ICLG

The International Comparative Legal Guide to:

Fintech 2017

1st Edition

A practical cross-border insight into Fintech law

A&L Goodbody
Anderson Mōri & Tomotsune
Anjarwalla & Khanna Advocates
BA-HR
Bär & Karrer Ltd.
BonelliErede
Bredin Prat
De Brauw Blackstone Westbroek
ENS Africa
Galicia Abogados, S.C.
Gilbert + Tobin
Gorrissen Federspiel
GVZH Advocates
Haiwen & Partners
Hengeler Mueller Partnerschaft von Rechtsanwälten mbB
Herzog Fox & Neeman
Hiswara Bunjamin & Tandjung (in association with Herbert Smith Freehills LLP)
Kim & Chang
Lee and Li, Attorneys-at-Law
Mannheimer Swartling
Mattos Filho, Veiga Filho, Marrey Jr. e Quiroga Advogados
McMillan LLP
Roschier, Attorneys Ltd.
Shearman & Sterling LLP
Shearn Delamore & Co.
Slaughter and May
SRP-Legal
Trilegal
Udo Udoma & Belo-Osagie
Uría Menéndez
Uría Menéndez – Proença de Carvalho
WKB Wierciński, Kwieciński, Baehr

glg
global legal group

global legal group

Contributing Editors
Rob Sumroy and Ben Kingsley, Slaughter and May

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Paul Mochalski

Editor
Caroline Collingwood

Senior Editors
Suzie Levy, Rachel Williams

Chief Operating Officer
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

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
Ashford Colour Press Ltd
May 2017

ISBN 978-1-911367-49-9
ISSN 2399-9578

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapter:

Country Question and Answer Chapters:

EDITORIAL

Welcome to the first 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:

One general chapter. This chapter provides an overview of Artificial Intelligence in Fintech.

Country question and answer chapters. These provide a broad overview of common issues in fintech in 33 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.

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" is the fintech buzzword of 2017, but what is AI, why is it so relevant to fintech, and what legal issues might be raised by its use? This chapter aims to start to answer these questions, by 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 interact with and serve 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 has risen from $282 million in 2011 to just shy of $2.4 billion in 2015 (World Economic Forum, 2017). Further figures from Bank of America Merrill Lynch are already suggesting that the global market in AI-based systems will reach a value of $153 billion by 2020 (Lewis, 2016); 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 behavior of stocks and markets." Thirty years on he may be proved wrong, as last year, Aidyia, the Hong-Kong based investment company switched on a hedge fund that is entirely automated, requiring no supervision or intervention by humans. At the heart of these newest 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 artificial intelligence as an academic and research discipline, and indeed even as a term, can be traced to a formal beginning at the US Dartmouth College in 1956. 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 Google DeepMind's "AlphaGo" AI beating a leading Go player in 2016.

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 can execute 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 is 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 is at the stage at present 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 this is still a long way off being 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 could start at the beginning of a customer interaction through intelligent identification using machine vision. Certain products or parts of a service could 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 which is capable of 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. For instance, research conducted by McKinsey has suggested that as many as 45 per cent of the activities that individuals are paid to carry out are capable of being automated by adapting technologies which already exist (Chui *et al*., 2015). McKinsey note that, in the US, this proportion of 'activities' represents $2 trillion in yearly wages (*ibid*.).

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 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. Private investments in fintech are growing at an exponential rate. In 2013, investment in global fintech was at less than $5 billion dollars (Ghose, 2016); this number reached $14 billion in 2014 and $19 billion in 2015. Citi estimate that only around one per cent of North American consumer banking revenue has migrated to new digital models (*ibid*.). The Western banking market therefore remains very much in the nascent stages of this disruption cycle, but the forecast is eye-widening: Citi predict that, by 2023, as much as 17 per cent of consumer banking revenue in North America will be derived from new digital models (*ibid*.). 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. Citi, for instance, has reported that there is an 'unbanked population' across India, Indonesia and the Philippines of almost 400 million. This is contrasted with c.80 per cent penetration of mobile phones in India (*ibid*.). The fintech space is 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 start-up that has developed an artificially intelligent 'chatbot' is a prime 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.

Pushing this service further, 8 Securities, a Hong-Kong-based start-up has launched a mobile-only robo-advisory service called Chloe. Chloe surveys users on risk tolerance and financial aspirations and then constructs a portfolio with exchange traded funds listed on the Tokyo Stock Exchange.

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 artificial intelligence, and 2015 saw two more major funds, BlackRock and Two Sigma, hiring top Google engineers.

Big banks, with their sprawling and complex data landscapes, have not been slow to implement AI in different sectors of their business. Citigroup, for example, have injected equity into Ayasdi, which uses machine intelligence to facilitate stress testing and capital planning. Another interesting example is BBVA's relationship with Fonetic, a speech-analytics outfit, to develop and support their record-keeping and compliance in connection with trading. BBVA uses the technology to directly monitor trading floor calls, capturing audio patterns, languages, pronunciations and accents.

The more established companies in the banking sphere have also recognised quickly that AI has massive potential to drive down costs. Compliance, for instance, at present monopolises around 10–15 per cent of staff in financial institutions (Arnold, 2017); according to an FT report, big banks spend over $1 billion annually on regulatory compliance (Arnold, 2016).

However, it should be recognised that, to a large extent, the take-up of AI within financial services is driven by customers. Firms and institutions have little choice. This is borne out in the interesting fact that we can already find in the larger financial institutions very similar instances of those AI systems (such as those referred to above) being developed by smaller-footprint, disruptive firms. UBS, for instance, is piloting both a client-facing financial assistant run on Amazon's Alexa software and a platform that models wealthy Singaporean clients' behavioural patterns to deliver personalised advice.

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 and compliance in the behaviour of an AI becomes very difficult.

The September 2016 report on 'Robotics and artificial intelligence' of the UK Parliament House of Commons' Science and Technology Committee expanded on this point with a helpful example:

"It is currently rare for AI systems to be set up to provide a reason for reaching a particular decision. For example, when Google DeepMind's AlphaGo played Lee Sedol in March 2016, the machine was able to beat its human opponent in one match by playing a highly unusual move that prompted match commentators to assume that AlphaGo had malfunctioned. AlphaGo cannot express why it made this move and, at present, humans cannot fully understand or unpick its rationale."

5.1 Regulatory issues

One currently 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 able adequately 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.

At this very early 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. 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 law and regulation buffers rather than smothers 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 models 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 claim that in 2016 they were granted more than 2,700 patents relating to artificial intelligence, cognitive computing and cloud computing (amounting to 25 per cent of IBM's patents granted in 2016) (IBM (2017)). Of course, the downside of a patent is that the applicant is required to disclose the patentable material (e.g., 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 licence a proprietary AI model to others, and how this licensing is 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 itself processes personal data when it is deployed.

As mentioned at the beginning of this chapter, transparency underpins all regulation. It is also explicitly enshrined in the way in which data protection is legislated for in the EU. Article 5(1)(a) of the General Data Protection Regulation ("GDPR"), which comes into force in the EU in May 2018 (and notably increases the maximum fine for data protection failings to the higher of €20m and 4 per cent of the relevant entity's annual global turnover), provides that personal data must be "processed fairly, lawfully, and in a transparent manner in relation to the data subject".

One way in which this is borne out in the detail of the GDPR, is that the "data subject shall have the right not to be subject to a decision based solely on automated processing". This is because the potential inscrutability of the way in which data is processed by AI can lead to unexpected and unfair outcomes by reflecting unintended biases. Guidance from the UK Information Commissioner 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). There have been other reports of discrimination in the UK, for instance a female doctor was locked out of a gym changing room because the automated security system had profiled her as male due to associating the title 'Dr' with men. (*Ibid*.)

The UK Information Commissioner has also touched on the problem of the obscurity of AI models from the point of view of allowing consumers 'informed consent'. It notes, importantly, that meaningful consent is difficult to provide in the context of AI because of the opaque nature of such machines. But, furthermore, consent as currently modelled may be altogether inappropriate because of its binary nature. A simple yes/no approach could well be incompatible with an AI context in which a computer's mandate may be to find entirely new uses for sets of data. The UK Information Commissioner considers that a more dynamic approach may be possible, "there are new approaches to consent that go beyond the simple binary model. It may be possible to have 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". (*Ibid*.)

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 the 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 12 April 2017].

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 12 April 2017].

3. Newspaper articles

3.1 Lewis, L. (2016). Mrs Watanabe bets on robots to rule. *Financial Times* [online]. Available at: https://www.ft.com/content/70ed10e4-35cb-11e6-9a05-82a9b15a8ee7 [Accessed on 12 April 2017].

3.2 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 12 April 2017].

3.3 Arnold, M. (2016). Market grows for 'regtech', or AI for regulation. *Financial Times* [online]. Available at: https://www.ft.com/content/fd80ac50-7383-11e6-bf48-b372cdb1043a [Accessed 12 April 2017].

4. Websites & online articles

4.1 *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 12 April 2017].

4.2 McCarthy, M. *et al*. (1955). A PROPOSAL FOR THE DARTMOUTH SUMMER RESEARCH PROJECT ON ARTIFICIAL INTELLIGENCE [Online]. Available at: http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html [Accessed 12 April 2017].

4.3 Chui, M., Manyika, J. & Miremadi, M. (2015). Four fundamentals of workplace automation [online]. *McKinsey & Company*. Available at: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/four-fundamentals-of-workplace-automation [Accessed 12 April 2017].

4.4 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 12 April 2017].

4.5 IBM (2017) "Why we patent". Available at: https://medium.com/@IBMResearch/why-we-patent-66ce5a986331 [Accessed 12 April 2017].

Acknowledgment

The authors would like to acknowledge their colleagues Matthew Harman and Harry Vanner for their invaluable contribution 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 and Outsourcing practices and co-heads the firm's Fintech 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 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 *Chambers UK* as a leading individual in the area of financial services.

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, and to have been able to apply our expertise in this innovative area by supporting clients such as Euroclear, Equinix, Stripe, Aviva, Arm Holdings, Google and Vodafone on projects and transactions in the tech and fintech sectors.

Chapter 2

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 within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Australia has seen a proliferation of active fintech businesses in sectors such as lending, personal finance, asset management and payments.

Insurance technology, or insurtech, has had exponential interest in methods of disrupting the individual sections of the insurance value chain, augmenting the existing processes of underwriting risk and predicting loss, and improving the existing capabilities of insurers, reinsurers, intermediaries and service providers.

As compliance costs increase, there has also been an increased focus on regulatory technology, or regtech, and the opportunities to automate regulatory reporting, manage compliance and ensure clarity regarding how regulation is interpreted. The Australian Securities and Investments Commission (**ASIC**) considers the emergence of regtech will assist in promoting a culture of compliance in financial services firms. It is anticipated compliance staff could have an expanded education focus arising from the efficiency gains regtech provides.

There has also been sustained attention on blockchain and distributed ledger technology (**DLT**). Fintech businesses have begun moving beyond proof-of-concept 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 exchange. The ASIC Chairman recently said that 2017 "will be a critical year for distributed ledger technology in financial services" as DLT solutions will begin to be implemented.

Businesses have also begun exploring new automated service methods, such as robo-advisors, for distributing financial advice in more cost-effective ways.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

At the time of writing, there have not been any specific prohibitions or 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)?

In terms of equity funding, businesses can seek funds from private investors (e.g., through private placement or initial public offering), venture capitalists, the Australian Government and through crowdfunding.

In March 2017, Parliament enacted the *Corporations Amendment (Crowd-sourced Funding) Act 2017* (Cth). The Act establishes a regulatory framework for crowdsourced equity funding (**CSEF**) to reduce regulatory barriers to investing in small and start-up businesses. Key requirements for accessing the regime include:

- the asset and turnover test (i.e., unlisted public companies with less than AUD$25 million in consolidated gross assets and annual revenue respectively);
- a fundraising cap of AUD$5 million in any 12-month period;
- that CSEF intermediaries hold an Australian financial services licence (**AFSL**) providing authorisation to operate crowd-funding services, comply with gatekeeper obligations such as due diligence on companies making CSEF issues, provide documentation regarding the CSEF offer in a compliant form and that the CSEF platforms meet certain functionality requirements;
- that retail investors in crowd-funding offers have a five day 'cooling off' period after subscribing in the offer; and
- investment caps for retail investors of AUD$10,000 per issuer per 12-month period, and the requirement for investors to provide a risk acknowledgment statement.

The Act also introduced further exemptions for persons operating markets and clearing and settlement facilities by expanding the types of exemptions which may be given from licensing regimes that are otherwise required to operate those facilities. These exemptions will provide a means by which any person providing a platform for secondary trading can seek exemption from more onerous licensing requirements. These amendments creating exemptions commenced on 29 March 2017, with the balance of the CSEF regime expected to take effect in the second half of the year.

The laws are likely to be subject to some reform in the near future as consultation is conducted to consider whether the regime should be made available to proprietary companies. The industry has asked the Government to explore the potential for the existing crowdfunding

framework to extend to debt funding and the Government has previously indicated it intends to consult on a crowdsourced debt funding framework.

Debt financing is less common than equity financing in the Australian fintech sector; however, businesses can approach financial institutions, suppliers and finance companies in regard to debt finance. The Department of Industry, Innovation and Science has found reliance on equity funding is in part because personal savings and personal credit remain a primary source of debt finance for innovative entrepreneurs in Australia.

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**). Broadly, a company is an ESIC if:

a) it has been incorporated for less than three years;

b) it has income of less than AUD$200,000 and expenses of less than AUD$1 million; and

c) it is undertaking an "eligible business" (i.e. a business with scalability, potential for growth and undertaking research and development).

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) and a 10-year exemption to capital gains tax (**CGT**).

(2) Eligible venture capital limited partnerships

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

For VCLPs, benefits include tax exemptions for foreign investors (limited partners) from CGT on their share of profits made by the partnership, and concessional treatment of the fund manager's carried interest in the partnership. For ESVCLPs, income tax exemption applies to both resident and non-resident investors, plus a 10% non-refundable tax offset is available for new capital invested.

Incentives for Fintechs

The R&D Tax Incentive programme is available for entities incurring eligible expenditure on R&D activities, including certain software R&D activities commonly conducted by fintechs.

Claimants under the R&D Tax Incentive may be eligible for:

a) *Most small businesses of less than AUD$20 million aggregated turnover*: a 45% refundable tax offset (i.e. 45c of each dollar spent paid to the company is refundable in lieu of a tax deduction).

b) *Other businesses*: a 40% non-refundable tax offset (i.e. equivalent to a 10% increase in a tax deduction).

