal Co., Ltd. is a law firm based in Bangkok, Thailand that specialises in regulations surrounding business, technology, and blockchain. Our dynamic team of proficient and experienced lawyers has deep experience solving a wide range of challenges, in a variety of different practices. Our first goal is to always help our clients succeed in their business. This became the leading factor in the conception of our firm. The law is our toolbox for making that vision a reality. Silk Legal has centred around exceptional service to clients who wish to expand their businesses in the Kingdom of Thailand. Silk Legal assists our local and international clients to achieve the height of their ambition through our dedicated service, legal expertise, and a clear view of what counts – our clients' success.

Turkey

Nihat Erciyas



Erciyas Law Office

Miraç Arda Erciyas



1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

It is possible to classify the applications that have been carried out in the field of financial technology, which is developing and expanding rapidly today, under two main sections. The first section consists of fintech applications that are performed by banks, and the second section consists of fintech activities that are performed by electronic money and payment organisations other than banks. Door payments, national and international money transfers, loyalty-based cashback programmes and electronic money applications are the leading and most popular applications, as well as conventional fintech applications like payment service providers, points of sale, and bill payments, especially in recent years in Turkey. On the other hand, peer-to-peer lending or investment activities are carried out only by the organisations which provide loans (banks, factoring, leasing, etc.) in Turkey, as they are considered to be ‘crediting’ activities; certificates of incorporation and activity are basically subject to Banking Law No. 5411, and the licence to be received from the Banking Regulation and Supervision Agency (BRSA) pursuant to the relative legislation. Blockchain technology is planned by the banks, and at this point some impossibilities will occur considering the fact that the banking sector in Turkey is audited by the BRSA in terms of technological content.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

Realisation of the financial services in the Turkish Legal System is possible only under the supervision of the BRSA. All institutions which will provide financial services within this framework shall obtain the certificate of activity from the BRSA in accordance with the relative legislation. Therefore, the execution of a financial service of which the equivalent is not available in the Turkish Legal System is not possible. For example, a cryptocurrency-based financial facility should be evaluated within the framework of the Law on the Payment Services and Electronic Money No. 6493, as the single relevant legislation hereof. In this regard, it does not seem

possible to offer a cryptocurrency-based financial facility, since servers of the electronic money organisations are available in Turkey and they are audited by the BRSA.

In addition, the Law on the Prevention of Laundering of Crime Revenues No. 5549 and sub-regulations thereof has made an investigation into money resources, subject to each financial facility, obligatory for the concerned obligors within the framework of certain rules. Therefore, all cryptocurrency-based financial facilities and activities including Bitcoin are likely to be considered among the assets which are defined in the law as not suitable for the nature of cryptocurrency, and the sources of which are illegal. But at present, the attitude of the government is likely to change in a positive way.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

A special financing model has not been regulated for companies which will be active in the fintech area, the Turkish Legal System, other than the conventional financing methods. Equity and debt loan financing options that are available all over the world are also available in Turkey. In addition to this, company shareholders can capitalise the monies, receivables, negotiable instruments and shares of the capital companies, intellectual property rights, movables and all kinds of immovables, right of utilisation and use on movable and immovable properties, personal effort, commercial standing, commercial enterprises, transferable electronic media that are utilised properly, values such as fields, names and signs, mining licences and such other rights having an economic value, and all kinds of values that can be transferred and utilised in cash, in accordance with the general provisions contained in the Turkish Commercial Code No. 6102. Notwithstanding that, the minimum capital requirements, paid in different amounts depending on the activity types, in terms of the companies of which the establishment and activities are subject to stricter conditions (in other words, which are incorporated under the BRSA), have been regulated. For example: 5 million TRY for the establishment of e-money or payment system companies; 10 million TRY for the establishment of asset management companies; 30 million TRY for banks; and at least 20 million TRY for factoring firms.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

There are no special subsidies for the investments made in the fintech area, the Turkish Legal System. However, the following general incentives can be applied to the investments made in the field of fintech or the companies which will be established to operate in this area.

For example, a certain number of tax incentives and exemptions have been applied to companies established in the Technology Development Zones, namely Technoparks that are founded in collaboration with the universities, research institutions, organisations and production sectors under the Law on the Technology Development Zones No. 4691.

As a matter of fact, technology/fintech companies which are very intensely integrated with the relevant technology will particularly be able to benefit from these incentives and exemptions.

Also, earnings of the venture capital investment funds or partnerships which are incorporated in Turkey under the regulation in Article 5 of the Corporation Tax No. 5520 have been exempted from the corporation tax.

Pursuant to the Stamp Tax Law No. 488, the agreements which are regulated with regard to the exclusive venture funds of the venture capital investment trusts and venture capital investments funds, and other papers issued for these agreements, have been exempted from the stamp tax.

Monies that are obtained by transactions made in the venture capital investment funds and the venture capital investment associations, pursuant to the Law on Expenditure Taxes No. 6802, are exempted from the bank and insurance transactions tax. Furthermore, transactions within the scope of the Banking and Insurance Transaction Tax are exempted from VAT.

All of the income obtained from the Venture Capital Investment Fund participation shares by the full and limited taxpayer real persons are subjected to a 10% withholding tax within the scope of paragraph (1), Provisional Article 67. The revenues obtained from the participation shares of all the funds mentioned above are taxed at 0% for both the full taxpayers and limited taxpayer corporations, pursuant to paragraph (1), Provisional Article 67.

The tech/fintech investment partnerships and the companies that operate in this area can benefit from all of these tax incentives and discounts.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

Although special conditions have not been brought in terms of the companies and partnerships which operate in the fintech area to take the companies public in Turkey, general provisions which are regulated in Capital Market Law No. 6362 shall also be valid for them. Accordingly, the companies that will go public and apply to the Capital Markets Board and Borsa Istanbul should:

- be joint stock companies;
- establish a working group consisting of mid-level managers, financial officers and public relations officers who will prepare the application procedures;
- execute an intermediary agreement with one of the intermediary firms which is entitled to go public and is authorised by the Capital Markets Board (CMB) on the webpage of the Board;

- enter into a Market Consultancy Agreement with a market advisor in order to carry out the necessary preparations, if planning to trade in the Emerging Companies Market (ECM), for which the minimum requirements are set by the Stock Market;
- prepare their financial statements in accordance with the Capital Market Legislation, and sign audit agreements by selecting one of the independent audit firms who are authorised by the CMB and have their financial statements audited by this independent audit company;
- amend the articles of association pursuant to the Capital Market Legislation; and
- determine the public offering prices and prepare necessary papers for public offering.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

In 2014, a share of Paybyme was purchased by the Malaysian MOLGlobal company with 9.3 million dollars, at a rate of 51%.

In 2015, a 25% share of hepsiburada.com (one of the popular e-commerce sites) was acquired by the Dubai-based Abraaj Group.

According to the news published in 2016, the Banking Regulation and Supervision Agency rejected Paypal's application for a certificate of activity on the grounds that all of the company servers are not available in Turkey pursuant to the relative regulations, and in turn, the company has announced to their customers on the website that the operations to obtain its necessary permits will continue against this decision to stop the company's activities in Turkey.

A 7% share of gittigidiyor.com – one of the popular e-commerce sites in 2016 – was purchased by eBay in exchange for 34.3 million USD.

In the same year, a 50% share of the local Ininal payment and electronic money company was purchased by Multinet, which is affiliated to the French Up Group.

In 2018, a 75% share of trendyol.com (one of the most popular e-commerce sites) was acquired by Alibaba in exchange for 728 million USD.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

All the banks that wish to operate in the fintech area, including online banking and non-bank institutions of electronic money and payment services, should be established to conform with the European Union Law legislation, and other regulations, particularly Banking Law No. 5411, Payment and Instrument Consensus Systems No. 6493, the Law on the Payment Services and Electronic Money Institutions, and the Law on Prevention of Laundering of Crime Revenues No. 5549; they shall make an application to the BRSA and T.R. Central Bank in order to obtain permits thereof.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

Even if access to cryptocurrencies has been growing rapidly over the last five years, there is no clear legislation specifically directed to these operations yet in Turkish jurisdiction. Cryptocurrency is

not accepted as electronic money or a payment instrument and it is also not defined as money either, so there is no definition and regulation in Turkish law.

In 2013, the BRSA issued a press statement and remarked that because of the possibility of illegal usage, suspicious transmission and overly volatile market value of cryptocurrencies, they should be used more circumspectly. In 2017, the Turkish Central Bank stated that cryptocurrencies and cryptoassets definitely contribute to financial stability, and in 2018, the Undersecretariat for the Treasury indicated that a legislation process is needed for cryptocurrencies. Even if the Turkish government stands as an observer for cryptocurrencies nowadays, the usage of it is severely restricted in the border of, especially, AML (Anti-Money Laundering), KYC (Know Your Customer) and other legal regulations. More than 50 companies accepted bitcoin as a payment method and most people use cryptocurrencies as an investment tool, and this trend will continue to grow. Up to today, no sanctions have been imposed on cryptocurrency and cryptoasset transactions. Although cryptocurrencies tend to spread, there is also no specific taxation procedure, method or definition in tax law. General provisions of the Turkish Code of Obligations might be used comparatively for cryptocurrencies and cryptoassets. We believe that the useful aspects of cryptocurrencies and cryptoassets and global improvements will help the government to legislate subjects in a positive way.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

Financial regulators such as the BRSA and T.R. Central Bank are receptive to changes in the technology and finance sector of Turkey to keep the sector alive, and provide circulation and keep pace with the rapidly developing and changing innovations of the world and global technology. Indeed, the presence of the government incentives abovementioned and the T.R. Prime Ministry Investment Support and Promotion Agency, and compliance of all legislation regarding this area with EU legislation, even though Turkey is not an EU country, indicate that the regulators are receptive in this area. Thus, receptiveness of the institutions and organisations facilitates entering into the market as well as new initiatives in the country.

"Regulatory sandbox" options for fintechs are definitely important in order to become a nerve centre in a certain sector. These options, which are provided by regulatory agencies, create a space for fintech companies to experience their new business models, even if there is no legal base. Also, companies may test their new business model and decide its feasibility before turning themselves into international hubs. This is a very effective method for adapting international markets with the fastest and most effective ways, but unfortunately there are no "regulatory sandbox" options in the Turkish jurisdiction as of yet. However, with the incentive activities of the government, Turkey and especially Istanbul has a vision of becoming a leading centre of finance within 10 years, especially in retail banking and e-commerce. Regulation is a critical indicator in becoming an international fintech hub, so we expect that the government will take action in order to rapidly rise in the world fintech ecosystem.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

We cannot say that cross-border operations are easy in Turkey, owing to the fact that these operations are difficult in all countries due to the difference in legal systems of the countries in a general sense. However, it is possible to examine the difficulties that businesses which are established outside our jurisdiction, which will be active in the fintech area, will encounter as they act to carry on business in Turkey under two main sections. The first section is the requirement for companies, without exception for domestic or foreign companies, pursuant to the relative legislation and regulations (which will be active in the fintech area) to obtain a licence from the BRSA and permits from T.R. Central Bank; and the other section is taxation. Collaborations with the licensed companies or banks already operating in Turkey can be proposed as solutions to overcome the requirements that must be fulfilled to be active by establishing a company from scratch.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

Today, developments such as the increase in the use of electronic devices along with the development in technology, and more adaptation of the transactions completed via online media to daily life, have brought about several cybersecurity problems. One of the recent studies carried out by the regulators in Turkey in order to prevent these cybersecurity problems is the Law on Personal Data Protection No. 6698 which recently came into force on April 7, 2016. The Law also regulates the imprisonment and judicial fines that will be imposed on those who act against the Law, as well as the rules for processing, using and transferring the personal data in the Law. As a matter of fact, this Law is also applied to fintech activities which are closely related to technology, and how personal data of customers should be processed, used and transferred in compliance with the law. Fintech activities should also be carried out taking into account the fact that the rights to compensate customers for damages arising from the processing, using or transferring of data may occur in accordance with the Turkish Code of Obligations.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