Broadly, eligible R&D activities include experimental activities whose outcome cannot be known in advance and are undertaken for the purposes of acquiring new knowledge (known as **core R&D activities**), and supporting activities directly related to core R&D activities (known as **supporting R&D activities**).

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

The Australian Securities Exchange (**ASX**), Australia's primary securities exchange, sets out 20 conditions to be satisfied in rule 1.1 of the ASX Listing Rules Chapter 1. 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.

The profit test requires entities to have conducted the same business activity during the last three financial years, to have an aggregated profit of at least AUD$1 million for the three financial years prior to admission and to have a consolidated profit of at least AUD$500,000 for the 12 months prior to admission.

The assets test requires entities to have net tangible assets of at least AUD$4 million and a market capitalisation of at least AUD$15 million. However, these thresholds vary for investment entities.

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

In one of the largest fintech M&A deals in Asia in 2016, financial markets software company, IRESS, purchased Financial Synergy, an Australian wealth and investment management business, for a reported AUD$90 million.

In their IPO, fintech compliance firm Kyckr raised approximately AUD$5 million after listing at an issue price of 20c per share in September 2016. The company's network of corporate data is provided to clients in exchange for a subscription fee. Kyckr provides "know-your-business" services to clients.

Payments company, Afterpay, listed on the ASX for AUD$25 million in May 2016 with an issue price of AUD$1.00 per share. Operating on the basis of no upfront fees or loans basis, Afterpay allows e-commerce customers to "buy now and pay later" in regular instalments.

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 that carry on a financial services business in Australia need to hold an AFSL, or qualify for an exemption. The definitions of financial service and financial product under the *Corporations Act 2001* (Cth) are very broad and will often capture investment, market place lending, crowd funding platforms and other fintech offerings.

Similarly, fintech businesses that carry on a consumer credit business in Australia need to hold an Australian credit licence (**ACL**), or qualify for an exemption.

In December 2016, ASIC released *Regulatory Guide 257: testing fintech products and services without holding an AFS or credit licence*, which details ASIC's framework for fintech businesses to test certain financial services, financial products and credit activities without holding an AFSL or ACL (referred to as the "regulatory sandbox").

Fintech businesses testing products and services without holding an AFSL or ACL must have no more than 100 retail clients, plan to test for no more than 12 months, have a total customer exposure of no more than AUD$5 million, have adequate compensation arrangements, have dispute resolution processes in place, and meet disclosure and conduct requirements.

There are strict eligibility requirements for the services and products that qualify for this licensing exemption. Products included are deposit products with a maximum AUD$10,000 balance, authorised deposit-taking institutions issued payment products with a maximum AUD$10,000 balance, general insurance for personal property and home contents with a maximum of AUD$50,000 insured, liquid investments for listed Australian securities or simple schemes and with a maximum AUD$10,000 exposure, and consumer credit contracts with certain features and a loan size of between AUD$2,001 and AUD$25,000.

In regard to services, fintech companies providing advice and dealing in or distributing products are eligible, but those issuing their own products, lending money to consumers, or operating their own managed investment scheme will not be able to rely on the exemption.

3.2 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?

In Australia, fintech is a focal point for economic growth and it is generally accepted that policy and reform in the financial services sector will be driven by fintech innovations. The Australian Government and regulators have generally been responsive to facilitating the development of fintech. More broadly there has been the AUD$1.1 billion National Innovation and Science Agenda (**NISA**) promoting commercial risk taking and encompassing tax incentives for early stage investment in fintech companies, changes to the venture capital regime, insolvency law reforms, the establishment of the FinTech Advisory Group to advise the Treasurer and the ASIC Innovation Hub.

The ASIC Innovation Hub is designed to foster innovation that could benefit consumers by helping Australian fintech start-ups navigate the Australian regulatory system. The Innovation Hub provides tailored information and access to informal assistance intended to streamline the licensing process for innovative fintech start-ups.

ASIC has also released *Regulatory Guide 255: providing digital financial product advice to retail clients* which details issues that digital advice providers need to consider generally, during the AFSL application stage and when providing advice. Digital advice is defined by ASIC as being that advice which is produced by algorithms and technology. The regulatory guide is also relevant to situations where digital advice is provided in a hybrid model and involves a human adviser. The guide should be considered by any fintech business that provides digital or hybrid advice, and is considering operating in Australia, to ensure that licensing requirements can be met.

Fintech businesses should also be aware that in March 2017, ASIC released *Information Sheet 219 Evaluating distributed ledger technology* for both existing licensees and new market entrants. The information sheet informs businesses considering operating market infrastructure or providing financial or consumer credit services using DLT of how ASIC will assess whether a proposed DLT solution is compliant with licence conditions. The assessment mechanism in the information sheet can be used to determine whether ASIC is likely to have concerns about the proposed implementation of a DLT solution by a fintech business.

The Australian Transaction Reports and Analysis Centre's (**AUSTRAC**) newly established Fintel Alliance has also announced an innovation hub targeted at improving the fintech sector's relationship with Government and regulators. The hub will also test a regulatory sandbox for fintech businesses to test financial products and services without risking regulatory action or costs.

The Government has also committed AUD$8 million to an Incubator Support Program to assist innovative start-ups by providing funding, mentoring, resources and business network access. The Government is also becoming a fintech "participant" via its "digital transformation office" seeking to provide better access to Government services online and looking to create a digital market place for SMEs and start-ups to deliver digital services to Government.

3.3 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 satisfaction of requirements relating to carrying on a business in Australia (which includes the requirement to incorporate a local subsidiary or register a branch office) and additional requirements applicable to carrying on a financial services business in Australia such as the requirement to obtain an AFSL or ACL, or satisfaction of conditions to entitle the provider to rely on an exemption. Broadly, this is 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.

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 1988* (Cth) (**the Privacy Act**) regulates the handling of personal information by Australian Government agencies, Australian Capital Territory agencies and private sector organisations with an aggregate group revenue of at least AUD$3 million. The Privacy Act does apply to some businesses, for example credit providers and credit reporting bodies, regardless of turnover. If a fintech business is providing credit or dealing with information related to credit, then the business may be subject to the Privacy Act, regardless of the revenues of the business. Fintech companies are subject to the same legal requirements and regulatory guidance relating to personal information as any other company.

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

- open and transparent management of personal information;
- disclosure to a person that their personal information will be collected;
- restrictions on the use and disclosure of personal information;
- obligations to ensure the accuracy of collected personal information; and
- obligations to protect personal information.

The APPs provide for personal information to be de-identified, including to enable information to be disclosed in a form which does not contravene the Privacy Act.

The Office of the Australian Information Commissioner (**OAIC**), which administers the Privacy Act, has published guidance on de-identifying personal information. The guidance describes methods for de-identification, which may include removing or modifying personal identifiers and aggregating information.

However, the application of existing privacy and confidentiality laws to fintech companies is the subject of current discussion and review so developments are expected in this area. The Government has requested the Productivity Commission to consider ways to increase data availability in Australia with a view to boosting innovation, which will be particularly important for fintech innovators.

In particular, the Commission will examine whether big banks should be forced to share more data on customer transactions with fintech companies. The Commission will hand down their final Data Availability and Use report to the Government in March 2017. The Report had not yet been publicly released at the time of writing.

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 an act 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 or holds personal information in Australia.

Under the framework for cross-border disclosure of personal information outlined in APP 8 and s 16C of the Privacy Act, APP entities must 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 comply with APP 6, which states that entities must 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.

OAIC has a range of enforcement powers, including the power to:

- make a determination requiring the payment of compensation for damages or other remedies, such as the provision of access or the issuance of an apology (enforceable by the Federal Court or Federal Magistrates Court);
- accept enforceable undertakings;
- seek civil penalties of up to, or apply for civil penalty orders of up to AUD$340,000 for individuals and up to AUD$1.7 million for companies; and
- seek an injunction regarding conduct that would contravene the Privacy Act.

The Australian Government also enacted the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth), which creates reporting obligations for businesses when eligible types of data breaches occur. Under the Privacy Act, OAIC carries the power to investigate non-compliance with respect to this obligation and can apply to the court to have civil penalties imposed for non-compliance.

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 given the rapid innovation present in the fintech space and the interplay between fintech products and new technologies.

ASIC also provides some guidance regarding cybersecurity. ASIC published *Report 429: Cyber Resilience – Health Check* and *Report 468: Cyber resilience assessment – ASX Group and Chi-X Australia Pty Ltd* in relation to financial market infrastructure providers and cyber-resilience, expressing ASIC's intention to work to assist other organisations in Australian financial markets to enhance their cyber resilience framework and environment.

In those reports, ASIC provided examples of good practices identified across the financial services industry and some questions board members and senior management of financial organisations should ask when considering their cyber resilience. ASIC also outlined the relevant legal and compliance requirements of different regulated entities. ASIC's Regulatory Guide 255 also particularised the standards and frameworks which providers of digital advice should test their information security arrangements against and nominated frameworks setting out relevant compliance measures which should be in place where cloud computing is relied upon.

As part of the NISA, a Cyber Security Growth Centre has also been set up with industry-led not-for-profit body, Australian Cyber Security Growth Network, responsible for administering the Centre's activities. As part of the strategy, the Government has proposed co-designing national voluntary Cyber Security Guidelines with the private sector to specify good practice in future and introducing national voluntary Cyber Security Governance 'health checks' to enable boards and senior management to better understand their cyber security status.

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.

To the extent a fintech company provides a designated service under the *Anti-money Laundering and Counter-terrorism Financing Act 2006* (Cth) (**AML/CTF Act**), such as by factoring a receivable, providing a loan, or issuing or selling securities or managed investment scheme interests, the company will be a reporting entity for the purposes of the AML/CTF Act. The company will have obligations to:

- enrol with AUSTRAC;
- conduct due diligence on customers prior to providing any 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 transfer instructions.

For fintech businesses engaging in digital currency exchanges, the Attorney-General's office has recently closed consultation on amending the AML/CTF Act to "regulate activities relating to convertible digital currency, particularly activities undertaken by digital currency exchange providers". The Government is aiming to draft legislative proposals later this year.

A fintech company, like any other company, is also required to comply with Australia's anti-bribery legislation, which includes a prohibition on dishonestly providing or offering a benefit to someone with the intention of influencing a Commonwealth public official in the exercise of their duties.

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

Not at the time of writing, however the Government recently issued a Proposals Paper suggesting the introduction of design and distribution obligations on issuers and distributors of financial products, and a new product intervention power for ASIC, which could impact fintech businesses. Neither of these amendments would necessarily affect fintech businesses, however some fintech businesses will need to comply with the legislation when it is introduced.

In relation to design and distribution obligations, under the proposed recommendations, businesses that fall under the definition of an issuer or distributor must ensure that products meet the needs of its target market and are marketed appropriately.

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 some employees (including professionals) are governed by modern awards. However, modern awards do not apply to employees earning over a threshold of AUD$138,900 (from 1 July 2016, threshold indexed annually), provided their earnings are guaranteed by agreement with their employer.

To terminate an employee's employment, an employer has to give an employee written notice. 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 also 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 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 ten National Employment Standards. Briefly, these include maximum weekly hours, requests for flexible working arrangements, parental leave and related entitlements, annual leave, long service 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 workplace 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 via the Department of Immigration and Border Protection (**DIBP**) in order to work in Australia, and each type has its own eligibility requirements. Businesses can nominate or sponsor such visas.

In September 2016, as part of NISA, the DIBP 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.

Eligibility criteria for applicants includes:

- the applicant proposes to undertake an entrepreneurial venture unrelated to residential real estate, labour hire and not involving purchasing an existing business or franchise;
- the applicant must not be older than 55, must have a competent level of English, and have at least 30% interest in their entrepreneurial venture; and
- there must be one or more funding agreements in place for at least AUD$200,000 between the entrepreneur or venture and a third party funding body or bodies.

Successful Entrepreneur visa holders can progress their permanent residency applications by meeting measures of success such as business turnover, employment of Australians and obtaining significant financial backing.

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, useful and inventive. 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 be innovative.

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.

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 such 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.

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 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 must be held to protect or enforce IP rights in Australia. However, 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 remain 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 and each come 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 use (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 NSW 2000
Australia

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

Peter is a Special Counsel in Gilbert + Tobin's Corporate Advisory team and specialises in Australian financial services laws and funds management. Peter's practice includes advising Australian and off-shore corporates, financial institutions, funds, managers and market participants in relation to establishing, structuring and operating financial services sector businesses in Australia. Peter also advises across a range of issues relevant to the FinTech and digital sectors including platform establishment, blockchain solutions, digital fundraising and currencies and regulatory compliance, and has extensive experience dealing with regulators. Peter has a Bachelor of Laws (Honours) and Bachelor of Commerce (Finance) from the University of Newcastle.

Brazil

Renato Schermann Ximenes de Melo

Mattos Filho, Veiga Filho, Marrey Jr. e Quiroga Advogados

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 within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Brazil has witnessed a significant increase in fintech businesses in the last two years, in many different sub-sectors (payments, finance management, online lending, investment advisory, funding, insurance, debt restructuring, cryptocurrency, blockchain, foreign exchange, etc.). Brazil leads the way in Latin America with 244 established fintechs (as per Radar FintechLab 2017) – most of them in the payments sub-sector (32% of Brazilian fintechs). Following the startup movement, there is also a trend of large financial institutions launching their own versions of digital financial services platforms, such as financial management apps, digitally managed bank accounts and credit cards.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

Many services in the Brazilian financial and capital markets can only be provided by regulated and authorised entities. Services such as the provision of loans or financing in Brazil as businesses are restricted to financial institutions and interest rates charged on loans are heavily limited for non-financial institutions, which leads fintechs operating in these fields to establish partnerships with typical financial institutions to perform their activities.

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. Recent legislation was enacted to promote a new form of investment in startups, referred to as "angel investment", which can be made in the form of capital contributions with a limitation in returns applicable during the initial period. An angel investor may only invest in microenterprises and small businesses. The angel investor is not deemed an equity holder of the investee, so it is not liable for development of the investee's activities, including in case of judicial recovery or disregard of legal entity. This is still an incipient legal mechanism to be tested. The Brazilian Securities Commission (*Comissão de Valores Mobiliários* – CVM) has also launched a public hearing for new rules on investment-based crowdfunding, which are expected to be published this year, enhancing confidence in this fintech sub-sector in Brazil and expanding funding sources for small businesses and startups.

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?

Some government incentives are available for startup projects in Brazil, such as fintech businesses, and incentives usually take the form of subsidised loan financing and tax exemptions or reductions, rather than cash grants. In Brazil, there are federal, state and local incentives. Federal government incentive programmes are designed to promote domestic policy objectives, including the growth of exports and the capitalisation of domestic private industry, whereas state and local incentive programmes are directed toward specific objectives such as increasing local employment opportunities. Thus, a fintech that decides to do business in Brazil needs to seek the best package of state and local incentives available when deciding where to locate its business. In addition to the incentives above, small and medium-sized businesses may opt for a simplified and less bureaucratic tax regime introduced by Complementary Law No. 123/2006 – the *Simples Nacional*. Under this regime, taxpayers collect most of their taxes via one unified document. Overall, legal entities assess the tax amount due by applying certain percentages established by the applicable law, depending on their activity, over gross revenues earned monthly. Such percentages may vary from 4% to 22.45%. Regarding technology innovation incentives, there are tax benefits with the purpose of fostering research and development of technological advances, applicable for most companies investing in technology innovation, which include, among others: (i) accelerated depreciation for income tax purposes of newly acquired equipment (destined to R&D); (ii) lower tax on manufactured products (IPI); (iii) accelerated amortisation for certain intangibles and expenses with R&D; and (iv) certain income tax and social contribution deductions. Moreover, there is a special tax regime for the export of information technology services (REPES – Special Taxation for Export of Information Technology Services) and a regime directed to hardware sales (digital inclusion programme).

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

In order to IPO in Brazil, a company needs to: (i) obtain its registration as a public company with 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, 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, as, 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 during this time. 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, 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 reduced number of 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?

Fintech is a recent trend in Brazil, so there have not been many investment exits yet. An exit was announced in 2016, when the investment fund manager Ideiasnet sold its equity interest in Moip Pagamentos (a Brazilian fintech founded in 2008) to Wirecard, a German fintech, for R$165 million – roughly US$50,000.

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 – CMN. Financial services are regulated by the Brazilian Central Bank and 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, 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 consider requesting authorisation to operate 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 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 which collection will be allocated to settle the deposits, 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 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?

The Brazilian Central Bank, CVM and SUSEP have been demonstrating interest to discuss innovative business models in the financial and capital markets. These regulators have been constantly present in events related to fintechs in the past year. Both CVM and Brazilian Central Bank have been promoting discussion forums and inviting fintechs and advisors in the fintech field for discussions on innovation and regulation. CVM and the Brazilian Central Bank have organised internal workgroups 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 to the stability and soundness of Brazilian markets and are now starting to make clear that some regulation is expected in this field to deal with these new market agents, specially unregulated agents, and their potential impact on public trust and financial stability. New regulations on internal controls and compliance systems enacted by the Brazilian Central Bank require regulated financial institutions to actively oversee all their outsourced activities and service providers, performing diligence on systems and activities and generally remaining liable for potential losses arising from such third parties operation, irrespective of any direct liability that may be imposed on them.

3.3 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. 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?

Brazil has not yet enacted a general personal data protection law. However, there are general principles and provisions on data protection and privacy in the Brazilian Constitution, in the Brazilian

Civil Code and in the Internet Act. Currently, there are two important bills regarding privacy and data protection under discussion in the Brazilian Congress and on the Senate. The Internet Act requires fintechs to hold user data (including access logs, IP address, time and date of connections) for six months. It also imposes on fintechs the burden to seek affirmative consent for data treatment. Moreover, fintechs will usually be subject to the Banking Secrecy Law that dictates that financial institutions and other institutions accredited to operate by the Brazilian Central Bank shall keep all customers data and transactions confidential, as well as the services rendered by them.

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 Internet Act applies to fintechs even if they are not established in Brazil, to the extent that fintechs 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, there is no special requirement other than providing the data subjects with clear and comprehensive information with respect to the treatment of data. It is worth noting that a proposed data protection law has a full chapter regarding international data transfers, so changes are expected in this matter in the near future. Due to their usual association with regulated entities, fintechs should generally be subject to the Banking Secrecy Law, even if they are stablished outside Brazil.

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

In addition to civil, criminal or administrative sanctions that may apply depending on the circumstances, failing to comply with the Internet Act with regard to data protection 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 its most recent financial 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. Banking Secrecy Law's penalties should affect the regulated entities only.

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

The Internet Act was regulated by a Decree, which imposes certain requirements for internet companies generally, including fintechs. Amongst such requirements, we could cite: (i) the obligation to keep record of employee access logs to database containing personal data of the company's customers; and (ii) the requirement for encryption or similar technology for static or moving data packages. The Internet Steering Committee is in charge of providing more rules and recommendations in this area.

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. 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.

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, it is specially worth noting that Brazilian Consumer Protection Laws will also apply. Consumer Protection Laws create an additional burden to fintech's activities because of heavier disclosure and suitability requirements and inversion of the burden of proof whenever litigation is initiated.

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, against payment and 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 Length of Service Fund (FGTS) in the course of the employment agreement. 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 ⅓ bonus, social security contributions (around 28.5% over salary) and deposits on the FGTS (8% over all regular payments), payments and benefits arising from collective bargaining agreements with the representative trade union, transportation voucher, among other benefits according to their personal situations (e.g., maternity leave for 120 days). Interns are not entitled to every employee benefit, but must be granted insurance against personal accidents. Moreover, all employees must be registered before 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 in order to apply for working visa, which can be either temporary or permanent. Brazilian law contemplates the following types of visa: (i) transit; (ii) tourist; (iii) temporary; (iv) permanent; (v) courtesy; (vi) official; and (vii) diplomatic. The temporary business visa is granted to the foreigner who intends to come to Brazil for the purposes of doing business or working temporarily in the name of the foreign company, without the intention of residing in the country. The holder of a business visa is not allowed to receive any remuneration for his services by Brazilian sources or to sign any documents in the name of a Brazilian company. Brazilian companies that intend to bring a foreign professional to Brazil, to render specialised services in the name of the foreign company, must request a temporary visa in their favour. The permanent visa is the appropriate visa for a foreigner who will take office or perform the activities of manager or director of any commercial or civil Brazilian company.

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, which was conceived in accordance with the TRIPS Agreement. In order to be protected under BIPL and granted a patent, the 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. However, it is protected under the Brazilian Copyrights Law and can be registered with the Brazilian Patent and Trademark Office (*Instituto Nacional Propriedade Industrial* – INPI).

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 INPI. BIPL 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 Bern Convention. Nonetheless, in order to be enforceable within Brazil, intellectual property rights (excluding copyrights) must be filed for and registered/granted by the INPI, in accordance with BIPL. Another exception is the protection granted to well-known marks by the BIPL (in accordance with 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 licensing of copyrights, including software. Restrictions apply to 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 imposes several restrictions for such remittances, which also apply to supply of technology agreements. The INPI limits the amount of royalties that can be remitted out of Brazil for patents, trademarks, industrial designs and unpatented technology. In case the entity earning the royalties controls the entity paying them, the restrictions are even more stringent and the royalty remittances in such cases cannot exceed 5% of the net sales of the product or service that used the IP right. The INPI does not recognise the concept of licence of technology. In other words, the technology has to be permanently transferred to the Brazilian recipient, and provisions that limit the Brazilian entity's ability to use the technology after the expiration of the agreement are normally not accepted by the INPI.

Renato Schermann Ximenes de Melo
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 7748*
Email: *rximenes@mattosfilho.com.br*
URL: *www.mattosfilho.com*

Renato 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. He advises clients on regulations issued by the Brazilian Securities Commission and the Brazilian Central Bank. His expertise includes matters related to payment systems, financial services, clearing and settlement of funds, financial assets and securities. Renato is a Bachelor of Laws graduated from Universidade Presbiteriana Mackenzie.

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*

Fabio practises in the telecom, 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 is Bachelor of Laws, from Pontifícia Universidade Católica de São Paulo, and 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, 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 Visa, Google, IBM, Worldpay, Stone, Geru, Goldman Sachs (cross-border financing to Nubank), Cielo, B2W, UOL (PagSeguro) and other fintechs on their regulatory compliance and everyday activities.

Canada

Pat Forgione

Jeffrey Nagashima

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 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. The Canadian banking sector has led the development of Canadian fintech by providing a source of talent, capital and technology to fintech businesses in addition to developing their own in-house technology. In particular, one fintech sector driven primarily by Canadian banks is payments technology. There has been widespread adoption of both near field communications payments, i.e. "tap", and digital cheque deposits.

However, it is important to note that a number of fintech start-ups are challenging banking core businesses in fields such as investments and asset management, particularly through the use of artificial intelligence and big data analytics. Furthermore, these fintech start-ups have been assisted by the proliferation of fintech incubators which provide initial sources of capital and expertise.

We expect 2017 to see a high degree of activity for fintech businesses. The launch of the Canadian Securities Administrators' regulatory sandbox initiative should prompt the development of both crowdfunding and peer-to-peer lending sectors. Similarly, the most recent federal budget outlined a focus on "digital industries". Specifically, $950 million will be invested over five years to fund "superclusters", that is, concentrated areas of technology businesses and incubators, likely prompting significant growth of fintech companies. The budget also provided that the government will create a modernized intellectual property strategy and spend $125 million to create a pan-Canadian artificial intelligence strategy amongst other developments.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

There are no prohibitions or restrictions that are specific to fintech businesses in Canada.

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. However, 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 a crowdfunding regulations which provides 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 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 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. More recently, on October 24, 2016, the Ontario Securities Commission granted a two year limited exemption for the operation of an online investing platform for accredited investors to connect with start-ups in the technology space. 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.

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 fintech small and medium sized enterprises ("**SMEs**"). The Canadian Government offers the following incentives for SMEs and growing businesses:

- The Scientific Research and Experimental Development programme 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 grant 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), that 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 1,000,000 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 recognises 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 1,000,000 freely tradable securities having a market capitalisation of at least $1 million 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 and having a market capitalisation of at least $500,000.

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

In March 2017, US private equity firm Vista Equity Partners acquired DH Corp, a Canadian fintech business with expertise in payments and lending, for $2.72 billion. More recently, PayPal Holdings, Inc. purchased TIO Networks Corporation for $233 million.

For equity financing, Shopify Inc. remains the leading case study for 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.

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 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?

Financial regulators and policy makers 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 preliminary steps towards developing a fintech regulatory framework. For example, the Department of Finance has launched a two-stage consultation process to help improve the financial sector regulatory framework. Similarly, the Competition Bureau is undertaking a market study on fintech which is expected to be published this spring.

In addition, the Canadian Securities Association has launched their own regulatory sandbox which should assist capital raising fintech businesses. This initiative is in addition to the existing crowdfunding

regimes and provincial security regulator programs already available, such as the Ontario's Launchpad programme which helps fintech businesses navigate securities regulations in Ontario.

3.3 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. Ontario has entered co-operation agreements with other jurisdictions, including Australia and the United Kingdom to refer and support fintech businesses.

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 transmission 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 collection, use and disclosure of personal information;
2. openness about information handling practices (and 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 (and 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 present 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 that the information will not be used for purposes other than the purposes for which it was collected. Most private sector privacy legislation, such as PIPEDA, also holds 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, in June 2015, PIPEDA was amended to introduce breach reporting and recording requirements in certain circumstances. Failing to report or record a breach will be an offence punishable by fines of up to C$100,000. These new provisions have not yet come into force, but will become mandatory once associated regulations have been enacted.

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 recipients 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 called the *Proceeds of Crime (Money Laundering) and Terrorist Financing*

Act ("**PCMLTFA**") and 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 investigation and prosecution of money laundering and terrorist activity financing offences.

The PCMLTFA applies to all "reporting entities" which includes, 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 Reporting 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 be registered with FINTRAC and must supply information about themselves and their activities.

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 not deal directly or indirectly in any property (including money) that is owned or controlled by or on behalf of a Designated Person, not facilitate any transaction in respect of such property, and not provide any financial or other related services in respect of such property. As well, 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 cause for dismissal, employers must generally provide employees with 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, maternity 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 it has conducted recruitment for a Canadian citizen or permanent resident and could not fill the position, or that the skills and requirements of the position are such that there is no Canadian citizen or permanent resident who could fill the position.

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, such as NAFTA and GATS. 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 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 it 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, 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 deal 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 practices 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.

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

Tel: +1 416 865 7136
Email: jeffrey.nagashima@mcmillan.ca
URL: www.mcmillan.ca

Jeffrey is an associate in the firm's Business Law Group in the Toronto office. His practice is focused on mergers and acquisitions, privacy and data protection, technology, insurance and general corporate matters. He has acted on a number of M&A transactions involving technology companies and regularly advises on data protection and privacy issues. He also led a project to automatically generate a customised set of transaction documents for M&A deals.

Jeffrey joined McMillan as a summer student in 2013 and completed his articles with the firm in 2015.

mcmillan

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.

China

Jinen Zhang

Haiwen & Partners

Xixiang Lin

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 within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

China is one of the most dynamic countries for fintech business around the world and is at the forefront of various types of fintech businesses including digital payments, online lending and investments. According to Accenture, in the first seven months of 2016, Asian fintech investments reached USD 9.6 billion and over 90% invested in Chinese companies.

China continues to take a leading role in digital payment. In 2016, the transaction volume of internet payment was RMB 1,900 billion and mobile payment was RMB 3,800 billion. QR codes have had an overwhelming influence on people's lifestyles – users can simply open WeChat or Alilpay to scan a QR code and make a payment. Fingerprint identification, face recognition and other advanced verification methods further guarantee payment safety.

Online lending and financing activities, represented by crowdfunding and peer-to-peer (P2P) lending have also been developing robustly. By the end of September 2016, there were more than 2,200 online lending platforms in normal operation in China.

For wealth management, with the development of artificial intelligence, intelligent robotic systems can provide "one-click customisation" services, which lower entry thresholds and management fees.

The application of big data has had an active influence on customer risk ratings and credit ratings. Take internet insurance for example – insurance companies create contextualised insurance by subdividing its target audience, to help clients choose products quickly. Also, blockchain, which is widely recognised as bringing fundamental changes to the financial industry, has already attracted lots of emerging companies focusing in this area.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

There are no prohibitions or restrictions that are specific to fintech business 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)?

Like other jurisdictions, new and growing businesses may raise funds through equity or debt financing in China.

For equity financing, normally, start-up businesses may raise funds through private equity investment or IPO, based on their respective economic scales and stages of development. In addition, equity crowdfunding is currently a developing market accessible to start-up or growing businesses. The well-known equity crowdfunding platforms in China mainly help start-up businesses find angel investment. It is reported that the overall scale of funds raised through equity crowdfunding in 2016 in China reached approximately RMB 22 billion.