The general rule for carrying out transactions, such as processing and transferring personal data in accordance with the provisions in Law No. 6698 on Personal Data Protection, is to obtain the express consent of the concerned person without discriminating between the domestic and the foreign. Transferring the data of the concerned person abroad is prohibited without the express consent of the concerned persons, other than in cases requiring the obtaining of a permit from the Personal Data Protection Board, according to the regulation as set forth in Article 9 of Law No. 6698.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

In Articles 17 and 18 of Law No. 6698 on Personal Data Protection, several imprisonment and judicial fines to be imposed on those who act against the Law are regulated. In the relevant Articles, those who record personal data in contradiction with the Law, referring to Turkish Penal Code No. 5237, were sentenced to imprisonment from six months to three years; those who disclose or capture data in contradiction with the Law were sentenced to imprisonment from one to four years; and those who fail to fulfil liabilities given in the Law and act in contradiction with the Board decisions were given an administrative fine of a minimum of 5,000 TRY and a maximum of 1 million TRY.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

In Turkish law, there are some regulations that should be implemented in the fintech area that are related to cybersecurity and technology:

- Article 243 of the Turkish Penal Code No. 5237 regulates the imprisonment and punitive fines that will be imposed on those who commit cyber crime, such as breaking into the information system, blocking the system, deteriorating the system, destroying or changing data, and abusing bank or credit cards.
- Regulations given in the Electronic Communication Law No. 5809 and the provisions regarding imprisonment and the punitive fines that will be imposed on those who offer electronic communication service in contradiction with the law.
- Provisions regarding judicial fines and sanctions in regards to combatting the certain crimes committed on internet media through content, hosting service and access providers, as specified in the Law on Regulation of Publications on the Internet and Suppression of Crimes Committed by means of such Publications No. 5651.
- Regulations in the Law on Regulation of Electronic Commerce No. 6563 and the provisions concerning the judicial fines to be imposed on those who act in contradiction of the regulations and law.
- Regulations in the Law on Preparation and Implementation of the Technical Legislation No. 4703 and the regulations pertaining to the judicial fines to be imposed on those who act in violation of the law, as well as Banking Law No. 5411 and Consumer Law No. 6502 are examples thereof.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

The money-laundering crime concerning bank and non-bank companies which are active in the fintech area is regulated by Article 282 of the Turkish Penal Code No. 5237, as “exporting abroad the asset values obtained from a crime necessitating a minimum of six months or longer imprisonment, or concealing the illegal source of these values or exposing them to various operations in order to give the impression that these assets were obtained by legal means, purchasing, accepting, keeping or using these assets while knowing the nature of their origin”.

However, the crimes related to terrorism and terrorism financing that are covered by Law No. 6415 – the crime of acting against the notification liability in case of any doubt or issue, which requires individuals to suspect assets transacted by those who provide and use banking, lending or other financial facilities in Law No. 5549 by illegal means, and other financial crimes as set forth in Banking Law No. 5411 – can be given as examples of crimes that are related to banks and other companies which operate in the fintech area.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

The Consumer Law No. 6502, Electronic Communications Law No. 5809, the Law on Regulation of Publications on the Internet and Suppression of Crimes Committed by means of such Publications No. 5651, the Law on Regulation of Electronic Commerce No. 6563, the Law on Preparing and Implementing the Technical Legislation on Products No. 4703, Capital Markets Law No. 6362, General Communiqué No. 5 of the Financial Crimes Investigation Board, and the Regulation on Distance Contracts are the other regulations that must be considered in the management of activities in the field of fintech.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

There are no other special arrangements that should be considered in this field other than the arrangements included in Labor Law No. 4857, which is applied to all relationships between employers and employees in all fields in the Turkish legal system, and which regulates the rights and responsibilities of employees who are employed on the basis of an employment agreement as executed in the Law.

5.2 What, if any, mandatory employment benefits must be provided to staff?

There is not a specific regulation for this area other than the detailed arrangements given in Labor Law No. 4857. In the Labor Law, there are regulations that employers must comply with: mandatory minimum wage; health insurance; workplace safety; maximum working hours; severance; and notice payments.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

In addition to the general procedures that will be implemented, such as residence permits and work permits of foreigners pursuant to International Labor Law No. 6735 and the Law on Work Permits of Foreigners No. 4817, the BRSA carries out detailed research about the shareholders of organisations who are subject to a licence and permit, such as bank, factoring, leasing, electronic money and payment organisations.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Turkey is a Member State of many agreements, such as the Patent Cooperation Treaty (PCT), European Patent Convention (EPC), and the Strasbourg Convention regarding International Classification of Patents, and it has mostly adapted its own domestic law in accordance with these agreements. It is important to note that the EPC is directly applicable in Turkey in terms of European patents. On the other hand, the national law on the protection of IP Rights is the Industrial Property Law No. 6769 that came in to force on January 10, 2017 (before the IP Law came into force, each IP right was protected and ruled under relevant Decree Laws). As per the IP Law, patents are granted for inventions in all fields of technology, provided that they are new, involve an inventive step and are susceptible to industrial application. Turkey also has the utility model system for so-called “small inventions”. Once an application for a patent or utility model is examined and granted by the Turkish Patent and Trademark Office (TPO) (for European Patents, the examination and grant decision of the European Patent Office (EPO) is followed and no additional examination is conducted by the TPO), a term of protection of 20 years for patents and 10 years for utility models is provided.

Until the expiry of these terms or the invalidation of the patent or utility model by the competent IP Court, the right owner is entitled to demand the prevention of the following acts:

- a) Production, sale, use or import of a product which is subject to a patent, or to keep it for any reason other than personal need for these purposes.
- b) Use of a procedure which is subject to a patent.
- c) Proposal to others to use a procedural patent, the use of which is known or should be known to be prohibited.
- d) Sale, use or import of products which are obtained directly via the procedure which is required for a patent or to keep them for any reason other than personal need for these purposes.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

The IP rights operation, particularly the examination and granting of IP rights, is conducted by the TPO. The TPO examines and sets a decision on all IP applications at a national level. In addition to that, due to the membership of Turkey to the EPC, the TPO cooperates with the EPO in terms of the European patents with which Turkey is designated.

Once an IP right is granted by the TPO (or validated in Turkey for European patents), it is nationally protected by an exclusive term. In relation to the infringement of IP rights or any dispute related to IP rights, the specialised IP Courts are the competent Courts. The specialised IP Courts are built in the big cities of Turkey such as Ankara, Istanbul and Izmir. In other cities, the Civil Court of First Instance handles IP-related matters.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

Due to the national protection principle, the IP rights should be granted at a national level before the TPO in order to protect and enforce IP rights in Turkey.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

Turning IP rights into cash by means of the conventional legal proceedings which are applied all over the world, such as the licence, transfer, purchase, or sale of the IP works, is possible in Turkey, pursuant to the international conventions, Industrial Property Law No. 6769 and the Law on Intellectual and Artistic Works No. 5846.



Nihat Erciyas

Erciyas Law Office
Oğuzlar Mahallesi 1364. Sokak
No:4 Kat:2 Balgat Çankaya
Ankara
Turkey

Tel: +90 312 905 5050
Email: nihat.erciyas@erciyas.av.tr
URL: www.erciyas.av.tr

Nihat Erciyas, one of the partners of Erciyas Law Office, graduated from Ankara University, Faculty of Law in 2002, and after completing his official law internship, went to Munich, Germany in 2003 in order to resume his education and gain experience abroad. After working in Zirngibl Langwieser Law Office in Munich for one year during 2003–2004, he decided to continue his education in Ludwig-Maximilians University during 2004–2005 and completed his Master's degree on EU and International Economics Law. After completing his Master's degree, Mr. Nihat returned to Turkey and worked at TUBITAK for a short time between 2005–2006, and he has been working in this family firm since 2007. Also, he is continuing his doctoral education at Istanbul Culture University, in Private Law. Mr. Nihat knows English and German, and he is a specialist in the fields of technology, finance and international trade.



Miraç Arda Erciyas

Erciyas Law Office
Koreşhitleri Cad. No:33/2
Esentepe Şişli
İstanbul
Turkey

Tel: +90 212 275 7538
Email: arda.erciyas@erciyas.av.tr
URL: www.erciyas.av.tr

Arda Erciyas, one of the partners of Erciyas Law Office, graduated from Ankara University, Faculty of Law in 2009, and after completing his official law internship, he went to London, England in 2010 in order to resume his education and gain experience abroad. After completing his Master's degree on the European Union at the University of Westminster in England, Mr. Arda returned to Turkey and he has been actively working in the family firm since 2011, and he is also continuing his PhD at Istanbul Commerce University, in International Trade and EU Law.

Mr. Arda knows English well and he is a specialist in the fields of technology, finance and international trade.

ERCİYAS
LAW OFFICE

www.erciyas.av.tr

Erciyas provides consultancy on official licensing of e-money companies through the Turkish Banking Regulation and Supervision Agency. Furthermore, the firm drafts customer and framework agreements with regard to products which are sold by e-money companies.

The firm also advises not only on the integration of e-money companies into international and national trade infrastructure, but also international and national security and technical certifications of e-money and electronic payment systems. The firm practises optimising goods and services of companies which operate in IT as per the new regulated Data Protection Law in Turkey, and in cooperation with business partners, the firm also provides legal services integration of artificial intelligence products into a work flow among big companies.

Moreover, the firm particularly advises e-commerce companies on the consequences of electronic agreements, the rights their customers (consumers) have in accordance with these electronic agreements, and preparing technical infrastructures, such as the diversification of payment systems of sale portals in compliance with administrative regulations.

Ukraine

Sergii Papernyk



Alexander Molotai



Evris Law Firm

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

In Ukraine, Fintech is beginning to take off with more than 60 firms at different stages of maturity. During the financial crisis of 2008–9, the first players among the Fintech startups started to appear in Ukraine. For the most part, these early Fintech initiatives focused on the area of payments and money transfers. However, the majority of Fintechs (58%) have been launched since 2015.

According to the result of a survey among Fintech companies, the “Hot Topics” for 2018 are: digital banking; automation; biometric identification; machine learning; AI; forecasting and modelling; smart contracts; chatbots; blockchain; big data; digitisation of all registries; ICOs; IT security; cybersecurity; and payment security.

Among the notable innovation trends of 2017 is the launch of the first digital bank in Ukraine – Monobank, which provides payment services, microlending and deposits for individuals via mobile application.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

There are no legislative prohibitions on providing any popular Fintech activities. However, according to the law of Ukraine, activities such as the emission of payment cards, opening an account and the emission of “electronic money” can be realised by banks only.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

In Ukraine, the most convenient types of funding for Fintech startups are private equity investments, banks or investor loans. The stock exchange marketplace or fundraising platforms are poorly developed.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

There are no special tax incentives for investment in tech/Fintech businesses in Ukraine. Nevertheless, Ukraine is a highly attractive location for investment due to the simplified tax regime, with a profit tax rate at an amount of 5% per year. In this instance, the entrepreneur does not pay Value Added Tax.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

Currently, the law provides for the requirements for IPO as to the company’s equity amount (minimum UAH 400 million), net income from sales (minimum UAH 400 million), free float of shares (minimum 10%), number of shareholders (minimum 200), corporate governance structure, and mandatory financial audit, etc. However, please note that the given requirements are about to be changed due to ongoing legal reforms.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

There have not been any recent notable exits in Ukraine.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

The main regulatory acts to be followed in Fintech are the Civil Code of Ukraine, the Law of Ukraine “On Payment Systems and Money Transfer”, the Regulation on Electronic Money in Ukraine, approved by the National Bank of Ukraine (NBU) in Resolution No. 481 of 4 November 2010, Regulations on the Procedure for Registration of Payment Systems, participants of payment systems and operators of payment infrastructure services (NBU Resolution No. 43 of 4 February 2014).