For debt financing, in general, traditional bank loans have been only available to enterprises that could provide mortgages or other collateral. With the guidance of China's "Mass Entrepreneurship and Innovation" policy, banks have introduced loan service solutions that provide easy access to credit for high-tech enterprises, but it is still difficult for start-ups to obtain loans from commercial banks. Simultaneously, lots of small-sum loan companies and online loan platforms are also accessible to growing business, allowing them to obtain debt financing.

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?

Tech/fintech businesses and small/medium-sized businesses in general, may enjoy tax preference and other incentives. In addition, there are also tax benefits for venture capital firms to encourage them investing in start-up companies:

- qualified high-tech enterprises enjoy a reduced income tax rate of 15% (compared to a standard rate of 25%); some special economic zones offer the policy of "exemption from income tax for the first two years and 50% reduction for an additional three years" for high-tech enterprises;

- qualified small low-profit enterprises enjoy a reduced income tax rate of 20%; taxable income amount may be further reduced if annual taxable income is below a certain amount according to relevant rules; and
- a venture capital firm investing in small/medium-sized high-tech enterprises for two years and above and satisfying certain criteria may offset 70% of the investment amount in such enterprises against its taxable income amount.

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

China has main-board markets and a growth enterprise market ("**GEM**") for IPO, and the conditions for listing differ between the two. Start-up enterprises normally choose to undertake IPOs on GEM because the conditions for a GEM IPO are much easier to satisfy.

The main conditions for a main-board IPO include:

- consecutive operations for at least three years;
- no change of control during the latest three years;
- sustained profitability;
- positive net profits during each of the latest three years of more than RMB30million in aggregate; and
- net cash generated from operations for the latest three years of more than RMB 50 million, or the operating revenue for the latest three years of more than RMB 300 million.

In contrast, the conditions for a GEM IPO are much less demanding and mainly include:

- consecutive operations for at least three years;
- positive net profits for each of the latest two years of more than RMB 10 million in aggregate, or positive net profit for the latest year with operating revenue of more than RMB 50 million over this time; and
- net assets of more than RMB 20 million and no undistributed deficit.

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

Yirendai, a P2P online loan platform, listed on the New York Exchange in December 2015, raising USD 75 million and becoming the first Chinese internet finance/fintech IPO. Lakala, a third party payment service company, has submitted its GEM IPO application to China Securities Regulatory Commission ("**CSRC**") recently.

Additionally, it is reported that several Chinese fintech enterprises, such as Ant Financial (raising USD 4.5 billion in its latest financing round in 2016), Lufax (raising USD 1.2 billion in its latest financing round in 2016) and JD Finance (raising USD 1 billion in its latest financing round in 2016) have started their IPO plans and have attracted high attention.

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, in essence, is the application of the internet and new technology to the current financial system. Whether they are fintech products or businesses combined with traditional financial business, like banking, insurance and funds, or new businesses beyond traditional financial business, like internet and mobile payment, equity crowdfunding and online lending, they are all regulated by the relevant financial industry authorities and licences are required.

In July 2015, the People's Bank of China ("**PBOC**"), the Ministry of Industry and Information Technology and eight other authorities jointly published the "Guiding Opinions on Promoting the Sound Development of Internet Finance" (the "**Guiding Opinions**"), which is regarded as the "constitution" for internet finance businesses in China. According to the Guiding Opinions, the PBOC regulates online payment, the China Banking Regulatory Commission regulates online lending (including individual online lending and online small-sum loans), online trust and online consumer finance, the CSRC regulates equity crowdfunding and online funds sales and the China Insurance Regulatory Commission regulates internet insurance.

The Guiding Opinions set up the following basic principles for the regulation of internet finance business and various administrative measures have been promulgated to implement the Guiding Opinions:

- internet finance businesses must go through the relevant approval or registration processes with the applicable regulatory authorities and must file with the Chinese telecommunications authorities;
- internet finance platforms must make sufficient information disclosure to customers, including such platforms' operation activities and financial status, business model and risk factors;
- internet finance platforms shall maintain the confidentiality of customers' materials and personal data;
- individual online lending institutions shall maintain their status as information intermediaries which mainly provide information service to the lenders and borrowers, and shall not provide credit enhancement services or conduct illegal fundraising; and
- equity crowdfunding must be carried out via equity crowdfunding intermediary platforms. Only small-sized businesses may raise funds through equity crowdfunding and investors must meet certain qualifications.

3.2 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?

Financial regulators in China are receptive to the development of the fintech industry. The Guiding Opinions and other central government policies clearly stated the authorities' strategic support for internet finance through:

- encouraging traditional financial institutions to cooperate with internet enterprises and create business and product innovation;
- supporting social capital investment in internet financial enterprises, encouraging internet financial enterprises to undertake public offerings and raise capital in domestic capital markets and prompting commercial banks to provide financial support for start-up companies;
- providing preferential financial and taxation treatment; and
- granting internet financial platforms access to the basic financial credit database.

3.3 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 business is highly regulated in China. For a foreign fintech enterprise to access new customers and thus do business in China,

generally it needs to have a business presence. Additionally, various regulatory approvals are required based on the business to be conducted.

Another difficulty for foreign enterprises to access the Chinese market, at least for some sectors, is the vagueness of regulations applicable to foreign investors. Take digital payment permits for example – pursuant to the "Administrative Measures for the Payment Services Provided by Non-financial Institutions" promulgated by the PBOC in 2010, a permit is required for a non-financial institution to provide payment services. The same Administrative Measures also provide that the rules for foreign investments in the payment service sector shall be separately formulated by the PBOC and submitted to the State Council for approval; however, as of now, such rules have not been promulgated yet and thus in practice it is difficult for a foreign enterprise to apply for a payment service permit 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?

The regulations in China related to personal data protection are scattered throughout the Criminal Law, the Tort Law, the Cyber Security Law ("**CSL**"), the Rules on Protection of Personal Data of Telecommunications and Internet Users and other relevant laws and regulations, and mainly apply to businesses holding particularly significant amounts of personal data, including: (i) telecommunications and internet information service providers; and (ii) banks, credit reporting agencies, insurance organisations and consumer finance companies, etc.

The relevant regulations provide two basic principles for the protection of personal data:

- "notification and consent" requirement: prior to collecting personal data from an individual, the relevant business operator must notify such individual of the purpose and proposed usage of the data collected and shall obtain the individual's consent; and
- further responsibilities on businesses holding particularly significant amounts of personal data: in addition to the basic "notification and consent" requirement, businesses holding particularly significant amounts of personal data must take additional measures to ensure the security of such personal data.

Additionally, the General Provisions of Civil Law ("**GPCL**") as adopted on March 15, 2017 also explicitly provides that a natural person's personal data is protected by law and all entities and individuals are obligated to keep secure the personal data they lawfully collect.

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 various regulations relating to personal data protection shall be generally applicable to foreign organisations as long as the collection and use of personal data in China is involved.
- The CSL requires that all personal data collected or created by a key information infrastructure operator ("**KIIO**") in China shall be stored within China, and if it is necessary to transfer such data overseas, a security assessment must be conducted according to measures formulated by the relevant authorities. A KIIO is vaguely defined as any entity whose information leakage may cause damages to national security, public wealth or other public interests.

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

The liabilities for the violation of personal data protection regulations include civil liability, criminal liability applicable to all subjects and administrative liability mainly applicable to businesses holding particularly significant amounts of personal data:

- Civil liability: individuals may be entitled to public apologies from infringers, compensation for damage and distress, rehabilitation of reputation for infringement of privacy.
- Criminal liability: any sale, illegal collection or transfer of personal data may be subject to fines and fixed-term imprisonment for up to seven years. Directors and officers in charge can be held personally liable for offences by entities.
- Administrative liability: businesses may be subject to warnings, fines, confiscation of illegal income and revocation of business licences for any violations.

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

The CSL was promulgated on November 7, 2016 and will become effective on June 1, 2017. The CSL and other relevant laws and regulations jointly regulate internet-related activities, including fintech businesses. In particular:

- all fintech businesses involving personal data are subject to rules regarding the collection and protection of personal data (please refer to the replies to question 4.1 above); and
- all fintech businesses must take sufficient measures to ensure their cyber security including: (i) formulating internal security management systems and operation instructions; (ii) taking technical measures to prevent computer viruses, network attacks and other activities that endanger cyber security; (iii) monitoring and recording network operation and cyber security events; and (iv) taking measures such as data classification and the backing-up and encryption of important data, etc.

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

Anti-money laundering regulations in China are generally applicable to fintech businesses. Specifically:

- the primary AML offence under the PRC Criminal Law is concealing, disguising, converting or transferring the proceeds of crime while knowing or suspecting it to be the proceeds of crime. The offence may take the form of: (i) providing accounts for the proceeds of crime; (ii) assisting with the exchange of proceeds into cash or any financial negotiable instruments; (iii) assisting with the transfer of the proceeds of crime through any funds transfer or any other form of settlement; and/or (iv) assisting with the remittance of the proceeds of crime to other countries. Money laundering offences are subject to fixed-term imprisonment for up to 10 years or criminal detention, or fines of different levels depending on the circumstances;

- the PRC Anti-money Laundering Law imposes AML obligations on financial institutions and certain non-financial-institutions, including establishing proper and comprehensive systems for customer identity verification, retaining customer identity information and transaction records, and a system of reporting large amount transactions and suspicious transactions, etc.; and
- fintech companies are regulated by anti-bribery regulations in the Criminal Law and the Law of Anti-Unfair Competition ("**AUC**") as well. Whoever accepts bribes, offers bribes or introduces bribes may be subject to criminal penalty.

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

Other than those described above, there are no regulations which are specifically applicable to fintech businesses only. Fintech businesses are, however, also subject to regulations generally applicable to business operations in China, such as those relating to consumer rights protection, anti-unfair competition and anti-trust, 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?

The PRC Labor Law and the PRC Labor Contract Law lay down the legal framework for employment matters. Subject to the mandatory employment benefits referred to in our response to question 5.2 below, generally an employer may hire an individual on terms mutually agreed upon between the employer and the individual. There is also a minimum salary requirement, but such requirement is generally easy to satisfy for most industries.

During the term of an employment contract, an employer may not terminate the employment contract without cause, otherwise the employee shall be entitled to choose between specific performance of the employment contract and economic compensation based on the employees' working years.

A particularly onerous requirement for businesses is the "permanent employment contract" rule, according to which an employer shall be obligated to enter into a "permanent employment contract" with an employee under either of the following circumstances: (i) the employee has been employed by the employer for 10 consecutive years; or (ii) the employer and the employee have entered into fixed-term employment contracts for two consecutive times.

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

Employees are entitled to the following mandatory employment benefits:

- working hours: no more than eight hours per day and no more than 44 hours per week;
- paid leave: besides public holidays, marriage or bereavement leave and maternity leave, 5–20 paid days' (depending on the working years) annual leave; and
- social insurance and benefit: employers and employees shall jointly contribute basic pension insurance, basic medical insurance, and unemployment insurance; work injury insurance and maternity insurance are 100% borne by employers. Additionally, employers and employees must jointly contribute to housing funds.

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 employment of foreigners is subject to the employment permit system. Under the relevant rules, any foreigner who plans to work in China shall be at least 18 years old, have no criminal record, have a definite employer and have the professional skills and appropriate vocational experience required for the intended position. China maintains a management system for the employment of foreigners in China, and classifies foreigners employed in China into foreign high-end talent (class A), foreign professional talent (class B) and foreign general personnel (class C). An employer intending to recruit a foreigner must apply to the competent local administration for a "Notification of Foreigner Employment Permit" and a "Foreigner Employment Permit", and those recruited foreigners must apply for a Z visa or an R visa and must apply for resident certificate. The employment permit system also provides a "green channel" for leading talent in the science and technology field, as well as for international entrepreneurs and foreign high-end talent, in order to simplify the approval process for their employment permits.

6 Technology

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

Fintech businesses create financial innovation by using advanced internet technology such as big data, artificial intelligence and block chain and mostly based on the development of computer software, which is protected as copyright. The PRC Copyright Law and the Regulations on the Protection of Computer Software stipulate the attribution, scope, licensing and assignment of computer software copyright, as well as the relevant legal liability in the event of infringements.

As for patent and trademark rights, fintech products are protected by the Patent Law as long as patents are successfully applied for and patent rights are granted by the patent administrative authorities of the State Council. At present, computer software and programs are not eligible for protection under the Patent Law. The registered trademarks of fintech companies and products shall be protected by the Trademark Law.

In addition, the general protection of trade secrets, know-how and scientific and technological achievements are set out in the GPCL, the AUC, the Contract Law, the Criminal Law and other laws.

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

The PRC Copyright Law generally provides that the owner of any copyright shall be its author. As to computer software copyright, the author shall be the software developer, who, as a legal person, has actually organised and directly executed the development of the software, or, as a natural person, has relied on his own means to independently complete the development of the software. As exceptions to the general rule above: (i) copyright of works that are

developed by an employee in the course of employment or mainly utilising the employer's materials and technology, shall belong to the employer; and (ii) copyright of works developed on commission shall belong to the commissioned party unless otherwise expressly agreed.

The PRC Patent Law also provides similar provisions and mechanisms for dealing with the ownership of inventions as the Copyright 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)?

IP rights are territorial rights. In addition to national registrations, IP owners can seek protection in China under the following situations:

- any foreign work not published first in China may enjoy the protection of the PRC Copyright Law if: (i) its author or copyright holder is a national or permanent resident of a member state of the Berne Convention for the Protection of Literary and Artistic Works or any other state with which China has a reciprocal arrangement; (ii) the work is firstly published in a member state to the aforesaid treaty; and (iii) the copyright holder of the work is a business registered in the PRC; and
- patent protection and trademark protection may be achieved via the national route under the Patent Cooperation Treaty ("**PCT**") (for patents) or Madrid System (for trademark). By filing an international application to the competent receiving offices under the PCT and Madrid System, an applicant may seek protection for relevant inventions or trademarks in designated jurisdictions. Upon the grant and registration by relevant authorities in China, the inventions or trademarks filed by the applicant will be protected and enforceable.

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, licence, mortgage or investment.

As a general matter, any IP assignment, licence, pledge or investment must be in writing. Also, it is important to register transactions concerning registered IP rights (assignment, licence or mortgage) with the relevant authorities in order to (i) publicly disclose the assignment, mortgage or licence of the relevant IP right, and (ii) maintain priority as against any third party.