The legal and regulatory environments supporting Fintech (and other) startups are improving. The most important changes

introduced recently by the Ukrainian legislation are: authorisation to sign an invoice and/or contract with an electronic signature; the use of simplified taxation for Ukrainian IT companies; the liberalisation on repatriation of dividends (to USD 5 million per legal entity per year); active advocating for the adoption of EU directives, in particular PSD2; and the recent coming into effect of the law on electronic identification and trust services for electronic transactions in the internal market (“Electronic Trust Services Law”).

Every company which is going to render financial services must receive a special licence from the National Financial Services Commission. Services operating foreign currency as well as the company doing so will be required to obtain the licence from the NBU.

Only banks can emit payment cards and “electronic money”, and open accounts. There is a proper regulation concerning electronic signatures and this can be used with financial services. The recent Electronic Trust Services Law enabled banks to delegate the approval of identity to third parties. Therefore, Mobile ID technology is to penetrate the market with significant speed. At least one of the Ukrainian mobile operators has already announced their Mobile ID service.

Furthermore, the new law on payment systems with similar regulation to PSD2 is expected to be adopted in 2019.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

While the use of cryptocurrencies is not prohibited, it is not regulated by any legal act. According to the mutual letter issued by the NBU and the National Financial Services Commission on 30 November 2017, cryptocurrencies cannot be considered as money, electronic money, currency or securities.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

Fintech development was actively supported through recent initiatives undertaken by the NBU in 2017. The NBU approved the Comprehensive Program of the Ukrainian Financial Sector Development (Resolution No. 391 dated 18 June 2017) which includes initiatives such as a Cashless 2020 Strategy, a possibility to use the Bank ID system for remote identification, and new rules to facilitate the licensing of payment service providers.

The NBU announced the institution of a “regulatory sandbox” for Fintech startups. Nevertheless, this initiative has still not been implemented.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

According to Ukrainian legislation, every payment system to be used on the Ukrainian market must be placed in the State register of payment systems. Nevertheless, the rules for registration are quite flexible.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

The issues regarding personal data are regulated by the Law of Ukraine “On personal data protection”.

The Law requires the database owner to obtain consent of the individual for the processing of his or her personal data, including the collection, use and distribution of such personal data. The personal data cannot be distributed without permission from the data’s owner.

The authority responsible for personal data control is the Ukrainian Parliament Commissioner for Human Rights. The owner of personal data informs the Commissioner about the processing of personal data, which constitutes a special risk for the rights and freedoms of the subjects of personal data.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

According to the Law, the transfer of personal data to foreign subjects is carried out only if the appropriate State provides adequate protection of personal data. The Member States of the European Economic Area, as well as the States which have signed the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, are recognised to provide an adequate level of protection of personal data.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

Ukrainian legislation provides for administrative and criminal liability for the violation of personal data law. Not complying with the law on the protection of personal data can be considered as an administrative violation with a fine of up to UAH 17,000 (about USD 600). The illegal collecting, saving, use and spreading of personal data without the consent of the owner is a criminal offence and can entail imprisonment of up to five years.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

Cybersecurity in Ukraine is mostly viewed through the prism of State defence and security. Therefore, applicable legislation is mostly focused on cybersecurity in the State sector and includes the Law of Ukraine “On Data Protection in Information and Telecommunication Systems”, the Law of Ukraine “On Information”, the Law of Ukraine “On State Secrets”, the Law of Ukraine “On National Security of Ukraine”, and the Law of Ukraine “On State Service of Special Connection and Information Protection”. As for cybersecurity in the private sector, the above legislative acts only establish separate basics, mostly addressing matters of State security and defence.

The new Law of Ukraine “On basic principles of cybersecurity” became effective in May 2018. This Law stipulates a special

regulation for telecommunication infrastructure and for points crucial to cybersecurity. This legislative act entrusts the NBU as one of the State authorities responsible for cybersecurity control. Therefore, new regulative acts of the NBU concerning cybersecurity in the financial sphere (and Fintech) are expected.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

The relevant AML law is the Law of Ukraine on the Prevention and Counteraction to Legalisation (Laundering) of the Proceeds of Crime or Terrorist Financing. According to the Law, the AML regulators in Ukraine are: the NBU; the State Committee for the Financial Monitoring of Ukraine and National Securities; and the Stock Market Commission.

The subject of primary financial monitoring shall proceed with the classification of its clients taking into account risk criteria. Financial operations/customers are subject to financial monitoring/due diligence if the transaction amount is more than UAH 150,000 (approximately USD 5,550). Following the reforms in the currency regulation sector, the NBU announced the possible raise of the controlled transactional amount up to UAH 300,000 (approximately USD 11,000).

The requirements to verify customer identification information for individuals are: name; date of birth; personal identity document details; residential (registration) address and actual address; taxpayer identification number; and source of funds. For legal entities: full name; registration address; information about the management and controllers of the company; shareholder structure; registration number; and bank account details. Beneficial owners need to be known in all cases, but the level of requirements for identification depends on the type of transaction and risk involved.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

There are no other regulatory regimes in place in Ukraine.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

According to the Labour Code of Ukraine, the employment relationship in Ukraine is established by an employment agreement between an employer and an employee. The employment agreement contains the terms of employment, including the title of the position, a description of the work to be performed by the employee, an obligation for the employee to observe internal labour rules, an obligation for the employer to ensure adequate working conditions, and the salary amount for performance of employment duties.

In general, most agreements are concluded for an indefinite term. Even though the Ukrainian labour law enables an employer to conclude fixed-term employment agreements, these agreements should be concluded only with those employees whose work is, by nature, of a limited duration. It is also possible to enter into an employment agreement “until the completion of agreed-upon work”.

Concluding the agreement, the employer must enter the relevant record in the employee’s labour book. The probationary period cannot exceed one month for blue-collar workers or three months for other employees. Considering the complexity involved in dismissing employees under Ukrainian law, employers frequently use the probationary period as a legal and practical way to ascertain the suitability of a candidate for the position.

In Ukraine the employer is a tax agent, obliged to pay payroll taxes on behalf of his employee (18%).

Presuming the complexity involved in the tax regime of employment, many companies in Ukraine use the entrepreneur contracts instead of the labour agreements. In such a case, the employee acts as a private entrepreneur contracted with the company for some scope of the job. This framework also allows the use of the simplified tax regime with no VAT and with the 5% tax rate of the entrepreneur’s income.

5.2 What, if any, mandatory employment benefits must be provided to staff?

The length of a working week is restricted to 40 hours. The minimum salary for a full time employee is UAH 3,723 (approximately USD 140). An employee has a right to an annual, minimum 24 calendar days of vacation. There are no additional mandatory employment benefits provided.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

Non-residents have the same rights to work in Ukraine as any Ukrainian has. However, non-residents have to provide certain documentation before starting work in Ukraine. The first one is the work permit. Because Ukraine does not belong to the EU, the work permit is mandatory for both EU and non-EU citizens. After obtaining a work permit, the non-resident can apply for a residence permit, which is the second mandatory document required for employment.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Assuming that Fintech solutions are mainly represented by certain business algorithms, software embedding such algorithms, data compilations and respective hardware solutions, the following options for protecting innovations and inventions in Fintech are available in Ukraine:

- Computer code and data compilations (databases) are protected by copyright (i.e. as literary works). Patent protection of computer programs and algorithms as such is specifically excluded. However, in certain cases, software can be the subject matter of patent protection as part of the hardware solution. Business methods and algorithms (representing, basically, ideas) are not protectable.
- In certain cases, user interfaces and screens may also be protected by industrial design patents. Equally, industrial design protection is also available for hardware solutions (portable and wearable devices, original design of pieces of hardware, etc.).

- Technical methods (processes) and respective hardware may be protected by either patents for inventions or utility models. The principal difference between the two is that the latter are issued without examination (under responsibility of the applicant) and may lack inventive step as a substantial feature, whereas patents for inventions are only granted based on full examination and should have inventive step.
- Brand names, slogans, and hashtags may be protected as trademarks. Equally, trademark protection in some cases may be enjoyed by original and distinctive 3D shapes (e.g. design of wearable, handheld or portable hardware), provided that the applicant is capable of proving their distinctiveness as trademarks.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Copyright ownership in Ukraine will first be owned by the author or authors of the copyright work. Subsequently, proprietary rights in the work may be assigned by the author to a third party. Personal non-proprietary rights in works of copyright are not assignable under Ukrainian laws.

As a matter of exception, proprietary rights in works created under an employment agreement or a civil law contract will be co-owned by the employee/employer and contractor/customer, unless otherwise provided in the respective employment agreement or civil law contract.

Copyright in Ukraine is protected throughout the whole life of the author and for 70 years after the death of the author.

Patent, utility model, design and trademark protection is granted on the basis of registration.

Patents for inventions are granted on the basis of full examination of the invention by the patent office, and protect invention for 20 years from the date of filing the application.

Patents for utility models and industrial designs are granted on a declarative basis (no substantive examination is conducted) and grant protection for 10 years from the date of the respective application.

In order to maintain rights in patents (inventions, utility models and industrial designs), the patent owner is to pay annuities.

Trademark protection is granted on the basis of full examination. Trademarks are protected for 10 years from the date of filing of the respective application and may be further extended for an indefinite number of subsequent 10-year periods.

The owner of any IP subject matter has the exclusive right to (1) use such object, (2) grant the right to use such object to third parties (licence), and (3) counteract illegal use or infringement of the owner's exclusive rights.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

Copyrighted matter enjoys worldwide protection. Thus, any copyright created outside of Ukraine will be equally protected in Ukraine.

Patents for inventions, utility models and industrial designs, as well as trademarks, should be registered in Ukraine under national or international (Madrid, PCT, The Hague) procedure.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

For the purpose of the monetisation of IP, Ukrainian businesses use licence agreements. Licence agreements are not subject to mandatory registration and they enter into force on the date of execution thereof. In the meantime, in case the licensor or licensee would like to avoid any risks which may arise with regard to such an agreement, and for the purposes of informing the public on such licences, the licence agreement may be recorded with the Ukrainian Patent Office.



Sergii Papernyk

Evris Law Firm
 Vector Business Center
 52 Bohdana Khmelnytskogo St.
 Kyiv, 01030
 Ukraine

Tel: +38 044 364 9191
 Email: sp@evris.law
 URL: www.evris.law

Sergii has more than 12 years of experience with a wide range of Ukrainian and foreign banks and other financial institutions. His experience includes legal support of banking transactions, financial restructuring, and representation of clients in commercial and corporate disputes. In the last few years, Sergii has engaged in legal support for Fintech initiatives within the leading Ukrainian banks and separate startups.

Sergii is the Head of the Financial Law Committee at the Ukrainian Attorney Association, a member of the Board of the Financial Law Committee of the Ukrainian Bar Association, the President of the Arbitration Committee on Financial Restructuring, attorney-at-law and the Head of the Attorney Office "Evris".



Alexander Molotai

Evris Law Firm
 Vector Business Center
 52 Bohdana Khmelnytskogo St.
 Kyiv, 01030
 Ukraine

Tel: +38 044 364 9191
 Email: a.molotai@evris.law
 URL: www.evris.law

Alexander has over 15 years of practice in various aspects of intellectual property and unfair competition law.