Jinen Zhang
Haiwen & Partners
20/F Fortune Financial Center
5 Dong San Huan Central Road
Chaoyang District
Beijing
China

Tel: *+86 10 8560 6820*
Email: *zhangjinen@haiwen-law.com*
URL: *www.haiwen-law.com*

Mr. Jinen Zhang is a partner at Haiwen and focuses on practice of mergers and acquisitions, foreign direct investment and corporate governance. He advises on all aspects of the financial regulation, e-commerce and data protection. His clients include prominent financial institutions, multinational companies, Internet companies and private equity funds.

Xixiang Lin
Haiwen & Partners
20/F Fortune Financial Center
5 Dong San Huan Central Road
Chaoyang District
Beijing
China

Tel: *+86 10 8560 6977*
Email: *linxixiang@haiwen-law.com*
URL: *www.haiwen-law.com*

Mr. Xixiang Lin is an associate at Haiwen and focuses on practice of mergers and acquisitions, anti-trust and competition law. He advises prominent financial institutions, multinational companies and Internet companies in connection with financial regulation, data protection and competition matters.

HAI WEN
海问律师事务所

Haiwen & Partners is a leading PRC law firm founded in 1992 and is among the first private law firms established in China, which provides a wide range of services to both domestic and international clients in the areas including securities offerings, foreign direct investment, mergers and acquisitions, antitrust, project financing, intellectual property, real estate, international arbitration and litigation. Haiwen's professional services have been widely recognized by its clients, and in the international legal and financial community. Haiwen has been awarded the "National Law Firm of the Year" or the "Best PRC Law Firm of the Year" for our overall practice five times and the "Deal of the Year" for our securities offering and mergers and acquisitions transactions many times by International Finance Law Review. Most recently, Haiwen was awarded the "Financial & Corporate Top Tier Firm" by International Finance Law Review, and the "M&A Firm of the Year" by China Business Law Journal Awards in 2016, and the "Outstanding law firm for Corporate/M&A" by Asia Law in 2017.

Denmark

Morten Nybom Bethe

Gorrissen Federspiel

Tue Goldschmieding

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 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 and is, together with the other Nordic countries, moving fast to embrace global fintech trends.

In general, Danish financial institutions are adapting well to the innovation and digital agenda and are working proactively to promote and provide digital solutions to their customers. Notably, e-payments have taken a turn towards mobile payment following the introduction of Danske Bank's "MobilePay" – an app originally designed to handle and streamline private money transfers, which is now being used as a payment method in shops and e-commerce.

It is, however, not only the financial institutions that are taking advantage of the innovative fintech trends. The Danish fintech scene materialises across a wide palette of financial sub-sectors and digital start-up businesses. Hence, a wide variety of Danish fintech businesses provide digital solutions to companies that support a completely digitalised management of payments, thus enhancing the movement towards a cashless society. Alternate financing methods supported by online platforms have become widespread in the Danish finance sector. Worth mentioning is the emergence of peer-to-peer lending or investment facilitators that enable non-financial actors to offer financial services in competition with traditional financial actors. Similarly, fintech innovation has 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.

Furthermore, other noteworthy Danish fintech innovation trends include online invoice trading, online debt collection, online advisory systems for pension and personal economical overview, as well as mobile-based lending services. The introduction of e-money is gaining more and more attention in the fintech landscape, alongside smart contracts supported by blockchain technology. The implementation of the PSD2 Directive in Danish law is expected to accelerate this trend.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

There is, at present, no specific Danish regulation governing fintech businesses. Consequently, there is no specific regulation prohibiting or restricting such businesses. The conduct of fintech businesses would, 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 ("*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 incentive schemes for investment in neither tech/fintech business 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 is challenged 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 Securities Trading 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"), 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 is covered by the Danish Securities Trading Act.

Nasdaq Copenhagen has also issued certain rules for issuers related to the admission to 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 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?

The Danish digital payment processor Nets Holding A/S was listed on Nasdaq Copenhagen in 2016. Nets is a provider of payment and digital identity services and the IPO was one of the largest Danish IPOs within the last five years. Nets was originally founded by a group of Danish banks as a joint payment systems company. The company later merged with a Norwegian company and became a Scandinavian provider of payment services. The IPO and the exit came just two years after the acquisition of Nets by private-equity-backed companies from a group of Danish and Norwegian banks.

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 at fintech activities, the conduct of such activities must take place within the current framework relating to 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 Danish Financial Supervisory Authority has expressed that the already existing legal framework should cover most fintech models.

The main Danish legislation is contained in the Danish Financial Business Act (general licensing requirements, etc. relating to financial business), the Danish Securities Trading Act (the conduct of securities trading, etc.) and the Danish Payment Services Act. The Danish FSA has expressed that the already existing legal framework covers most fintech models.

3.2 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?

The focus on fintech innovation is relatively new in Denmark and therefore an area subject to rapid development. As fintech is recognised as an important driver for innovation, the Danish Ministry for Industry, Business and Financial Affairs published in April 2016 a policy paper on how the Danish government is seeking to improve the environment for the fintech sector. The focus of the policy paper was especially on how Denmark can benefit from international experiences with respect to the successful implementation of fintech solutions. Further, there was 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 obtain the necessary licences/authorisations. This is, however, a focus on the application process and not the licensing requirements as such.

Further, The Danish Government has initiated two individual projects where one will examine how to strengthen digitalisation, and the other will examine how to improve the environment for start-ups in Denmark. Though the focus of both project lies within

the general perspectives, both are relevant to fintech businesses since these are often start-ups offering new digital solutions to traditional financial services.

3.3 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 constitutes the conduct of 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?

The collection, processing and transfer of personal data are governed by the Danish Act on Processing of Personal Data, implementing Directive 95/46/EC. Accordingly, any processing of personal data undertaken by a fintech or financial service provider established in Denmark will be subject to the Danish Act on Processing of Personal Data. Once the EU General Data Protection Regulation enters into force in May 2018, the provisions of the Regulation will apply to the collection, processing and transfer of personal data in Denmark. In addition, the Danish Financial Business Act also regulates the transfer or use of confidential customer information by a financial service provider.

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?

In line with Directive 95/46/EC, the Danish Act on Processing of Personal Data will apply to organisations established outside the EU/EEA if the organisation, for purposes of processing personal data, uses equipment, automated or otherwise, situated in Denmark, unless such equipment is used only for purposes of transit through the territory of the Community. As of May 2018, when the EU General Data Protection Regulation enters into force, organisations offering goods and services to EU residents will be subject to the Regulation. As a result, also fintech service providers established outside the EU/EEA will be subject to the Regulation when offering fintech services to Danish consumers.

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

Violation of the Danish Act on Processing of Personal Data may result in fines or up to four months' imprisonment (violations by legal entities can only result in fines). The Danish Data Protection Agency's decisions will usually be posted on the Agency's website. The Agency will in most cases require that the data controller takes the necessary steps to rectify the non-compliance before e.g. imposing a fine. However, any non-compliance can in principle be sanctioned as set out above.

While the current level of fines is relatively low, it is expected that the introduction of the EU General Data Protection Regulation will lead to a significant increase in the level of fines.

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

Fintech businesses operating in Denmark will be governed by the security requirements set out in the Danish Act on Processing of Personal Data. Further, depending on the nature of the fintech business, additional security requirements apply (i) to telecom providers under the Danish Act on Net and Information Security, and (ii) to financial service providers under the Danish Financial Business Act and in particular Executive Order on Outsourcing of Material Areas of Activity.

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 will be implemented by end 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 wish as regards the timing of the holiday, including the employee's wish to take the main part of the holiday during the school holiday of the employee's child(ren).

It is normal practice in individual employment agreements and most collective bargaining agreements to provide for additional five 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 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 permit.

The Danish Aliens Act:

The Danish Aliens Act, Consolidated Act no. 412 of 9 May 2016 (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.

Under the Pay Limit Scheme an applicant will further be eligible for a work and residence permit if the applicant has been offered a job with an annual gross salary of no less than DKK 408,000 (February 2017), irrespective of the field or specific nature of the job.

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 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 seen 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 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.

Acknowledgment

The authors would like to acknowledge their colleague Kenneth Kvistgaard-Aaholm for his invaluable contribution to the preparation of this chapter.

Kenneth provides advice to technology-intensive Danish and international clients on patent law, including litigation as well as contractual aspects and IP strategies. He is also engaged in marketing law, franchising and matters relating to the intersection between competition law and intellectual property law. He has extensive experience with Danish and international disputes and transactions concerning intellectual property rights.

Email: kka@gorrissenfederspiel.com, Tel: +45 86 20 75 19.

Morten Nybom Bethe
Gorrissen Federspiel
Axeltorv 2
1609 Copenhagen V
Denmark

Tel: +45 33 41 41 14
Email: mnb@gorrissenfederspiel.com
URL www.gorrissenfederspiel.com

Morten Nybom Bethe provides advises 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
Axeltorv 2
1609 Copenhagen V
Denmark

Tel: +45 33 41 42 03
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 400 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.

Chapter 7

Finland

Niklas Östman

Sonja Heiskala

Roschier, Attorneys 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 within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Finland has an exceptionally long history in fintech having, *e.g.,* pioneered the digitalisation of salary payments in 1965, the debit card system at a nationwide scale already in the 1980s, online banking in the 1990s and mobile micropayments through Nokia Money in 2009. The current fintech landscape in Finland is diverse and evolves fast. As one indication thereof, there have already been bitcoin based ATMs operational in Finland for several years and about 30 businesses in Helsinki ranging from hotels to grocery stores to tattoo parlors accept bitcoin for payment.

While all the larger banks and other financial institutions tend to have their own projects, several startups specialise in payments (*e.g.,* PayiQ, Scrooge, Mistral Mobile and MONI), peer-to-peer lending (*e.g.* FellowFinance, Fixura and Lainaaja), bitcoin and other blockchain-based virtual currencies (*e.g.,* Prasos Oy, Bittiraha.fi, online investment advice or the so-called "robo advisory" (*e.g.,* Taviq, Evervest, and Planago), and crowdfunding *e.g.,* Invesdor, Vauraus, CrowdValley, Fundu, and Mesenaatti.fi). There are also fintech companies specialising in strategic financial planning and risk management (*e.g.,* Detech), and financial data search engines (*e.g.* AlphaSense).

Services designed for small and medium sized enterprises (such as Zervant for invoicing and Arex for smaller-scale financing), and "light entrepreneurship" services for private individuals (such as Ukko.fi) have also gained popularity in the recent years.

In addition to start-ups and smaller companies, also established larger banks continue developing their online applications, *e.g.,* in the field of payments (such as MobilePay by Danske Bank, and Pivo by OP Bank), and venturing into insurance technology (such as OP Syke).

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

Most types of fintech business are subject to regulation in Finland, but none of the established areas of fintech business are completely forbidden.

Some examples of such businesses restricted in Finland include:

Consumer credit. The Finnish Competition and Consumer Authority, along with the Finnish Consumer Ombudsman, supervises offering of products and services to consumers. The Finnish Consumer Protection Act (38/1978, as amended) sets an interest rate cap for credit deals offered to consumers. If the amount of credit, or the credit limit in a credit card, is EUR 2,000 or less, the actual annual interest must not exceed the reference rate increased by 50 percentage points. This also applies to consumer credits that include the right to withdraw cash. Further, the marketing of consumer credit deals must comply with the Consumer Protection Act, and certain information must be included in the advertisement of consumer credit deals.

Investment services. The Finnish Financial Supervisory Authority (FSA) supervises the operations of banks, investment firms and fund management companies providing investment services. Investment services include investment advice, portfolio management, and the reception, transmission and execution of orders relating to financial instruments. Providing certain investment services requires authorisation from the FSA.

Payment services. The Finnish Payment Services Act (290/2010, as amended) sets restrictions to provision of payment services. Generally, payment services can be provided in Finland only by authorised payment institutions or entities that the Finnish FSA approves for provision of payment services. However, there are certain exceptions to these requirements. Recent EU legislation will bring about further changes to regulation of payment services, and is likely to improve the position of smaller payment services providers. The revised EU Directive (EU) 2015/2366 on payment services ("PSD2") must be transposed nationally by January 2018. The Directive will extend the scope of regulation to new types of payment services, and update payment services regulation in line with market developments.

Precious metals. When precious metals are placed on the market in Finland, the Finnish Act on Precious Metals (1029/2000) regulates labelling, and sets restrictions on the allowed concentrations of dangerous substances in the products, and minimum thresholds for the concentration of the precious metal.

See also the fintech regulation specified in question 3.1 of this chapter.

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 Finnish Funding Agency for Innovation (Tekes) finances innovative businesses in Finland, by funding companies from start-

ups and small and medium-sized enterprises to larger companies. Tekes has specific "*Digiboost*" funding programs aimed at small and medium-sized enterprises and Midcap companies seeking to increase their expertise to better utilise digitalisation and to achieve rapid growth in their international businesses.

Sitra, a fund operating directly under the Finnish Parliament, invests in Finnish early stage companies mainly through venture capital funds. Sitra's funding operations consist of corporate investments, fund investments and project funding. In its investment operations, Sitra specifically targets market actors who solve ecological, social and well-being challenges, with many types of fintech businesses potentially eligible.

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 of companies in Finland is fairly neutral, and currently there are no specific incentive schemes specifically for investment in fintech businesses. However, the Finnish state is generally supportive of the increasing development of fintech applications, and there are official initiatives to make Finnish fintech startups more visible globally. For example, the project Export Finland has arranged events jointly with Fintech Circle in London, to promote Finnish fintech companies. Export Finland is a part of public organisation Finpro, which helps Finnish small and medium-sized enterprises to develop internationally and encourages foreign direct investment in Finland.

Recently the Finnish government has also sought to improve the business environment for small and medium-sized enterprises by setting higher minimum limits triggering a company's obligation to pay value added tax.

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

In accordance with the Rules of the Exchange of Nasdaq Helsinki, the following requirements must be satisfied for a business to IPO in Finland. On a case-by-case basis, an entity may be exempted from certain requirements:

- The company must be duly incorporated or otherwise validly established according to the relevant laws of its place of incorporation or establishment.
- The shares of the issuer must: conform to the laws of the company's place of incorporation, and have the necessary statutory or other consents.
- The shares of the company must be freely negotiable. This means that the Articles of Association of the company or any arrangements should not limit the negotiability of the shares.
- The company must have published annual financial statements for at least three years in accordance with the accounting laws applicable to the company.
- In addition, the line(s) of business and the field of operation of the company and its group must have a sufficient operating history.
- The company must demonstrate that it possesses documented earnings capacity on a per business group level.
- The company must fulfil the conditions for sufficient demand and supply in order to facilitate a reliable price formation process.
- The company must have a sufficient number of shareholders, and fulfil the requirement of a sufficient number of shares being distributed to the public under the Nasdaq rules.
- The expected aggregate market value of the shares must be at least EUR 1 million.
- The board of directors of the company must be composed so that it sufficiently reflects the competence and experience required to govern a listed company and to comply with the obligations of such a company.
- The management of the company must have sufficient competence and experience to manage a listed company and to comply with the obligations of such a company.
- The company must have adequate procedures, controls and systems, including systems and procedures for financial reporting in accordance with the Nasdaq rules.
- The company must disclose how it complies with the corporate governance recommendations issued in its home jurisdiction.

Certain requirements are subject to some level of discretion by the Nasdaq Helsinki Exchange, and therefore fulfilling the requirements listed here does not guarantee that the company may proceed with the IPO in Finland.

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

Nokia sold its mobile micropayment business, which had been serving tens of millions of customers in the developing world, to the Indian based FINO in June 2012.

The Finnish fintech application Holvi was sold by its founders to the Spanish bank BBVA in 2016.

Heeros, company specialising in cloud-based financial management software solutions, went through an IPO in 2016, and was the first fintech company in Finland to have completed a crowdfunding round – using the crowdfunding platform of the Finnish fintech company Invesdor – to fund its 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 addition to the restrictions set out above in the question 1.2, certain fintech activities are specifically regulated.

Deposit banks. Only authorised deposit banks can accept deposits from the general public. Such authorisations are granted by the European Central Bank (ECB). The requirements for such authorisation include that the owners and administrative personnel are trustworthy, and that the institution is managed professionally and in accordance with prudent business principles. Also issuance of electronic money falls within the operations regulated under the provisions concerning deposit banks.

Crowdfunding. The Finnish Crowdfunding Act (734/2016, as amended) was adopted in 2016. The act applies to acquiring, offering and professionally mediating loan-based and investment-based crowdfunding, which both seek a financial return, for the purpose of financing business activity. A provider of a crowdfunding service must be registered at the Finnish FSA. Additional legislation may apply to the crowdfunding service, depending on its specific features.

Peer-to-peer lending. Currently the provision of peer-to-peer lending platforms does not typically require authorisation. However, certain types of peer-to-peer lending activities require registration as a credit provider at the Regional State Administrative Agency of Southern Finland.

Bitcoin and other cryptocurrencies. These do not currently fall within the definition of payment instruments in the Finnish Payment Services Act. Cryptocurrencies are therefore regulated as a contract between the issuer and the buyer of the currency, in which relation especially consumer protection obligations may arise. The realised rise in the value of cryptocurrency held by private individuals is taxable income.

3.2 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?

The regulatory environment in Finland is generally open to technological development and digitalisation. Finnish society is known for early adoption of online applications of daily banking services, such as online banking, electronic invoicing, and contactless payment methods. As an example, salary payments in Finland were digitised as early as 1965, and PC-banks were widely used in 1980's for employees in certain sectors.

The Finnish regulators and authorities are mainly receptive and supportive of fintech innovation. However, as the macro-level regulators of the stability of the financial sector, the FSA and the Finnish Ministry of Finance have also publicly emphasised the need for regulation guaranteeing the long-term stability of the financial system at the face of disruptive online technologies.

The Ministry of Finance has set up an expert group to monitor and enhance the conditions for development of financial services technologies. The group seeks to help bring about a diverse financial services ecosystem, and improve the competitiveness of the Finnish financial markets.

In addition, the Finnish Institute of Financial Technology Helsinki ("5th") has been founded by the Ministry of Finance and the Bank of Finland. It coordinates research related to fintech in Finland, and aims to boost the Finnish fintech environment, including fintech startups, financial institutions, IT providers, academia, as well as regulatory and public authorities.

3.3 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?

Provision of certain banking services in Finland require that the service provider is established within the Europan Economic Area (EEA). However, there are several branches of foreign credit institutions operating in Finland. A foreign company may set up a branch in Finland, or provide services across the border without a fixed location in Finland, if it is duly authorised in another EEA country.

Certain fintech services are subject to notification to the Finnish FSA when provided outside of Finland. For example, a foreign payment institution authorised in EEA may also provide payment services in Finland, provided proper notification is made to the Finnish FSA. Investment services may also be provided by certain service providers in the EEA that have a branch office in Finland or have notified the Finnish FSA of their intention to provide services in Finland.

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 Finnish Personal Data Act (523/1999, as amended) applies to all processing of personal data, and is based on the EU Directive 95/46/EC on personal data (Data Protection Directive). The Finnish Personal Data Act applies to all business activity where personal data is processed, such as collected, organised, or disclosed. The obligations set by data protection legislation apply both to the processing of customer data, as well as to the processing of the personal data of the employees within a company. Good data processing principles, such as duty of care, must be observed in all data processing.

It should be noted that Finnish legislation concerning the processing of the personal data of the employee is strict compared to certain other jurisdictions. Finnish legislation restricts, *e.g.,* the employer's access to the employee's e-mail, both during and after the employment. In the processing of employee data, sufficient consents should be obtained from the employees in Finland for the processing of their personal data.

In May 2018, the EU General Data Protection Regulation (EU/679/2016, "GDPR") will replace national legislation based on the Data Protection Directive. The GDPR sets more stringent requirements for data processing, and provides for higher sanctions for breach of data protection legislation. Along with the novel obligations set by the GDPR, the planning obligations set by the current data protection legislation will become more all-encompassing, and thus good data processing practices should be implemented in all stages of processing, from the moment the data is collected, to the moment it is destroyed.

Further, the bank secrecy rules set by the Finnish Act on Credit Institutions (610/2014) restrict the disclosure of financial information of private persons. Under the principle of bank secrecy, an employee of a bank or a credit institution who has obtained information on the financial position or private personal circumstances of a customer, or of any other person, must keep such information secret, unless the person consents to disclosure.

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 Personal Data Act primarily applies to processing of personal data where the so-called "data controller", the entity determining the purposes of the data processing, is established in the territory of Finland. However, the act applies also in cases where the data controller is not established in the territory of a Member State of the European Union, but uses equipment located in Finland in the processing of personal data.

An exception of the application of Personal Data Act in such situations is where the equipment is used solely for the transfer of data through Finnish territory. In such a case the controller shall designate a representative established in Finland.

The Finnish Personal Data Act restricts transfers of personal data outside of the EU or the EEA. Transfers are allowed only on the basis of the conditions provided in the Personal Data Act, and subject to notification to the Finnish Data Protection Ombudsman. Also storage of personal data in a cloud service constitutes transfer of personal data to a third country under Finnish data protection legislation, and requires that the Data Protection Ombudsman is notified of the transfer.

The GDPR will change the scope of application of the data protection legislation. Under the GDPR, any processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU is subject to the GDPR obligations, regardless of whether the processing takes place in the EU or not. The GDPR also applies to the processing of personal data of private individuals who are in the EU, even if the data controller or processor is not established in the EU, where the data processing relates to:

- the offering of goods or services, irrespective of whether a payment of the data subject is required, to data subjects in the EU; or
- the monitoring of the behaviour of data subjects, as far as their behaviour takes place within the EU.

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

The sanctions for failing to comply with the Finnish Personal Data Act include damages, administrative sanctions, and, in the gravest cases, criminal sanctions. In case an activity breaches Finnish data protection legislation, the Data Protection Ombudsman may request that the Finnish Data Protection Board: i) prohibits the personal data processing in question; ii) compels the person concerned to remedy an instance of unlawful conduct or neglect; iii) orders that the operations pertaining to the personal data file be ceased; or iv) revokes a permission to process personal data previously granted by the Data Protection Board.

From May 2018 onwards, the sanctions provided by the GDPR will apply. The most notable new sanction introduced by the GDPR is the power of national data protection authorities to impose considerable administrative fines for breaches. The monetary penalties may reach of up to 4% of the worldwide annual turnover of the entity breaching the GDPR.

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

There are no statutory cybersecurity obligations applicable to fintech businesses operating in Finland, but the authorities such as the FSA may issue guidance specifying the requirements set by the legislative framework.

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

The Finnish Act on Preventing and Clearing of Money Laundering and Terrorist Financing (503/2008) applies to provision of banking services, and is based on several EU directives regulating anti money laundering obligations. The EU directives are based on the guidelines of Financial Action Task Force (FATF), an international standard setter operating under the OECD to combat money laundering and terrorist financing.

The Finnish AML legislation sets the obligations for customer due diligence and a risk-based approach to money laundering and terrorist financing. Providers of financial services have an obligation to monitor customer relationships, use of services, and transactions on a regular basis throughout the lifetime of a customer relationship, to the extent as risk management related to the customer relationship requires.

The fourth and most recent anti money laundering directive (2015/849) must be transposed into national legislation by June 2017, and therefore in Finland there is a comprehensive reform of the Finnish AML legislation ongoing. The most significant change in the current legislation will be the introduction of an obligation to all legal entities to identify and report the beneficial owner of the entity despite the entity having the general reporting obligation under the AML legislation.

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

Consumer protection legislation in Finland sets relatively strict requirements for all provision of services to consumers. Further, the Finnish Act on Credit Institutions sets banking secrecy and customer due diligence obligations for businesses operating as registered credit institutions, including deposit banks and credit societies.

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 Finnish Employment Contracts Act (55/2001, as amended) sets the general framework for hiring and dismissal of staff in Finland. When hiring employees, statutory non-discrimination obligations apply to the employer's decision-making. Dismissal of staff requires a legal basis. The employment of an employee who has neglected or breached his employment duties cannot be terminated before he has been given a warning, and a chance to change the conduct which led to the warning.

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

The Finnish labour market is based on the generally binding collective bargaining agreements for each sector. Collective Bargaining Agreement for the Financial Sector (*Fin: Rahoitusalan työehtosopimus*) applies to a wide variety of jobs in the financial sector, and sets out the employment benefits that are mandatory for employees under the agreement. Depending on the employment duties of an employee, another collective bargaining agreement may apply, in which case different mandatory benefits may be required. Typical mandatory employment benefits under a collective bargaining agreement include vacation time, minimum salary levels, minimum length of lunch and coffee breaks during the working day, and obligations to pay higher compensations under certain special circumstances.

In Finland, the employer is responsible for deducting the employment pension contributions and statutory social security payments from the employee's salary, and transferring them to the Finnish state.

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?

Within the EU and the EEA, the free movement of workers allows EU citizens to freely work in another EU Member State.

For employees coming from outside of the EU and EEA, working in Finland generally requires a residence permit. An employee who has already concluded an employment contract may work in Finland under a residence permit for an employed person, granted by the state of Finland. However, certain highly skilled specialists meeting the salary thresholds set by the Finnish Immigration Service may be exempted from the residence permit requirement.

The conditions set by the collective bargaining agreements apply for foreign and local employees alike. Depending on the type of employment, specific additional obligations such as insurance requirements may apply.

6 Technology

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

Finland is signatory to the Paris Convention for the Protection of Industrial Property ("Paris Convention"), and the Berne Convention for the Protection of Literary and Artistic Works ("Berne Convention"), and protects IP at the level required by these conventions, as also further specified by other applicable regulation such as the TRIPS agreement and various EU directives. The Finnish Patent and Registration Office is responsible for the registration of patents, trademarks, designs, and utility models, whereas the Finnish Communications Regulatory Authority administers the registration of domain names through designated registrars. In addition, business secrets are protected under the Finnish Unfair Business Practices Act (1061/1978, as amended) and also under criminal law.

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

Gaining ownership of "hard" IP, such as trademarks and patents, requires registration. Registered IP is typically subject to annual payments to the national officials responsible for the registers. Certain intellectual property rights, such as copyright, arise without 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)?

Certain IP rights are purely territorial, such as Finnish patents and trademarks which have only been registered in Finland. Finland recognises IP rights that have been registered in the European Patent Office (EPO) or in the European Union Intellectual Property Office (EUIPO), in case the registration at these international bodies includes registration in Finland.

Further, the European patent with unitary effect ("unitary patent") will become an option for innovators besides already-existing national patents and the current European patents. In 2016, Finland ratified the Agreement on a Unified Patent Court. The agreement creates a specialised patent court ("Unified Patent Court", or UPC) with exclusive jurisdiction for litigation relating to European patents and unitary patents. According to estimates by European patent officials, the unitary patent system will be adopted at the earliest in the end of 2017.

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 may use the patented invention, trademark, or copyrighted work, either exclusively or authorise others to use the same through a licence. The IP may also be sold, which is becoming an increasingly common form of monetisation. Most IP rights in Finland provide for the right to seek injunctions against unauthorised use of the IP. There are no particular rules or restrictions for monetisation of IP in Finland, provided that the monetisation of the IP complies with fair business practices, competition law and other the legislation generally applicable to all types of businesses.

Niklas Östman
Roschier, Attorneys Ltd.
Keskuskatu 7 A
FI-00100 Helsinki
Finland

Tel: +358 40 589 7199
Email: niklas.ostman@roschier.com
URL: www.roschier.com

Partner specialised in technology and IP with uniquely broad global experience, given his background. Niklas was previously the General Manager of IP Licensing at Microsoft in the USA, and before that Head of Patent Licensing at Nokia. He has also worked at Quinn Emanuel's Los Angeles office.

On the business side, he has broad experience from both software (app, on-prem and cloud) and cellular (handsets and infra) industries gained in prominent in-house roles.

Niklas has played a key role in creating and operating two IP monetisation programmes that rank among top three in the world. Thus, he has negotiated complex IP and tech transactions with virtually all major software, consumer electronics and telecom companies across the US, EU, JP, CN, KR and TW.

Niklas has led several global patent wars with up to 970 external lawyers involved and been involved in 100s of IP lawsuits all over the world.

Sonja Heiskala
Roschier, Attorneys Ltd.
Keskuskatu 7 A
FI-00100 Helsinki
Finland

Tel: +358 40 966 3532
Email: sonja.heiskala@roschier.com
URL: www.roschier.com

Associate specialised in technology and IP, fintech and protection of personal data. Sonja has a particular interest in the intersection of EU data protection law and innovative online applications such as IoT and fintech products.

ROSCHIER

Roschier is one of the leading law firms in the Nordic region. The firm is well-known for its excellent track record of advising on demanding international business law assignments and large-scale transactions. Roschier's main offices are located in Helsinki and Stockholm, with a regional office in Vaasa. The firm's clients include leading domestic and international corporations, financial service and insurance institutions, investors, growth and other private companies with international operations, as well as governmental authorities.