His experience embraces a wide range of issues related to intellectual property rights, such as the drawing up and implementation of IP protection strategies for various types of businesses, structuring of transactions that involve IP assets (transfer and licensing of technology and goodwill), suppression of unfair business practices and litigation of IP-related disputes.

Alexander has advised clients representing a broad variety of business sectors, including financial institutions, media and advertising companies, manufacturers of consumer products, accommodation, leisure and entertainment facilities, life sciences, oil and gas, etc.

He is a member of the Ukrainian Bar Association, the International Intellectual Property Law Association (IIPLA), and the International Association for the Protection of Intellectual Property (AIPPI).

E V R
 I S •
 L A W

Evris is a Kyiv-based full-service law firm which has gathered talented and dedicated lawyers who think creatively in their systems approach to the law. The firm provides 360-degree legal advice on various matters related to corporate and M&A, banking and finance, tax, real estate, and dispute resolution.

Evris sees its mission in advocating the investment potential of Ukraine through its legal work, and demonstrating to the international community how effective business can be here when it is planned and developed with the proper legal advice.

The Fintech line of services is part of the banking and finance practice. The Evris lawyers have the legal expertise and sector insight to launch, fund and grow a Fintech business. Among others, Evris offers: legal advice on finance State regulation; negotiations with financial institutions; legal support for blockchain startups; IP protection; tax structuring; and consumer protection, etc.

United Kingdom

Rob Sumroy



Ben Kingsley



Slaughter and May

1 The Fintech Landscape

- 1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).**

London is consistently ranked as one of the most ‘fintech-friendly’ cities in the world and, as such, a broad spectrum of fintech business is represented both in London and the UK more widely. The UK was an early adopter of payments technology and this market has now reached a degree of maturity. Likewise, the sharing economy and crowdfunding are well-established in the UK.

Open Banking, an initiative led by the UK Competition and Markets Authority, was launched in January 2018, and refers to a secure set of technologies and standards that allow customers to give companies other than their bank or building society permission to access their accounts securely. Although customer uptake has been relatively low, it is expected to translate into an emerging market of new third-party online service providers.

Big Data continues to be an important area of innovation and research both for start-ups and established financial services firms. We expect that an increasing capacity to analyse and use Big Data will dovetail with the rapidly developing Internet of Things to, for example, provide financial services firms (such as insurers) more complete sources of customer data. Regtech – tools and services to automate compliance tasks – continues to gain momentum and is now considered to be an integral component of the UK financial services landscape.

The application of fintech to asset management continues to grow; in particular, in 2018 we have seen a broader range of propositions in the robo-advice market.

The discussion surrounding blockchain technology continues, with much recent dialogue focussed on the use of bitcoin and other cryptocurrencies and the related topic of Initial Coin Offerings (ICOs), which continues to attract global regulatory scrutiny. The impact of blockchain technology is moving from a phase of theory to practice as the broad range of possible use cases expected from the application of the technology is now widely recognised.

Progress of, and investment into, the UK’s fintech sector has continued since the UK voted to leave the EU, with statistics showing that total capital invested into UK fintech in 2018 comfortably exceeded 2017 levels.

- 1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?**

There are currently no prohibitions or restrictions that are specific to fintech businesses in the UK.

The UK financial regulator, the Financial Conduct Authority (FCA), is set to consult in 2019 on a potential prohibition on the sale to retail consumers of derivative products and transferable securities linked to certain cryptoassets (see further question 3.2 below).

2 Funding For Fintech

- 2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?**

The UK has mature debt and equity capital markets accessible to businesses above a certain size. For example, raising finance through an IPO has been a popular avenue for certain fintech businesses in recent years (see further our answers to questions 2.3 and 2.4 below). However, even for those fintech businesses which are not yet in a position to raise finance through these ‘traditional’ routes, there are a number of funding sources available in the UK once the resources of ‘friends, family and fools’ have been exhausted.

Equity

Early-stage venture capital funding before it is possible to put a valuation on a company is often done through a form of convertible loan note (CLN). The CLN becomes convertible into equity on the occurrence of certain events such as a material funding round, an exit or an IPO, usually at a discount to the value per share applied by such event. Investments in loan notes will not qualify for certain tax reliefs, including SEIS and EIS as described in question 2.2 below. An alternative to the CLN, structured so as to qualify for such reliefs, is the advanced subscription agreement, whereby the investor subscribes for future equity determined by reference to the relevant trigger event.

As a company matures, it will typically undergo a series of equity fundraisings (seed funding, Series A, Series B and so on).

Crowdfunding, where members of the public pool resources through an intermediating platform (typically in exchange for shares), is growing in popularity in the UK for start-up businesses. In particular, it offers private investors an opportunity to invest in early-stage

businesses which would previously have only been accessible to business angels or venture capitalists. The UK crowdfunding sector is well-established and growing in size and, as such, it is sometimes possible to raise substantial sums. The mobile bank Monzo raised £20 million in a third crowdfunding campaign in 2018, the largest ever crowdfunding round by a UK fintech company, while challenger bank Revolut raised £3.9 million in its 2017 crowdfunding round. Many fintech start-ups have combined crowdfunding finance with finance raised from more traditional sources, such as from venture capital and business angels. Incubators, which generally offer facilities and funding for start-ups in return for an equity stake, are also increasingly prevalent in the UK and may present an attractive option to small and growing fintech businesses.

Debt

Whilst small businesses are unlikely to have recourse to 'traditional' bank loans, there are more tech-focussed banks, such as Silicon Valley Bank and OakNorth Bank, which specifically provide debt finance to tech start-ups. There are also numerous peer-to-peer lending platforms and invoice financing firms operating in the UK, which provide alternative sources of debt finance to small and growing businesses.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

The UK Government offers the following tax incentives for investment in start-ups:

- The Seed Enterprise Investment Scheme (SEIS) offers a 50% income tax relief for UK taxpayers investing up to £100,000 in qualifying start-ups. A company can raise no more than £150,000 in total via SEIS investment. To qualify for SEIS, a company must (among other qualifying criteria) be no more than two years old, have assets of less than £200,000 and have fewer than 25 employees. This complements the Enterprise Investment Scheme (EIS) which offers tax relief for investment in higher-risk small companies, though the tax relief available under the EIS is less than under the SEIS.
- SME R&D tax credits of up to 230% for certain companies with fewer than 500 employees.
- The Patent Box Scheme, which allows companies to apply a lower rate of Corporation Tax to profits earned from patented inventions.

It should be noted that these incentives are not specific to the tech or fintech sectors and are generally available to qualifying companies and investors in all sectors.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

The precise conditions depend on the type of listing and the market on which the shares will be listed. A premium listing on the main market of the London Stock Exchange will, for example, entail more onerous requirements than a listing on the more junior Alternative Investment Market.

In summary, a standard listing on the main market of the London Stock Exchange would require compliance with the following key requirements:

- The company to be duly incorporated, validly existing and operating in conformity with its constitution and its shares to comply with the laws of the company's place of incorporation, duly authorised and have all necessary statutory and other consents.

- The company's shares to be freely transferable and free from any restrictions on the right of transfer.
- A minimum market capitalisation of £700,000.
- The company to publish an approved prospectus.
- The company to ensure that at least 25% of its shares are in public hands.

In contrast, to list on the Alternative Investment Market, there are no requirements in respect of the percentage of shares to be in public hands or market capitalisation and, in certain cases, no requirement for admission documents (such as the prospectus) to be pre-vetted by the market or UK regulators.

To obtain a premium listing on the London Stock Exchange, a company would need to comply with requirements additional to the standard listing requirements above, such as supplying three years of audited financial accounts and demonstrating a sufficient revenue-earning record and working capital.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

A notable example from the past 12 months is that of Funding Circle, a peer-to-peer lending platform, which listed on the London Stock Exchange in September 2018 and was valued at close to £1.5 billion. The UK's largest ever fintech IPO is Worldpay, the payments processor, which floated on the London Stock Exchange in 2015 with a valuation of £4.8 billion. Worldpay was bought by US rival Vantiv for £9.1 billion in 2018.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

There is no specific regulatory framework for fintech businesses, which are subject to the existing body of UK financial regulation. Fintech firms will fall within the regulatory perimeter if they carry on certain regulated activities (specified in legislation) by way of business in the UK and do not fall within the scope of an exemption. This regulatory perimeter covers 'traditional' financial services, such as provision of banking, consumer credit and insurance services, as well as certain areas more typically associated with fintech start-ups, such as crowdfunding. It is important to note that just because a firm regards itself as more 'tech' than 'fin', this does not necessarily mean that it will escape regulation; many activities that might be regarded as mere technological services can fall within the scope of the regulatory perimeter. Whether a particular activity constitutes a regulated activity can, therefore, be a complex question and we recommend obtaining specific legal advice.

A firm that wishes to undertake regulated activities in the UK will need to obtain authorisation from one of the UK's financial regulators, the Financial Conduct Authority (FCA) or the Prudential Regulation Authority (PRA). Once authorised, those firms will be subject to a range of additional primary legislation, as well as detailed (and in some cases, activity-specific) rulebooks published by the FCA and the PRA.

The FCA, like other regulators, has recently expressed concern about the regulatory status of coin and token offerings. It reiterated warnings about the risks of consumer harm and fraudulent activity associated with ICOs in its January 2019 consultation on Guidance on Cryptoassets (CP 19/3).

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

Not specifically, as it stands. Whether and what regulation applies to a particular cryptoasset instrument or activity is decided on a case-by-case basis.

In October 2018, the joint HM Treasury-Financial Conduct Authority-Bank of England Cryptoassets Taskforce ('the Taskforce') published a report setting out the UK's policy and regulatory approach to cryptoassets and Distributed Ledger Technology. Among other things, the Taskforce committed to provide further clarity on the regulation of cryptoasset activities and to explore whether unregulated activities should be captured by regulation in the future.

The FCA published a Guidance consultation document in response to the report mentioned in question 3.1 in January 2019 (CP 19/3), focussing on the interaction between cryptoassets and the regulatory 'perimeter'. In particular, it considered where cryptoassets would be considered regulated specified investments under existing legislation or captured by the existing regimes for payment services or e-money. The FCA's framework for categorising cryptoassets is generally based on their intrinsic structure and their proposed use. A Policy Statement on cryptoassets in response to CP19/3 is expected in summer 2019.

The FCA expects to consult on a potential ban of the sale to retail customers of derivatives linked to certain cryptoassets during 2019.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

The financial regulators and policy-makers in the UK are very receptive to fintech. The UK Government's publicly stated position is to make the UK the 'global capital of fintech', and it continues to provide political and policy support to the sector. This support has included developing the UK's digital infrastructure (for example, through the provision of high-speed broadband), creating a favourable tax and investment regime for start-ups (for which, see further questions 2.1 and 2.2 above) and promoting the UK fintech industry globally through its network of embassies and trade delegations.

This favourable political environment naturally has influenced the approach of the PRA and the FCA. In particular, the FCA is generally regarded as one of the most forward-thinking regulators in the world in this area and has established 'Project Innovate' to assist both new and established businesses to introduce innovative financial products and services into the UK. Project Innovate consists of three core elements:

- an 'Innovation Hub', which supports innovative businesses in understanding the regulatory framework and how it applies to them, assists with preparation of authorisation applications for qualifying firms and provides a dedicated contact for up to a year after an innovator business is authorised;
- an 'Advice Unit', which provides regulatory feedback to firms developing automated models that seek to deliver lower cost advice to consumers; and
- a 'Regulatory Sandbox', which the FCA describes as a 'safe space' for businesses to test innovative financial products, services, business models and delivery mechanisms in a live environment without immediately incurring all the normal regulatory consequences of engaging in the activity in question.

The Global Financial Innovation Network (GFIN) was formally launched in January 2019 by an international group of financial regulators and related organisations, including the FCA. This built on the FCA's early 2018 proposal to create a global sandbox. The aim of the GFIN is to support financial innovation in the interests of consumers by providing a more efficient way for innovative firms to interact with regulators. A pilot for firms wishing to test innovative products, services or business models across more than one jurisdiction is expected to run from Q2 2019.

Other regulators are also considering regulatory sandboxes. The UK's Information Commissioner's Office (ICO) is setting one up to support organisations in developing innovative products and services, using personal data in different ways.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

Where a fintech firm wishes to perform regulated activities in the UK, it will need to consider whether it requires authorisation to do so. It is important to note that a person does not need to be established in the UK in order to carry out regulated activities in the UK – a fintech business based overseas which deals with customers in the UK is likely to be viewed as carrying on activities in the UK.

Where an overseas fintech firm performs regulated activities in the UK, it will need to obtain authorisation from the UK financial regulators (as described further in our answer to question 3.1 above), rely on an exemption to the authorisation regime or, if established in an EU Member State, rely on any passporting rights which may attach to the activities in question.

There are numerous exemptions to the performance of regulated activities, some of general application and others associated with specific activities. Application of these exemptions is, of course, fact dependent, but it is worth noting that one exemption – the 'overseas person exemption' – is specifically targeted at firms established outside of the UK. This exemption is, however, restrictive in scope, applying only to certain activities and where there is direct involvement of an authorised or exempt firm in the performance of the activity or a 'legitimate approach' by an overseas person (e.g., an approach that does not breach the UK's financial promotions regime).

As noted above, another route to undertake regulated activities in the UK without authorisation from a UK financial regulator is to rely on a passport provided for in European legislation, at least until the UK's departure from the EU. This would enable the firm to use an authorisation in another EU country to perform regulated activities in the UK. EU firms that currently passport into the UK will be able to continue operating in the UK after Brexit through a temporary permissions regime established under UK legislation.

Overseas fintech firms should also have regard to the UK financial promotions regime under which firms are not permitted, in the course of business, to communicate (or cause to be communicated) an invitation or inducement to engage in investment activity, unless that person is authorised or the communication falls within the scope of an exemption. As with regulated activities, one such exemption relates to overseas communicators.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

On 25 May 2018, the General Data Protection Regulation (GDPR) became applicable in the UK. It has direct effect in all EU Member States and applies to fintech organisations established in the UK which process personal data. Processing is defined widely to cover any operation performed on personal data including collecting, storing or destroying that data. It applies to:

- ‘controllers’ – defined as those organisations which process personal data and determine the purpose and means of such processing; and
- ‘processors’ – which includes service providers and other persons which process personal data on behalf of a controller.

The GDPR retains a principles-based approach: those processing personal data must comply with a set of principles (for example, personal data must be processed fairly, lawfully, transparently and securely) and need a ‘lawful basis’ for the processing (for example, consent). It also codifies case law and best practice guidance developed under the previous regime. However, the GDPR is more prescriptive and restrictive than the law it replaces. For example, it includes mandatory breach notification provisions and high monetary sanctions, and imposes obligations on both controllers and processors (the previous regime only imposed obligations on controllers).

While the GDPR aims to harmonise data protection legislation across the EU, it does give Member States limited opportunities to make provisions for how it applies in their country. In the UK, the Data Protection Act 2018 (DPA 2018) took effect on 25 May 2018: it includes these provisions for the UK. It also covers areas (such as law enforcement) not covered by the GDPR. There are also the Data Protection (Charges and Information) Regulations 2018, which impose a data protection fee of between £40 and £2,900 on data controllers (depending on the size and type of organisation, unless they are exempt).

Note: Unsolicited direct marketing by electronic means is also covered by the Privacy and Electronic Communications Regulations 2003 (PECR), which implement an EU Directive. A new Regulation, to replace this Directive, is currently being negotiated at EU level, although it is unclear when it may be finalised. In addition, sector-specific regulators, including those in the finance sector, regulate the use of data by organisations that fall within their remit.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

Yes to both questions. The GDPR:

- has a wide extra-territorial reach, applying to any controllers and processors established outside the EU who process the personal data of EU individuals and offer goods or services to them, or monitor their behaviour; and
- restricts the transfer of personal data outside the EEA unless adequate protection is in place. The EU Commission has approved a number of jurisdictions as being ‘adequate’,

including, in January 2019, Japan. If there is no formal adequacy decision in place for a jurisdiction, other mechanisms set out in the GDPR and the DPA 2018 may be relied on to transfer personal data out of the EEA. These include using ‘approved form’ standard contractual clauses relating to data export or obtaining consent from the individual whose data is being transferred.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

There are a range of sanctions available, including:

- Large fines – the UK’s ICO can issue fines of up to 4% of annual worldwide turnover or €20 million (whichever is greater).
- Criminal liability – the DPA 2018 includes a number of criminal offences, for example, knowingly or recklessly obtaining or disclosing personal data without the controller’s consent. Directors, managers and officers can (in certain circumstances) be held personally liable for offences by corporations.
- Damages claims – individuals who have suffered as a result of infringement of the GDPR may be entitled to compensation. There is also the potential for representative and group actions in certain circumstances.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

There are a variety of laws and regulations which could apply following a cyber breach in the UK, and many of them derive from EU legislation. For example:

- data protection rules (for example, around security and breach notification) will apply where personal data is involved (see above);
- sector-specific regulators may take action, for example: (i) in the financial services sector, the FCA may take action if a cyber breach was caused by a bank or other regulated entity failing to implement effective systems and controls (which is likely to include having robust cyber security measures); and (ii) fintech businesses which are telecoms operators or ISPs may face action from the ICO for breach of PECR, and Ofcom for breach of the Communications Act 2003; and
- the Computer Misuse Act 1990 creates a number of cybercrime offences relating to actions such as unauthorised access or interference with a computer and DDoS attacks. It was amended in 2015 to implement the EU’s Cybercrime Directive.

The EU’s NIS Directive, implemented in the UK through the Network and Information Systems Regulations 2018, lays down measures aimed at achieving a high common level of security of networks and information systems within the EU. These include imposing security requirements and incident notification obligations on ‘operators of essential services’ together with certain digital service providers. Banks are included in the list of sectors relevant to operators of essential services in the Directive. However, the UK Government has chosen to exclude them from the list of relevant sectors when implementing the Directive into UK law. In their view, the finance sector is already sufficiently regulated in this area.

The UK also has laws relating to the interception of communications and the ability of public bodies to carry out surveillance, although they are beyond the scope of this chapter.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

The UK's key piece of anti-money laundering legislation is the Proceeds of Crime Act 2002 (POCA). There are essentially three principal money-laundering offences: (i) concealing, disguising, converting or transferring the proceeds of crime; (ii) becoming concerned in an arrangement to facilitate the acquisition, retention or control of, or to otherwise make available, the proceeds of crime; and (iii) acquiring, possessing or using property while knowing or suspecting it to be the proceeds of crime. There are also 'secondary' offences of: (i) failure to disclose any of the above offences; and (ii) tipping-off of persons engaged in money laundering as to any investigation.

Firms operating in the regulated sector, including fintech firms, must also comply with the Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 which set out detailed requirements in respect of customer due diligence and anti-money laundering policies and procedures, among other things.

In addition, the FCA specifies additional rules in respect of anti-financial crime systems and controls in its Handbook, which will apply to authorised firms. Both the PRA and the FCA regard adoption of rigorous and robust anti-financial crime systems and controls as essential to meeting the ongoing regulatory requirements of being an authorised firm.

The Bribery Act 2010 (BA) is the UK's anti-bribery legislation. The BA is generally regarded as rigorous and onerous by worldwide standards, and specifies offences in respect of bribing another person, being bribed, bribery of foreign public officials and a corporate bribery offence relating to the failure of commercial organisations to prevent bribery. As with the basic anti-money laundering offences in POCA, the BA applies generally to any entity doing business in the UK.

Finally, there are two corporate offences for failing to prevent the facilitation of domestic or overseas tax evasion, which can be committed by any body corporate or partnership under the Criminal Finances Act 2017.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

Please refer to our comments above on the UK data protection regime and cyber security laws or regulations. There is no legislation in the UK which is aimed specifically at the fintech sector. Any additional relevant regulatory regimes would likely be specific to the sector in which a particular fintech firm operates.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

Subject to the mandatory benefits referred to at question 5.2 below, individuals can generally be hired on whatever terms are considered appropriate. When hiring, it is important to bear in mind that the prohibition of discrimination in employment applies to everything from job advertisement, candidate selection and recruitment, to

employment terms and reasons for dismissal. Unlike most other employment-related claims, compensation for discrimination is uncapped.

Under UK law, the term 'dismissal' incorporates employer terminations, expiry of fixed-term contracts and constructive dismissals (where the employee resigns and treats himself as dismissed due to a repudiatory breach by the employer).

Broadly, employees with two years' service can claim unfair dismissal if a dismissal: (i) does not fall within one of five fair reasons (such as conduct, capability or redundancy); (ii) does not follow a fair procedure (including compliance with relevant codes of practice); or (iii) is not fair and reasonable considering all the circumstances, including the employer's size and resources. Remedies include compensation (subject to statutory caps), or in limited circumstances, reinstatement or re-engagement. Dismissals for certain reasons (such as whistleblowing) are automatically unfair; they do not require a qualifying period of employment, and compensation is uncapped.

Except in cases of gross misconduct or other repudiatory breach, dismissing an employee without the required notice period (or payment *in lieu*, where permitted under the contract) generally leads to a wrongful dismissal, allowing the employee to claim for loss of earnings which he would have received during the notice period.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Employers must pay all workers at least the specified national minimum/living wage, and must contribute to the state pension and health system on the workers' behalf. In addition, eligible jobholders must be automatically enrolled into a personal or occupational pension scheme meeting certain minimum requirements (unless they opt out).

All workers are entitled to at least 28 paid days of annual leave (which includes public holidays and is pro-rated for part-time workers), as well as specified minimum daily and weekly rest periods. Shifts longer than six hours must usually also include breaks. Workers may not work more than 48 hours per week averaged over 17 weeks, unless they opt out of the 48-hour limit (which is very common in practice).

Employees who are unfit for work may be entitled to statutory sick pay after the third day of absence, although employment contracts often provide for more generous company sick pay. Special rules apply in respect of the minimum periods of leave and pay for employees taking maternity, paternity, adoption or shared parental leave and certain other family or study-related types of leave.

Bonuses, which are typically linked to performance criteria, are often non-contractual or involve discretion if included in the contract. Many companies also offer share incentives to their employees.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

Immigration rules apply to all companies and are not specific to the fintech sector. EEA (excluding Croatia) and Swiss nationals, some Commonwealth citizens and qualifying family members may currently work in the UK without permission. When the UK exits the EU, the free movement rights of EEA and Swiss nationals will

be restricted, although the details are yet to be finalised as part of the Withdrawal Agreement. The UK government has proposed that, subject to a deal being agreed, any EU citizens residing in the UK before 31 December 2020 can apply (by 30 June 2021) for the right to remain in the UK indefinitely under a new EU settlement scheme. The same UK immigration rules will then apply to all migrants from 2021. Some aspects of the existing points-based system summarised below will be amended at the same time.

Most other migrants are subject to a five-tier points-based system and (with some exceptions) must be sponsored by an employer and pass a points assessment. The sub-category covering skilled roles which cannot be filled with a UK/EEA worker is subject to an annual limit divided into monthly quotas. Where applications exceed the quota, those scoring the highest points are given priority. Minimum skill and salary levels apply, and all workers must satisfy minimum English language skills and maintenance requirements. The system also allows for a transfer of overseas employees to UK companies within the same corporate group in some circumstances.