With some 230 lawyers/practitioners in Finland and Sweden, and a vast network of established relationships with leading law firms, Roschier is internationally recognised as top tier in all of its core practice areas.

Chapter 8

France

Mathieu Françon

Bredin Prat

Bena Mara

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 within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Currently, more than 150 fintechs are operating in France, in particular in the following businesses:

- payment services (including 36 payment institutions and electronic money institutions);
- alternative lending and funding (such as crowdfunding, with 89 crowdfunding platforms);
- 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 with a view to anticipating implementation into French law of the Revised Directive on Payment Services ("PSD2"), even though it has not been formally enacted into French law at this stage.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

So far, there are no particular types of fintech business which are prohibited, but regulated sectors require a licence to conduct business (banking and insurance activities especially) and ongoing compliance with applicable regulations. It can be noted in this respect that the French banking authority has already withdrawn the banking licence of a fintech company acting in the collaborative banking sector pursuant to its general power of sanction, due to the lack of compliance with prudential regulations. Operating without such licence may lead to criminal and civil sanctions for the fintech and their directors as well as regulatory sanctions.

Regarding foreign investors, 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 equity instruments commonly used in France include:

- straight equity (shares); and
- straight, contractually-subordinated, loans.

In practice, equity financing in France generally consists of a combination 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, issuing high yield bonds, using 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 market authority AMF and the banking authority ACPR – see below) have jointly set up a support service in order to provide advice on crowdfunding legislation and rules applicable to fintech businesses with a view to gaining a competitive advantage and to attract foreign investors.

In accordance with SMEs' incentive tax schemes, and under specific conditions, private individuals investing in fintech companies may qualify for tax benefits (deductions or deferrals) in personal income tax (*impôt sur le revenu*, or "IR") and/or wealth tax (*impôt de solidarité sur la fortune*, or "ISF"); entrepreneurs or signatories of shareholders' agreements may, since 1 January 2017, also benefit from tax deferrals on capital gains if the purchase price is used for the direct or indirect acquisition of shares of certain SMEs.

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

The main company types authorised to open their capital on a French stock exchange are French limited companies ("*société anonyme*") or French limited partnerships with a share capital ("*société en commandite par actions*"), 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 French market authority, the AMF;
- companies to be listed on Alternext have to provide two years of accounts, such accounts having only to be certified for the most recent year (and additional half-yearly interim accounts in certain cases), either under IFRS or French accounting standards. The minimum float must represent €2.5 million. The IPO requires preparation of a prospectus cleared by the AMF except in the case of a private placement with qualified investors, when an offering circular that does not need to be cleared by the AMF has to be prepared; or
- for companies listed on the "*Marché Libre*", there are no admission procedures and issuers are not subject to any disclosure requirements. It is, however, recommended to provide accounts for the past two years under IFRS or French accounting standards. There is no minimum marketing amount but the IPO requires the preparation of a prospectus certified by the AMF in the case of a public placement.

It can be noted that the requirements are more stringent for Euronext and Alternext than for the *Marché Libre*.

In order to facilitate access to the 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 few notable exits by founders in France, such as Boursorama's acquisition of Fiduceo, a fintech company specialised, *inter alia*, in account information services. In the meantime, 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 French market authority (*Autorité des Marchés Financiers*, 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 including the application of a lighter regulation to Fintech businesses, FinTech businesses in France do not benefit from a general derogatory set of regulations. The French regulators' approach consists in a personalised assistance of fintechs by providing a comprehensive support in regulation requirements.

However, a specific regime has been set up for crowdfunding actors, creating two specific statuses:

- crowd-sourced investment advisers ("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 ("IFP"), which make available on their website a platform allowing natural persons only to assess a project's investment potential for the purchase of goods or 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 natural person may provide loans of up to €2,000 per project with interest and €5,000 per project without interest. No threshold shall apply in the case of a gift.

As regards other fintech companies, the applicable regulations depend on their business. Specific statuses include, *inter alia*:

- credit institutions, investment services providers, payment institutions or electronic money institutions (requiring a licence); and
- financial investment advisors (*Conseiller en Investissement Financier* or "CIF"), banking or payment service intermediaries (*Intermédiaire en opérations de banque et en services de paiement* or "IOBSP") or insurance intermediaries (*Intermédiaire d'assurance*) (requiring simple registration).

Certain exemptions exist from having to obtain a licence for pursuing payment services or electronic money services.

Meanwhile, it should be noted that companies providing payment initiation services (*Prestataires d'Initiation de Paiement / Initiateurs*) and account information services (*Prestataire d'information sur les comptes / Agrégateurs*) have already been increasing in number outside any specific regulatory framework, as PSD2 is not to enter into force until 13 January 2018.

The licence or registration so granted does not imply an authorisation for "door-to-door" selling, unsolicited commercial contact at home, at work or any other unusual place, which falls under a different specific regulation.

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 or governance practices.

3.2 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?

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. Both regulators are also anticipating the entry into force of PSD2 on 13 January 2018.

In the meantime, the French legislator also appears to be 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 advisors or investment service providers. Such commercial papers may be registered in the books of the issuer individually or registered by shared electronic means (blockchain technology), making France one of the first countries in the EU to legislate on this new technology.

In the same way, the "Sapin II Law" allows the use of blockchain technology for the transfer of shares in non-listed companies under certain conditions. An implementing decree will be published shortly laying the foundations of blockchain technology under French law.

3.3 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, the freedom to provide services and the freedom to establish a branch can overcome these hurdles. 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).

Conversely, for non-EU entities, there are significant hurdles as they must obtain a French regulatory status to carry on fintech business in France if such business is regulated.

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, incorporating EU Directive 95/46/EC into French law, as well as articles 226-16 to 226-24 of the French Criminal Code. Those provisions apply to fintech businesses operating in France to the extent such businesses must process a huge amount of personal data, including sensitive data. Those provisions notably require the data controller to declare to, and/or request authorisation from, the French Data Protection Agency in order to conduct such data processing. Most of this legal framework will, however, be repealed as of 25 May 2018, when the new EU General Data Protection Regulation will enter into force and impose even more stringent requirements on data controllers and data processors.

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 3 of the French Data Protection Law provides that, as a principle, the Law 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 2 of the EU General Data Protection Regulation ("GDPR") – applicable as of 25 May 2018, provides that, as a principle, 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, if the processing relates to: (a) the offering of goods or services to EEA residents; or (b) the monitoring of their behaviour. Under both the French Data Protection Statute and the EU 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.

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, 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.

Data protection regulatory offences in France currently carry a fine of up to €3 million; this amount will be increased to up to €20 million (or, in the case of an undertaking, either up to €20 million or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher) with effect from 25 May 2018 when the EU GDPR comes into force. Criminal data protection offences carry a fine of up to €300,000 and up to five years of imprisonment for private individuals (€1.5 million for legal entities).

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

French data protection laws and the EU GDPR provide that data controllers and data processors must take all appropriate measures, with regard to the nature of the data and the risks of the processing, to protect the data and, in particular, to prevent it from being altered, lost or accessed by non-authorised third parties.

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.

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 implementation of the Fourth EU 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 a strict position on 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 to €1,000 by month, and (iii) the amount of electronic money stocked on a prepaid card to €10,000.

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 hiring his first employee, the employer must inform the labour inspector of the hiring.
- The employer must register his company with the complementary pension funds.
- When hiring a non-French employee, the necessary immigration formalities must be completed.
- The full names of all employees must be recorded in the personnel ledger.
- The employer must arrange for the employee to undergo a medical visit.

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 the 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).
- Severance pay which is provided for by the law, the collective bargaining agreement or, in some cases, the employment contract.

Should the dismissal be held as unfair by a court, 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 a 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 to be hired as an employee by a French Company.

For this purpose, 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 geographic area).

The same applies for transnational posting of workers (i.e. when an employer, usually based outside of France, gives a specific assignment to its employees that has to be carried out in France, with the intention that, once the assignment has been completed, the employees 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 patterns 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 (the "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 part to such conventions, innovations or inventions will filed with the INPI only, and will protect the intellectual property rights associated therewith only 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?

A monopoly of exploitation of IP rights is granted to the owner for a certain duration whereby the owner may 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 their owner and may be also subject to a licence allowing their exploitation.

Acknowledgment

The authors would like to acknowledge Maxime Garcia, associate at Bredin Prat, for his invaluable contribution to the preparation of this chapter.

Tel: +33 1 44 35 35 35. Email: maximegarcia@bredinprat.com.

Mathieu Françon
Bredin Prat
53 quai d'Orsay
75007 Paris
France

Tel: +33 1 44 35 35 35
Email: mathieufrancon@bredinprat.com
URL: www.bredinprat.fr

Mathieu Françon is a counsel specialising in banking and financial regulation. He holds a law degree from the University of Nancy, and a degree in banking risk and regulation from New York University. He is admitted to the Paris Bar.

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.

BREDIN PRAT

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.

Now with 170 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 a renowned competence 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. Christian Schmies

Dr. Susan Kempe-Müller

Hengeler Mueller Partnerschaft von Rechtsanwälten mbB

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 within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

The fintech landscape in Germany is quite broad and diversified. A recent study commissioned by the German Ministry of Finance and published in November 2016 identified 346 fintech companies active in Germany and a broad range of fintech businesses. The main areas in which fintechs in Germany are active are financing (crowdinvestment, crowdlending/P2P lending), asset management (robo advice, social trading, personal finance management); payment services as well as insurtech, with the latter in the meanwhile moving from mere brokerage to actual underwriting. The study showed that all FinTech segments experienced high growth rates in Germany recently.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

There are no specific types of fintech businesses which are at present generally prohibited or restricted in Germany.

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 the largest economy in Europe, Germany has well-developed markets for both equity and debt financing, even though in a country which has traditionally been dominated by bank financing rather than financing through capital markets, the funding of relatively new companies in their early stage through IPOs is less common than in Anglo-Saxon countries. Germany has a very competitive banking sector with a lot of experience in the financing of small and medium enterprises. For those start-ups who may nevertheless not be able to obtain bank financing, there is a multitude of promotional schemes providing financing to new and growing companies in Germany.

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 special incentive schemes both on a federal level but also on a regional level. The German Ministry of Economics has launched the incentive programme "INVEST" under which business angels can be reimbursed for 20% of their investment in start-ups provided they invest at least EUR 10,000. There are furthermore a number of incentive programmes, typically administered or established by the federal promotional bank *Kreditanstalt für Wiederaufbau (KfW)*, such as various "ERP programmes". These programmes offer a wide variety of instruments, including loans on attractive terms, equity capital for start-up and growth companies, co-financings alongside business angels, as well as investments in other funds investing in venture capital. In addition to the programmes on the federal level, there is a wide variety of incentive schemes on a regional level, in particular by the 16 German federal states which typically have their own promotions banks, funds and other programmes.

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

The exact conditions depend on the type of listing and the market on which the shares shall be listed. There are several stock exchanges in Germany, the most important being the Frankfurt Stock Exchange operated by Deutsche Börse AG. The stock exchanges can establish different market segments with "Regulated Markets" being regulated in detail by European and German law in contrast to the "Open Markets" (*Freiverkehr*) regulated mainly by the stock exchanges themselves.

The Frankfurt Stock Exchange offers two market segments in the Regulated Market, namely the Prime Standard and the General Standard. Admission to the general standard requires, among other:

- Valid and audited securities prospectus.
- Reporting history dating back at least three years.
- Probable total price value of at least EUR 1.25 million.
- Number of shares admitted to trading to be at least 10,000.
- Free-float to be at least 25%.

In March 2017, Deutsche Börse launched "Scale", its new segment for small and medium-sized enterprises (SMEs). A listing on "Scale" would include the following requirements:

- Inclusion documents or prospectus.
- Company history of at least two years.
- Estimated minimum market capitalisation of EUR 30 million at the time of the inclusion into trading.
- At least 20% free float or at least 1 million free float share.

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

In June 2016, the Luxembourg-based FinTech My Bucks S.A. completed its IPO on the Frankfurt Stock Exchange. In early 2015, Ferratum, an international provider of mobile consumer loans headquartered in Helsinki, concluded its IPO in on the Frankfurt Stock Exchange. There also have been notable sales of business, such as the acquisition of Fidor Bank AG by the French BPCE.

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 legal framework for fintech business in Germany. Rather, depending on the services such business offers, such services may qualify as a regulated activity under general German financial regulatory laws. The German Banking Act provides for a licensing requirement for banking activities and investment services and the catalogue of regulated activities in some respects goes beyond the underlying European Directives. For example, in Germany any form of lending on a commercial basis, including loans to corporates, is subject to a licensing requirement as is leasing and factoring business. Payment services are subject to a licensing requirement under the German Payment Services Supervisory Act and the management of investment funds is regulated under the German Capital Investment Code. Given the comprehensive and still expanding nature of financial regulation, careful analysis of applicable regulatory regimes is indispensable prior to starting any fintech business in Germany.

3.2 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?

Financial regulators and policy-makers are generally receptive to fintech innovation and technology-driven new entrants to the financial services markets. This has been manifested in various ways recently. Most recently, the German Ministry of Finance in March 2017 established the German FinTech Council which shall advice the Ministry on fintech matters. Also prior to this, the Ministry of Finance documented its interest in fintech by organising events and also commissioning a comprehensive study on the German fintech market which was published in late 2016. BaFin has also intensified its fintech relates activities significantly recently and, among other, provides dedicated information for various fintech business types on its website.

3.3 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 the administrative practice of the German financial regulator BaFin, service providers domiciled abroad but actively targeting the German market by offering financial services (including banking, investment, payment and insurance services) to clients domiciled in Germany are generally subject to German financial regulatory law, including its licensing requirements. Therefore, before accessing the German market from abroad it is crucial to analyse whether licensing requirements are triggered by such activities.

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 in Germany is regulated by the Federal Data Protection Act 1977/2003 (*Bundesdatenschutzgesetz*) ("FDPA"). The purpose of the FDPA is to protect the individual against his/her right to privacy being impaired through the handling of his/her personal data. The FDPA implements the European Data Protection Directive (95/46/EC).