Businesses wishing to employ overseas workers must obtain a sponsor licence for the appropriate tier(s), allowing them to issue certificates of sponsorship to migrants. Sponsors must comply with various requirements, including conducting right-to-work checks, complying with record-keeping duties and reporting certain employee events to authorities. Sponsors are rated based on their compliance; if a sponsor's rating is downgraded below a certain threshold, it is not able to issue new certificates of sponsorship (but can usually still sponsor extensions for its existing workers).

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Fintech products will typically be based on computer programs or software, which in the UK is primarily protected by copyright as a type of literary work. Copyright will arise automatically in the computer code and may also subsist in other elements of the software, such as screen displays, or graphics, such as on-screen icons and designs.

In terms of monopoly rights offered by a patent, there are limits on the protection available. Hardware may benefit from patent protection. However, under UK patent law, computer programs as such are excluded from patentability. Business methods are also generally excluded from patentability in the UK. However, it may be possible to obtain a patent where it can be shown that the application of a computer program possesses a technical character and there is research to show that a significant number of patents are being filed in this sector in the UK. Given these difficulties, the law of confidence is an important means to prevent disclosure of technical information, in particular source code. Database rights may also be relevant where the product comprises a type of information management system.

Registered trade marks will protect the branding applied to a fintech product and registered design protection should also be considered for other types of fintech products, such as portable or wearable devices.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Under UK copyright law, the general rule is that the first owner of copyright will be the author, and in the case of a computer-generated

work, the author will be the person who undertakes the arrangements necessary for the creation of the work. An important exception to this rule is that works made by a person in the course of his employment will belong to the employer. However, where a company contracts with a third party to create works (e.g. software) on its behalf, the contractor will own the copyright and the company commissioning the work will need to deal expressly with the ownership of these rights by obtaining an assignment of the rights.

A patent for an invention is owned by the inventor. There are also statutory provisions dealing with the ownership of inventions created by employees.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

IP rights are territorial rights. In addition to national registrations, IP owners seeking UK protection can obtain international and EU-wide registrations for certain IP rights and in some cases can obtain cross-border relief, although this will change in the case of EU Trade Marks and registered Community Designs when the UK leaves the EU (see below).

International copyright conventions provide automatic reciprocal protection overseas for UK qualifying works. The WIPO Copyright Treaty particularly deals with protection of copyright for software and databases.

Patent protection in the UK may be secured via the national route or under the European (EPC) or international (PCT) patent application systems. Upon grant, these registrations provide a bundle of national rights enforced individually as a national patent in the relevant jurisdictions. In Europe, a new unitary patent right, the Unitary Patent (UP) and a complementary centralised enforcement system, the Unified Patent Court, have been agreed but, owing to delays in ratification, is not yet in force. The new patent right will offer protection in up to 26 countries in Europe, with the UPC providing cross-border enforcement for UPs as well as for European Patents.

Trade marks and designs can be registered nationally as EU-wide unitary rights (EU Trade Mark and registered Community Designs), and under international registration systems. The EU rights are enforced in national courts which are designated EU courts and can issue pan-European relief. However, following the UK's departure from the EU, IP owners will need to maintain both EU and UK rights to have comparable protection to the rights that are available now, and on enforcement will need to bring separate actions to enforce UK rights.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

IP is usually exploited/monetised by means of assignment (transfer), licensing, and the granting of security interests.

There are slightly different formalities for the various IP rights for assignments and licences. Generally, however, an assignment must be in writing and signed by the assignor. Copyright licences can be oral or in writing (exclusive licences must be in writing). Patent licences do not need to be in writing but it is encouraged for registration (see below). Trade mark licences must be in writing and signed.

It is important to register transactions concerning registered rights (assignments, licences and mortgages) on the relevant public

register in order to maintain priority as against third-party interests registered in the interim. Where details of an assignment or licence are not registered for trade marks and patents, the assignee/exclusive licensee cannot claim the costs of infringement proceedings relating to the period before registration of the assignment/licence.

Security interests granted through either legal mortgages or charges (in writing and signed) must be registered at Companies House within 21 days following the date of their creation in order to protect against creditors. This is in addition to the registration requirements at the relevant IP registry.



Rob Sumroy

Slaughter and May
1 Bunhill Row
London EC1Y 8YY
United Kingdom

Tel: +44 20 7090 4032
Email: Rob.Sumroy@slaughterandmay.com
URL: www.slaughterandmay.com

Rob is Head of Slaughter and May's Technology and Outsourcing practices and co-heads the firm's Fintech and Emerging Tech Team. He advises on all aspects of IT, outsourcing, e/m-commerce, Big Data, data protection, cyber security and IP, as well as assisting organisations with their digital strategies. Rob is ranked in the IT and Outsourcing sections of *Chambers UK*, recognised as a leading individual for Commercial Contracts in *The Legal 500* and is listed in *SuperLawyers*.



Ben Kingsley

Slaughter and May
1 Bunhill Row
London EC1Y 8YY
United Kingdom

Tel: +44 20 7090 3169
Email: Ben.Kingsley@slaughterandmay.com
URL: www.slaughterandmay.com

Ben is a Partner in Slaughter and May's Financial Regulation practice and co-heads the firm's Fintech and Emerging Tech Team. His clients span the full spectrum, from established global financial and TMT groups to high growth start-up challengers. He advises on all aspects of UK and EU financial regulation, including in the areas of banking, insurance, asset management, payments, mobile banking, e-money, and digital financial services. Ben is recognised in *The Legal 500* as a leading individual in the area of fintech.

SLAUGHTER AND MAY

Slaughter and May is a full-service international law firm headquartered in London with first-class European technology and fintech practices. We are pleased to have been retained as UK and EU legal advisers to a broad range of investors, entrepreneurs, high growth start-ups, established businesses and multi-national corporations. Among our many tech and fintech sector clients we are delighted to have supported Stripe, Euroclear, Equinix, WorldRemit, Aviva, Arm Holdings, Google and Vodafone.

USA

Reena Agrawal Sahni



Eli Kozminsky



Shearman & Sterling LLP

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Innovative financial technology has received enormous interest, popularity and regulatory attention in the United States in recent years. Fintech players in the United States come in various forms and sizes and are offering their institutional and retail customers an increasing variety of services. While the U.S. fintech landscape and the regulation thereof continue to be developing areas, the increase in new fintech start-ups and investment in the sector show no immediate signs of slowing.

Given the emphasis on technology, the United States has seen many prominent players in fintech, including a significant number of start-ups, emerge out of Silicon Valley, like Square, PayPal, Lending Club and Stripe. The types of fintech businesses that have garnered popularity in the United States provide an array of financial services, such as payments, online lending, robo-advice, insurance, and bitcoin and other virtual currency financial products that rely on distributed ledger technology (DLT), with many of such services being provided on a mobile platform as well. New fintech providers and platforms continue to emerge, with each endeavouring to provide consumers with increased access to convenient and secure financial interactions.

DLT, in particular, has garnered a significant amount of regulatory attention in the past several years, as regulators recognise the immense potential for DLT to transform the world of finance and the implications that DLT may have for market participants. Likewise, regulators and courts are increasingly scrutinising virtual currency offerings, such as initial coin offerings (ICOs) and token sales, to ensure that the appropriate securities and/or commodities laws are being followed in the offer and trading of such virtual currencies. Robo-advising has also been receiving increased attention by consumers and regulators alike, with predictions that the percentage of investment assets being managed by robo-advisers will only continue to increase in the coming years.

Another notable trend in the fintech space over the past couple of years is the increase in fintech companies partnering with traditional brick-and-mortar banks to offer financial services to consumers, providing mutual efficiencies that can serve to further increase consumer inclusion and access to financial technology. While the fintech industry was once seen as solely a threat to consumer dependence on traditional banks, banks' partnerships with, and

investments in, fintech firms have helped to alleviate at least some of this concern, as traditional banks find a way to participate in new platforms for traditional bank products.

Finally, regulators in the United States are also monitoring growth in the emergence of innovative technology aimed at helping banks achieve effective compliance with regulations, also known as "regtech".

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

There are currently no U.S. laws or regulations that identify types of business that fintech companies are prohibited from engaging in. However, the business of fintech firms must be in compliance with the general regulatory framework described below in Section 3.

Moreover, as noted above, ICO and token offerings are garnering increasing scrutiny by regulators who are expressing concern about compliance with securities and commodities laws, and who are bringing a critical eye to the role of advisors, accountants, and law firms, to police that compliance.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

Funding from a wide variety of sources and types is available for new and growing businesses, including angel, seed and later rounds of equity, debt and convertible debt investment. Capital can be raised both for lending purposes (if the company is a lending marketplace) as well as investments in the company itself. Funding could come from institutions and corporates, venture capital and hedge funds, and family offices as well as high-net-worth individuals. Publicly sourced crowdfunding has also become an important source of funding for start-up companies in recent years.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

There may be incentives available from certain local jurisdictions or areas to encourage investment in that region. For example, Arizona

recently became the first state in the United States to adopt a regulatory sandbox to encourage the development of fintech within its borders (*see* question 3.3 below for details on this and other such sandboxes). It is recommended to check with the local governments or chambers of commerce for more information.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

The United States uses a disclosure-based system for public securities offerings, including IPOs, meaning that it is the responsibility of the issuer to disclose all risks and uncertainties regarding the issuer and its business/industry in the IPO prospectus. The U.S. Securities and Exchange Commission (SEC) is the chief regulator. There are no specific financial requirements imposed by the SEC, but there may be certain minimum thresholds regarding the number of post-IPO shareholders, the size of the public share float, and certain financial measures depending on which trading exchange is chosen for the listing.

Practically speaking, the most important elements for a successful IPO are a business model that is both proven and not easily replicated by potential competitors, a strong management team that can win and keep the trust of their shareholders, and sustainable growth momentum that can attract quality investors.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

Lending Club, OnDeck and Square have all achieved IPOs. In addition, China-based fintech company Qudian also achieved an IPO in the United States. Therefore, the U.S. capital markets can be used to fund non-U.S. businesses as well through both private and public offerings of equity or debt.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

Fintech businesses in the United States are not subject to a fintech-specific regulatory framework by any single federal or state regulator. Rather, depending on the activities of a fintech company, that fintech company may be subject to a myriad of federal and state licensing or registration requirements, and, thereby, also subject to laws and regulations at both the federal and state levels. The number and complexity of potentially applicable U.S. regulations to any single fintech firm has drawn some criticism as a potential barrier to entry and hindrance to the growth of U.S. fintech. As regulators work to develop regulations that will govern the fintech space, there is also uncertainty as to precisely how the U.S. regulation of fintech will evolve, and the degree to which fintech companies will receive government support and collaboration as the industry develops.

Many fintech companies find that offering their services throughout the United States requires licensing and registration with multiple state regulators, subjecting such fintech companies to regulation and supervision by the laws and regulations of each such regulator. The types of licences that may be required at the state level include consumer lending, money transmission, and virtual currency licences. Depending on the number of states and licences that are

required to be obtained, a fintech company may find the compliance burden to be extensive as each state has its own distinct set of rules and regulations. However, banking regulators of seven U.S. states have recently agreed to simplify the way financial technology companies can apply for licences. These states will recognise each other's findings when assessing the suitability of companies applying for money service business licences.

At the federal level, the Consumer Financial Protection Bureau (CFPB) has jurisdiction over providers of financial services to consumers. Because many fintech businesses are aimed at providing services predominantly to consumers, the CFPB has the ability to enforce a range of consumer protection laws (such as consumer lending laws and anti-discrimination laws) that apply to the activities of such companies. The CFPB also has authority to enforce against the use of unfair and deceptive acts and practices generally.

To the extent that the activities of a fintech provider fall within the licensing regimes of other federal regulators, such as the SEC or the Commodity Futures Trading Commission (CFTC), such fintech providers will be required to register with such agencies and become subject to enforcement by the same. For example, robo-advisers, being a subset of investment advisers, may be subject to SEC registration requirements for such advisers. Finally, fintech companies may also be required to register with the U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCEN) and thus, as described below, comply with the Bank Secrecy Act and other anti-money laundering laws and regulations.

The Office of the Comptroller of the Currency (OCC), the primary federal bank regulator for national banks, announced in July 2018 that it would begin accepting special purpose national bank charter applications from fintech companies that receive deposits, pay checks or lend money. Fintech companies that choose to apply for and receive this special purpose national bank charter will become subject to the laws, regulations, reporting requirements and ongoing supervision that apply to national banks, and will also be held to the same standards of safety and soundness, fair access, and fair treatment of customers that apply to national banks. The OCC intends that, among other things, this special purpose national charter may help level the playing field between national banks and competing fintech companies, while also protecting consumers and providing greater consumer access to fintech services. The chartering of fintech companies by the OCC has drawn some criticism from state regulators, among others, who argue that the regulation of such companies is better accomplished at the local level by regulators who may have a deeper knowledge of certain fintech industry participants and more tailored regulations. In fact, the charter had been on hold due in part to lawsuits from certain state regulators which believe that an OCC charter exceeds the agency's authority.

Regulators with jurisdiction over fintech businesses have not shied away from issuing enforcement actions where fintech businesses are conducting activities in violation of the law. In recent years, fintech companies have been subject to enforcement actions by regulators, including the CFPB, SEC and CFTC. Enforcement orders have been issued for, among other things, insufficient data security practices, violations of federal securities laws, including anti-fraud laws, failing to obtain requisite licences or registrations, and unfair and deceptive practices.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

At the federal level, there is no regulation specifically directed at cryptocurrencies and cryptoassets. However, March 2013 guidance from FinCEN explains that, depending on the nature of their

financial activities, certain businesses that act as exchangers or administrators of cryptocurrency may fall within the definition of a “money transmitter” under FinCEN regulations. Such businesses would thus be required to register with FinCEN as a “money services business” and comply with applicable BSA/AML requirements.

Certain states have adopted, or are considering adopting, cryptocurrency-specific licensing requirements. For example, in New York, the New York Department of Financial Services adopted an expansive virtual currency licensing regulation, or “BitLicense”, in 2015. The BitLicense requires certain businesses that are engaged in virtual currency transmission, custody or exchange services, among other things, in New York or with New York residents, to be licensed to engage in such activities. More recently, similar efforts in other states, such as California, have failed.

Although not specific to cryptocurrencies or cryptoassets, fintech firms must also contend with state-level money transmission licensing statutes. Depending on how cryptocurrency transactions are structured – especially with respect to any involvement of sovereign currency – they could come within the ambit of regulated money transmission, and thus require licensure. Some states, like Texas and Kansas, have issued guidance detailing the treatment of cryptocurrencies under each state’s money transmission licensing statutes. Meanwhile, Wyoming has explicitly exempted receiving cryptocurrency for transmission, or buying, selling, issuing, or taking custody of payment instruments or stored value in the form of cryptocurrency, from the state’s money transmission statute. In the vast majority of states, though, the treatment of cryptocurrency under money transmission statutes remains ambiguous or at least unsettled.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory ‘sandbox’ options for fintechs in your jurisdiction?

Federal financial regulators have been outspoken regarding the vast potential for financial technology innovation and the simultaneous need to tailor the regulation of the sector to protect consumers and mitigate risk without stifling such potential for industry growth. As the fintech space continues to develop, fintech companies have seen an increasing desire on the part of regulators to gain an understanding of the industry from, and work with, fintech market players. Examples of such efforts include the following:

- The CFPB’s “Project Catalyst” initiative aims to increase the CFPB’s outreach to and collaboration with fintech companies in connection with the development of fintech policies. As part of this programme, the CFPB has implemented a no-action letter policy, whereby fintech providers may request a non-binding no-action letter from CFPB staff stating that the agency, subject to certain caveats and limitations, does not recommend enforcement or supervisory action against the entity in respect of specific regulations that may apply to new fintech products to be offered by the entity. The CFPB issued its first such “no-action” letter in September 2017 to a consumer lending firm providing an online lending platform that uses alternative data when making lending decisions, indicating that the staff has no present intention to recommend an enforcement or supervisory action with regard to application of the Equal Credit Opportunity Act and its implementing regulation.
- The OCC has created an Office of Innovation in order to help provide a regulatory framework that is receptive to responsible innovation. The Office of Innovation is intended to serve as a central point of contact for requests and information relating to innovation and has been holding office hours to provide increased OCC staff access to fintech market players.

- In October 2018, Chairman Jelena McWilliams of the Federal Deposit Insurance Corporation (FDIC) announced that the FDIC will launch an innovation office. The innovation office will focus on cultivating a more hospitable environment for banks to explore fintech opportunities. Chairman McWilliams explained how the FDIC can approach innovation in three main ways: firstly, via industrial loan company applications for deposit insurance. Chairman McWilliams has spoken favourably about such applications before, indicating a possible end to the FDIC’s informal moratorium on approving them and sparking interest among some fintech firms. Secondly, through regulation of banks’ third-party vendor relationship. Thirdly, by working with technology companies to improve bank processing, service and efficiency.
- The CFTC approved the creation of LabCFTC, an initiative aimed at promoting responsible fintech innovation. LabCFTC will also look to accelerate CFTC engagement with fintech and regtech solutions. LabCFTC is intended to make the CFTC more accessible to fintech innovators and to serve as a platform to inform the CFTC’s understanding of new technologies, which may influence policy development.

There have also been efforts at both the state and federal levels to establish regulatory “sandbox” options for fintechs:

- In December 2018, the CFPB issued proposed revisions to its 2016 final policy on issuing “no-action” letters (NALs), together with a proposal to create a new regulatory sandbox. The sandbox would be open to fintechs as well as any other entity covered by CFPB regulations. The sandbox would implement a streamlined application and review process through which the CFPB would intend to grant or deny an application within 60 days of notifying the applicant that its application has been deemed complete. Through the application process, applicants would be required to, among other things, describe the product or service that will be offered through the sandbox, explain the potential benefits and risks of the product or service and identify the statutory and regulatory provisions from which the applicant seeks relief. Participants in the sandbox would be required to agree to share data with the CFPB that will allow the agency to determine if the product or service is causing “material, tangible harm to consumers”. Participants would also be required to agree to compensate consumers for any material economic harm caused by the participant’s offering while in the sandbox. The relief provided to firms under the proposed sandbox would be generally consistent with the relief provided through NALs under the proposed NAL policy. However, participants would also be granted additional relief under three statutory safe harbour provisions, and the CFPB would be able to exercise its authority to exempt firms from certain statutory or regulatory provisions. The relief provided through the sandbox would be time-limited, which would likely be for a period of two years in most cases. A firm would be able to apply for an extension of a specified period of time following the expiration of its participation in the sandbox, though. As of the time of writing, the CFPB has not yet issued a final rule on such sandboxes.
- In July 2018, the U.S. Department of Treasury released a report on nonbank financials, fintech and innovation. Among the over 80 recommendations in the report, Treasury identified the ability of regulatory sandboxes to promote innovation. Specifically, Treasury recommended that federal and state financial regulators establish a unified solution that coordinates and expedites regulatory relief under applicable laws and regulations to permit meaningful experimentation for innovative products, services, and processes. Alternatively, if financial regulators are unable to meet those objectives, Treasury recommended that the U.S. Congress consider legislation to provide for a single process, including preemption of state laws if necessary. The report also highlighted the use of regulatory sandboxes internationally to foster innovation.

- On March 23, 2018, Arizona Governor Doug Ducey signed HB2434 into law, making Arizona the first state in the United States to enact a fintech regulatory sandbox. The sandbox is administered by the Arizona Attorney General's Office. The programme's first participant started in October 2018. For businesses that apply to and are accepted into the programme, the sandbox period lasts two years, though participants may seek an extension of up to one year to obtain proper licensing and authorisation to launch the product or service more widely. Consumers are required to be Arizona residents, with participants generally allowed to service as many as 10,000 customers.
- On February 19, 2019, Wyoming Governor Mark Gordon signed HB 57, the "Financial Technology Sandbox Act", which similarly creates a regulatory sandbox programme in Wyoming for companies to test innovative financial products and services, including those using including blockchain technology. The sandbox will allow testing of such products for up to two years, with the possibility of an additional year-long extension before participants must apply for formal licensure. The act will take effect on January 1, 2020.
- On February 14, 2019, Washington, D.C. Mayor Muriel Bowser established a 21-member District of Columbia Financial Services Regulatory Sandbox and Innovation Council. Among other things, the council is tasked with investigating the feasibility of developing a regulatory sandbox for financial services, assessing the benefits of establishing a financial services regulatory sandbox in D.C., and studying the dangers to consumers and the market from regulatory relief of a regulatory sandbox and the necessary safeguards to protect consumers and the financial services markets. The council is slated to produce a report that includes recommendations regarding the development, implementation and administration of a regulatory sandbox in D.C. for fintech and other technology businesses.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

While there is no regulatory framework that applies specifically to non-U.S. fintech companies, such companies must comply with the general licensing and regulatory framework described herein. The regulatory burden accompanying this framework has been critiqued as potentially presenting a barrier to entry for non-U.S. fintech businesses when compared to the regulatory framework applicable to fintech businesses in other jurisdictions. In theory, the Committee on Foreign Investment in the United States (CFIUS), which is charged with deciding whether takeovers of U.S. businesses by foreign companies pose a threat to national security, could prove an impediment to non-U.S. fintech companies accessing U.S. customers through the acquisition of U.S. companies.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

Instead of having one national data protection law, a variety of federal laws regulate how fintech businesses collect, use and

transmit personal data, including: the Gramm-Leach-Bliley Act (GLBA); Fair Credit Reporting Act (FCRA); Federal Trade Commission Act (FTC Act); the Wiretap Act; and the Electronic Communications Privacy Act (ECPA). Key federal agencies that have the jurisdiction to enforce these laws include: the OCC; the CFPB; the SEC; the CFTC; and the Federal Trade Commission (FTC). A number of states have also passed laws that limit the collection, use and transmission of sensitive information, including social security numbers, drivers' licence information, financial data, health data, and others, and have rules relating to data breach reporting notifications. In particular, the expansive California Consumer Privacy Act of 2018 was signed into law in 2018, and becomes effective on January 1, 2020.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

U.S. data privacy laws have generally been accepted to apply to data that is collected by U.S. organisations and stored in the United States, and no U.S. law as of yet has imposed any restrictions on international transfers of data (restrictions on data being transferred out of the United States). However, the question of whether the U.S. Department of Justice can use a warrant to seek data that is stored overseas has been litigated in the courts, and in April 2018, the U.S. Congress passed the Clarifying Lawful Overseas Use of Data, or CLOUD, Act, which purports to clarify when data that is stored overseas must be turned over to U.S. law enforcement. Fintech companies should pay close attention to this area of law and monitor developments in the implementation of the legislation.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

Various federal agencies and state attorneys general have brought enforcement actions against companies for failing to comply with data privacy and consumer protection laws. For example, the FTC has brought over 130 spam and spyware cases and more than 40 privacy lawsuits, whereas the California state attorney general has created a "Privacy Task Force" in 2012 and brings criminal and civil actions against companies and individuals relating to data privacy violations, including failure to post privacy policies and issue timely data breach notifications. Similarly, the West Virginia attorney general joined Massachusetts in suing Equifax, the credit scoring bureau, for failing to safeguard the consumer information of hundreds of thousands of state residents.

In addition, some privacy laws are enforced through class action lawsuits for significant statutory damages and attorneys' fees. Companies can also be sued for violations in data security and privacy practices, such as failure to adequately protect payment card data or for behavioural tracking of consumers without proper privacy notices.

In March 2016, the CFPB brought its first data security action, exercising its authority under the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) to enforce unfair and deceptive acts and practices. Dwolla, an online payment platform company, was ordered to pay a \$100,000 penalty to the CFPB's Civil Penalty Fund after finding that Dwolla's data security practices were insufficient and that Dwolla misrepresented the quality of its data security practices to its consumers.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

Cybersecurity for financial market participants is among one of the top concerns for U.S. regulators. Federal financial regulators have established various customer data and information technology security rules, examination manuals, handbooks and guidance. Furthermore, in October 2016 the federal banking agencies published for comment in an advanced notice of proposed rulemaking on enhanced cyberrisk management standards, which, if implemented, will apply to, among others, any fintech companies that obtain a special purpose national bank charter from the OCC. With respect to consumer financial service providers, the CFPB has also issued enforcement actions against such providers, including at least one fintech service provider (as described above), relating to deficient data security practices.

Notably, at the state level, the New York State Department of Financial Services' cybersecurity rules became effective in March 2017, requiring institutions regulated by the state's financial regulator, including money transmitters, to establish and maintain cybersecurity programmes. It is possible that other states will soon follow suit in establishing their own cybersecurity regimes, which could also apply to fintech businesses that obtain licences from such states' financial regulators.

Given the particular concerns that fintech businesses pose to customer's information security and the increasing regulatory emphasis on the subject, it is critical that U.S. fintech companies identify and comply with all applicable laws, regulations and best practices.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

At the federal level, the Bank Secrecy Act (BSA) is the primary piece of U.S. anti-money laundering (AML) legislation. The BSA requires, among other things, the establishment of a robust AML compliance programme and various reporting requirements, including currency transaction reports and suspicious activity reports (the latter of which also now requires the reporting of cybersecurity-related events). The BSA applies to financial institutions, which definition includes "money services businesses". Many fintech businesses conduct activities that require registration with FinCEN as a money services business, including payment system providers. Moreover, FinCEN has provided guidance specific to the transmission of virtual currency (see question 3.2 above), and has brought enforcement actions against U.S. and non-U.S. companies that have failed to comply with registration and filing requirements under the BSA for their virtual currency transmission activities.

Moreover, "financial institutions" are required to have in place under the USA PATRIOT Act customer identification programmes (CIP) that allow such institutions to know and verify the identity of their customers. CIP requirements applicable to certain financial institutions were also bolstered by a FinCEN rule issued in 2016 requiring further diligence as to beneficial owners in respect of legal entity customers.

Certain states also have in place their own AML requirements that may apply to licensed fintech businesses within such states. In addition, the U.S. Treasury Department's Office of Foreign Assets Control administers economic sanctions that prohibit all U.S. persons from transacting with certain persons and countries that may pose a threat to U.S. national security.

It is imperative that fintech companies understand the scope of BSA/AML and sanctions regulations applicable to their businesses, by virtue of registering as a bank, broker-dealer, money services business or otherwise, and subsequently implement robust AML programmes in compliance with such regulations to avoid enforcement by U.S. regulators who have been placing increased emphasis on AML concerns.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

With the increase in partnerships between traditional banking institutions and fintech companies, fintech businesses should be mindful of the robust vendor management/third-party outsourcing regulations that banks are required to comply with. The requirements of such regulations could subject fintech partners of banks to rigorous diligence, contract negotiations, indemnification requirements, and the jurisdiction of federal bank regulators.

Additionally, it is important to reiterate that depending on the nature of the activities conducted by a fintech business, such business could be subject to the various laws and regulations specific to such activities at both the state and federal level, including lending laws, securities laws, data protection laws and certain consumer protection laws.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

With the exception of immigration law (see question 5.3 below), there are few formal legal requirements or impediments to hiring or dismissing employees in the United States, which generally is an "at will" employment jurisdiction. That being said, employment actions (including employers' decisions regarding hiring, firing, promotions and compensation) with the purpose or effect of discriminating on the basis of sex, age, race, national origin or other categories protected by local law may give rise to government enforcement actions or private litigation. In addition, under federal and, in some cases, state and local law, advance notice (or pay *in lieu* of notice) may be required in the event of "plant shutdowns" or "mass layoffs".

5.2 What, if any, mandatory employment benefits must be provided to staff?

Generally, none, although mandatory payroll taxes are used to contribute to certain government-provided benefits. Benefits are a matter of agreement between employees and employers, but businesses customarily provide some kinds of retirement and medical benefits as well as paid vacations. Once benefits are provided to any employees, there may be legal restrictions on excluding other employees from coverage. The Family Medical Leave Act mandates up to 12 weeks of unpaid, job protected leave per year, for the birth or care of a new-born child, as well as for medical leave for the employee and the care of family members. In addition, the Fair Labor Standards Act and its state and local analogues require that "non-exempt" employees be paid one-and-a-half times their normal rate of pay for hours worked beyond 40 in a

work week. “Exempt” employees are salaried employees receiving compensation above a specified level and performing supervisory or managerial duties. Note that the most important threshold issues in determining whether the above and other legal requirements apply to a “staff” member is whether the individual is an employee or an independent contractor. Many technology companies have been subject to enforcement actions or litigation where they have attempted to categorise service providers as independent contractors but the government or service providers assert employment status, thereby entitling them to certain legal protections, including overtime pay.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

All employers must verify the eligibility of prospective employees to work in the United States through completion of an I-9 form and presentation of documentation confirming identity and employment authorisation. Technology companies have availed themselves of the H-1B visa programme to bring scientists, programmers and other specialised educated employees from outside the jurisdiction to the United States. This programme, which issues 85,000 temporary visas per year to permit the hiring of highly-skilled workers where there is a shortage of qualified workers in the country, as of the time of writing is subject to heightened scrutiny and potential modification by the Trump administration, which has vowed to combat “fraud and abuse” of the programme and ensure that it is not utilised by employers to replace qualified domestic with less-highly-paid foreigners.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

In the United States, inventions can be protected by patents. By statute, a process (or method), a machine, manufacture or composition of matter are all considered eligible for patenting. The patent-eligibility of methods is important to fintech companies whose inventions often involve methods practised using computer technology. While patent protection of methods appears quite broad, recent court decisions have narrowed it considerably. In *Alice Corporation Pty. Ltd. v. CLS Bank International*, the U.S. Supreme Court held that certain claims in a patent were ineligible for patenting because they were drawn to an abstract idea. Abstract ideas are not patentable in the United States. Furthermore, claiming the use of a generic computer implementation failed to transform the abstract idea into patent-eligible subject matter. Fintech companies should be aware that applications that simply require an otherwise abstract method to be performed on a computer will not be considered patent-eligible subject matter.

Software code and certain aspects of computer programs (like text presented on a screen) are copyrightable works in the United States. Copyrighting software offers protection from rivals copying a firm’s software.

Finally, fintech companies can protect their inventions and innovations, particularly the source code in computer programmes, through trade secret law. Unlike patents and copyrights, trade secrets do not expire. Since trade secrets are primarily protected by state law, there is a patchwork of different laws protecting trade

secrets across the United States. However, in 2016, the Defend Trade Secrets Act created a federal cause of action for trade secret misappropriation. Fintech companies should be aware that trade secrets must be continuously guarded by them from public disclosure and do not protect against independent development by another party.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Ownership rights in a patent or trade secret originate with the inventor(s). Ownership rights in a copyright originate with the author(s) of the copyrighted work, unless the copyrighted work is a work made for hire, in which case the entity that commissioned the work is considered its author by the United States Copyright Office (USCO).

Each fintech company should take steps to make sure that it owns the IP generated by or for its business. For example, it should insert a clause into all contracts with employees and contractors that requires the other party to assign all rights to the company in any inventions or works made during the engagement or employment. This clause may add that the parties agree all copyrightable works made by the employee/subcontractor during the term of engagement are works made for hire with the authorship attributed to the company. Furthermore, these contracts should also contain confidentiality obligations that obligate the other party to maintain the confidentiality of all proprietary information generated by them during the engagement or employment.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

In the United States, IP rights are granted locally on the national or state level. The United States Patent and Trademark Office grants patents and registers trademarks. Copyrights are granted by the USCO. State agencies also register trademarks used within their borders. Copyrights and trademarks do not need to be registered as the owner’s rights commence from the creation of the work and the use of the mark, respectively. There is no registry for trade secrets. Instead, rights in trade secrets derive from the owner taking reasonable measures to keep proprietary information which gives its business an advantage secret.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

The primary means of exploiting IP in the United States is through selling goods and services that incorporate the IP and enforcing them against a competitor that uses the IP without permission in its own goods or services.

IP has also become an important tool for raising money. IP portfolios can be sold like any other asset. Fintech companies can use their IP as collateral in loans and gain better terms from the lenders. Also, more complex approaches to patent monetisation are becoming more common. Fintech companies with long track records of generating revenue from their IP assets may securitise them, thereby securing a large, up-front injection of capital in exchange for making payments in the future. The terms of these deals are negotiable, providing flexibility in deal structure. Finally, fintech companies can attempt to monetise their IP by licensing it to others for a royalty or suing infringers for damages.

Acknowledgments

The author would like to acknowledge Jordan J. Altman, a partner in Shearman & Sterling's Intellectual Property Transactions Group, John J. Cannon, a partner in Shearman & Sterling's Compensation, Governance & ERISA Group, Sean Anderson, an associate in Shearman & Sterling's Derivatives and Structured Products Group, and Andy Baxter, a business analyst in Shearman & Sterling's Derivatives and Structured Products Group, for their assistance in preparing this chapter.



Reena Agrawal Sahni

Shearman & Sterling LLP
599 Lexington Avenue
New York 10022
USA

Tel: +1 212 848 7324
Email: reena.sahni@shearman.com
URL: www.shearman.com

Reena Sahni is a partner in the global Financial Institutions Advisory & Financial Regulatory Group. She has extensive experience advising on bank regulation, bank insolvency, recovery and resolution planning and bank capital markets transactions, including Dodd-Frank implementation for U.S. and non-U.S. banks and other financial institutions. Ms. Sahni is shortlisted for the 2016 Euromoney Americas Women in Business Law Awards – Best in Financial Regulation. She was also recognised as a "Rising Star" by *IFLR1000* in 2016. Ms. Sahni also advises on corporate governance, OFAC and AML compliance, internal investigations and regulatory enforcement actions.



Eli Kozminsky

Shearman & Sterling LLP
599 Lexington Avenue
New York 10022
USA

Tel: +1 212 848 7358
Email: eli.kozminsky@shearman.com
URL: www.shearman.com

Eli Kozminsky is an associate in the global Financial Institutions Advisory & Financial Regulatory Group.



Shearman & Sterling LLP distinguishes itself by harnessing the intellectual strength and deep experience of its lawyers across its extensive global footprint. The firm is organised as a single, integrated partnership that collaborates to deliver its best to clients. With approximately 850 lawyers in many of the commercial centres around the world, we operate seamlessly across practice groups and offices and provide consistently superior results. Our lawyers come from some 80 countries, speak more than 60 languages and practise U.S., English, EU, French, German, Italian, Hong Kong, OHADA and Saudi law. We also practise Dubai International Financial Centre law and Abu Dhabi Global Market law. With a deep understanding of our clients' needs, we develop creative ways to address their problems and are ideally situated to counsel them in this challenging 21st century global economy.

Current titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Financial Services Disputes
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms



59 Tanner Street, London SE1 3PL, United Kingdom

Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255

Email: info@glgroup.co.uk