Fintech organisations established in Germany which are "data controllers" (*Verantwortliche Stelle*) (defined as person or body collecting, processing or using personal data on his or its own behalf or commissioning others to do the same) are regulated by the FDPA. Their obligations primarily relate to:

- Appointment of data protection official: Prior to the use of automated data processing procedures, data controllers shall appoint a data protection official (*Datenschutzbeauftragter*) or shall register such automated data processing procedures with the competent supervisory authority.
- Compliance: A data controller is under a duty to comply with several data protection principles, for example, (i) to collect, process and use data only if permitted by law or with the consent of the data subject, (ii) to reduce the collection, processing and use of personal data and to render it anonymous as far as possible, (iii) to collect data directly from the data subject, (iv) to collect data only for specific purposes which have to be made transparent, and (v) to use collected data for advertising purposes only in limited cases.

The German data protection regime is currently viewed as one of the more individual-friendly European data protection regimes. However, the European (including German) data protection regulatory regime is changing. From 25 May 2018, the General Data Protection Regulation ("GDPR") will replace the FDPA in substantial parts, and the FDPA will only apply to a very reduced extent. The GDPR has direct effect in all EU Member States and is a more prescriptive and restrictive regime. For example, it includes further mandatory breach notification provisions, higher monetary sanctions, and imposes obligations not only on controllers but also on data processors (those who process on behalf of a data controller).

The use of data for unsolicited direct marketing by electronic means is governed by the Act against Unfair Competition (*Gesetz gegen den unlauteren Wettbewerb*). For internet services of fintech organisations, the collection and use of data is also regulated by the Telemedia Act (*Telemediengesetz*). Both acts are again based on EU Directives. In addition, sector-specific provisions, i.a. the Banking Act (*Gesetz über das Kreditwesen*), the Payment Services Supervision Act (*Gesetz über die Beaufsichtigung von Zahlungsdiensten*), the Act on the Supervision of Insurance Undertakings (*Versicherungsaufsichtsgesetz*) 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 FDPA applies to data controllers which are established outside the EU and EEA, and which collect, process or use personal data in Germany (except for transit). The GDPR has a slightly narrower 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.
- The FDPA and GDPR both restrict the transfer of personal data outside the EEA unless adequate protection is in place. There are different ways to obtain adequate protection, including using standard contractual clauses 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 is a range of sanctions available, including:

- Regulatory action – fines of up to EUR 300,000 can be issued for certain breaches of the FDPA (administrative offences). When determining the fine, the financial benefit derived from the breach shall be taken into account. Fines under the GDPR will be higher (up to 4% of annual worldwide turnover or EUR 20 million, whichever is greater). All individual circumstances are to be considered when determining the fine, including measures taken to ensure compliance with data protection laws.
- Criminal liability – certain administrative offences, e.g. the collection or processing of personal data without authorisation, are criminal offences if committed intentionally and in exchange for payment, or with the intention of enriching oneself or another person or of harming another person. Liable for criminal offences are natural persons, e.g. in corporations directors, managers or officers.
- Damages claims – individuals may be entitled to compensation for damages caused by unauthorised processing or other breaches of the FDPA. Liability can be avoided if the entity which breached the data protection laws can demonstrate that it took all due care as required by the circumstances. The claim for damages provided by the FDPA has seen little practical relevance so far. Damages for immaterial losses or compensation for personal suffering are not granted under this claim. However, there may be claims under tort law for infringement of personal rights, which often can be enforced more easily. The GDPR has a wider reach, providing for compensation for material and non-material damages.
- Cease and desist claims – if personal data of consumers are unlawfully collected, processed or used, i.a. the Injunction Act (*Unterlassungsklagegesetz*) provides for claims for cease and desist as well as for elimination. These claims can be asserted by consumer organisations and similar associations.
- Deletion right – the FDPA provides data subjects with claims for the correction, deletion and blocking of personal data.

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

There are various laws and regulations relating to cyber security which may apply to fintech business operating in Germany:

- Various BaFin circulars impose minimum requirements for IT security on financial service providers. Most recently, in March 2017, BaFin released a draft circular on "Banking Regulatory Minimum Requirements applicable to IT". The new circular specifies in more detail IT requirements which already in the past have been addressed by BaFin in more general circulars addressing minimum requirements for risk management by financial institutions.
- Special requirements apply to internet payments. A BaFin circular on Minimum Requirements for the Safety of Internet Payments (*Mindestanforderungen an die Sicherheit von Internetzahlungen)* ("MaSi") establishes a number of minimum requirements in the area of the security of internal network payments. This circular applies to the provision of payment services offered via the internet by payment service providers as defined in Article 1 of the PSD. The MaSi preempts some of the requirements under PSD II which is currently being implemented in Germany and also contains sector-specific requirements regarding cyber-security, in particular the obligation to notify serious IT incidents to BaFin.
- On a more general level, the German IT-Security Act (*IT-Sicherheitsgesetz*) came into force in July 2015. The Act sets out several obligations to protect IT-Systems and digital infrastructure in Germany which apply to all operators of critical infrastructures. Critical infrastructures include power and water supply systems, the healthcare sector, the telecommunication sector but also certain parts of the financial system infrastructure.

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

The German Anti-Money Laundering Act (*Geldwäschegesetz*) contains a catalogue of entities subject to AML requirements, which notably include credit institutions, investment firms and payment services providers. To the extent fintech business qualify as one of the entities listed in the AML, they will be subject to AML and related requirements as any other entity. The German AML Act is generally based on European law and, in particular, obliges relevant entities to identify their contractual counterparties and economic beneficiaries of transactions, to monitor business relationships on an ongoing basis, to notify suspicious transactions and to implement organisational measures for the prevention of money laundering and financial crime, including the appointment of an AML officer.

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

There is no specific other regulatory regime that applies to fintech business in Germany but such business would be subject to the laws of general application to the operation of business in Germany, such as, for example, laws dealing with unfair competition or antitrust.

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 Germany, employers are generally free which terms and conditions they offer to prospective employees. However, job advertisements as well as the other steps in the hiring process must not be discriminatory. The Documentation Act (*Nachweisgesetz*) requires that the employer notifies the employee in writing of the essential terms of the employment no later than one month after the stipulated commencement of employment. No such notification is necessary where the parties have entered into a written contract of employment which contains the required particulars.

In addition to the terms and conditions under the individual employment agreement, the terms and conditions of employment may also be determined by collective bargaining agreements (if applicable) and by works council agreements (if a works council has been established for the relevant establishment).

Contracts of employment can be terminated by either party by giving notice of termination. The notice of termination must be in written form to be valid. If no applicable collective bargaining agreement provides otherwise, the statutory notice periods have to be observed as a minimum. The statutory notice period is four weeks to the fifteenth or the end of the month at the beginning of the employment and increases with the length of service of the employee to be terminated (from one month after two years of service to seven months after 20 years of service, the termination to become effective only at the end of a calendar month) (Civil Code (*Bürgerliches Gesetzbuch*), s. 622). Statutory notice periods are minimum notice periods and cannot be contracted out. Longer notice periods may be agreed upon between the parties, but the notice period for a termination by the employee must not be longer than the notice period for a termination by the employer. No notice periods need be observed where there is good cause (*wichtiger Grund*) justifying immediate termination (Civil Code, s. 626).

The right of the employer to terminate a contract of employment has been severely restricted by statutory law. The Termination Protection Act (*Kündigungsschutzgesetz*) in general protects all employees who have been in service with the terminating employer for more than six months, provided the employer employs more than 10 employees in the relevant establishment (or, with respect to employees who were hired before 1 January 2004, five employees). Any ordinary termination of a contract of employment with an employee who enjoys protection under the Termination Protection Act is invalid, unless the employer can show that the termination is 'socially' justified. As a rule, 'social justification' is deemed to exist only if the termination is caused either by reason of the person or behaviour of the employee or by urgent business reasons which prevent the continuation of the employment. The existence of a works council (*Betriebsrat*) will complicate a termination by the employer even further because the works council has to be heard prior to giving notice (Works Constitution Act, s. 102, para. 1). The works council may consider the termination within a period of one week and raise objections but, ultimately, it cannot block a termination.

Certain classes of employees, such as works council members, disabled employees, pregnant women or employees who took parental leave, enjoy additional special protection against termination.

Additional legal requirements apply if the employer intends to implement mass redundancies and a works council exists which represents the relevant employees. In such case, a so-called compromise of interests as well as a social plan must be negotiated with the competent works council. The compromise of interests will provide for a plan of action, i.e. regulations as to whether, when and how the mass redundancies may be implemented. The social plan will provide for regulations to mitigate the financial disadvantages for the affected employees, typically including severance payments.

Neither the statutory notice periods nor the Termination Protection Act will apply if an employment contract has been entered into for a limited period of time. Such a contract will automatically terminate at the end of its agreed term. However, the agreement on a limited duration is only valid if an acceptable reason for the limitation exists (as defined in s. 14 of the German Act on Part-Time and Time-Limited Employment (*Teilzeit- und Befristungsgesetz*)), such as work on a temporary project, or if a new employee is hired for a period not to exceed two years and if it has been agreed upon in writing.

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

The Minimum Wage Act (*Mindestlohngesetz*), which has become effective on 1 January 2015, provides that a certain minimum wage must be paid to all employees in Germany. Since 1 January 2017, the minimum wage amounts to EUR 8.84 gross per hour. Every two years, an adjustment of the minimum wage amount shall be resolved upon by the government.

Further, employees are mandatorily subject to the German social security system, which comprises health and nursing care insurance, pension insurance as well as unemployment insurance. The contributions to the social security system are about evenly shared between employer and employee, i.e. the costs of the employer's contributions come on top of the costs for the employee's gross remuneration. The social security contributions amount to slightly above 40% in total (employer's and employee's) share, provided that certain contribution ceilings apply.

Other different laws to protect employees exist. Among others, the Act on Continued Remuneration (*Entgeltfortzahlungsgesetz*) entitles employees to six weeks of continued remuneration in case of absence from work due to illness and the Federal Holiday Act (*Bundesurlaubsgesetz*) defines minimum standards of holiday entitlements (at least four weeks of paid holidays annually in addition to public holidays). Further, employees may have a claim to be granted parental leave, or to work part-time unless certain exemptions under the German Act on Part-Time and Time-Limited Employment apply.

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 Germany, no specific regulations regarding the requirement of a permission to work apply to fintech businesses.

The taking on of an employment (be it as employee, freelancer or other service provider) by a citizen of a Member State of the European Union is generally unrestricted. The same principally applies to citizens of the Member States of the European Economic Union and of Switzerland. The taking on of an employment by citizens of other countries generally requires a respective permission as part of the residence permission (Residence Act (*Aufenthaltsgesetz*), s. 4), unless an intergovernmental agreement or legislative ordinance provides for an exemption.

6 Technology

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

Any innovations and inventions made in the fintech business will typically concern software, computer programs and sometimes databases. Software, computer programs and databases are works protected by copyright under the German Copyright Act (*Urheberrechtsgesetz*, GCA) provided that they are the result of a personal intellectual creation. This requires a certain originality ("*Schöpfungshöhe*") which is usually given with regard to computer programs. Databases are protected if they require a substantial investment.

Computer programs "as such" are excluded from patentability. However, certain program-related inventions might be patentable.

The branding of the software product can be protected by trademarks. Certain elements of the design of the websites, in particular texts, graphics and pictures can be protected by copyrights if they have the required level of originality.

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

Under German copyright law, the owner of the copyright is the author of the work which can only be a natural person. Copyrights cannot be registered in Germany and they cannot be transferred, only by way of inheritance. Any 'transfer' of copyright amounts to a full exclusive licence. Legal entities therefore have to take licences over all use rights, which always leads to a licence chain back to the author.

Copyrights in employees' works are commonly understood to be fully licensed to their employer by virtue of their employment contract and under statutory interpretation rules, unless the nature of the employment relationship indicates otherwise. For computer programs, the GCA explicitly sets out that the employer is exclusively entitled to assume all commercial exploitation rights, unless agreed otherwise. There are no such general rules for consultants, freelancers, shareholders, directors or suppliers so that a legal entity needs licensing clauses for safe exploitation.

A patent for an invention is owned by the inventor. With regard to service inventions made by an employee in the course of his employment, the mandatory provisions of the German Act on Employee Inventions (*Arbeitnehmererfindergesetz*) apply which contain certain requirements regarding the notification and claiming of inventions.

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, but certain IP rights offer EU-wide protection. A trademark can be registered as European Union trademark with protection for the entire European Union. A design can be protected as (registered or unregistered) Community design right with an EU-wide scope of protection. The owner of a European Union trademark or a Community design can enforce his claims in national courts which are designated as Community courts and which can grant EU-wide claims for injunctive relief. They are also entitled to award damage compensation for infringing acts committed in other jurisdictions on the basis of foreign law.

The protection of a German patent and the German part of a European patent only relates to Germany. It is likely that a new unitary patent right, the Unitary Patent (UP), which will offer protection in up to 26 EU Member States, will come into force in late 2017 together with a centralised enforcement system, the Unified Patent Court, providing cross-border enforcement for UPs as well as for European Patents.

German citizens and certain other persons treated as such enjoy copyright protection for their works irrespective of the place where the work has been published. With regard to foreign citizens the scope of protection for their works is governed by international treaties, in particular the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) and the WIPO Copyright Treaty (WCT) which both deal with the protection of copyrights for software and databases.

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

The assignment, granting of security interest and licensing of trademarks, patents and designs do not require a particular form. The registration of the transfer of title or the granting of the security interest in the respective register of the German Patent and Trademark Office (DPMA) is not constitutive but only of declaratory nature. The registration of a licence in the register of the DPMA is only possible with regard to exclusive patent licences.

Copyrights as such cannot be transferred, but it is possible to grant licences. The GCA does not set out special requirements for copyright licences to be valid. Written form is only required for licences in unspecified future works and over currently unknown forms of use. The owner of a copyright licence can grant security rights with regard to such licence with the consent of the author.

Dr. Christian Schmies
Hengeler Mueller Partnerschaft von Rechtsanwälten mbB
Bockenheimer Landstraße 24
60323 Frankfurt am Main
Germany

Tel: +49 69 17095 975
Email: christian.schmies@hengeler.com
URL: www.hengeler.com

Christian is a partner in the Frankfurt office of Hengeler Mueller. Christian advises a broad range of financial market participants on financial regulatory matters with a focus on asset management and payment services.

Dr. Susan Kempe-Müller
Hengeler Mueller Partnerschaft von Rechtsanwälten mbB
Bockenheimer Landstraße 24
60323 Frankfurt am Main
Germany

Tel: +49 69 17095 399
Email: susan.kempe-mueller@hengeler.com
URL: www.hengeler.com

Susan is a counsel in the Frankfurt office of Hengeler Mueller. Susan advices financial institutions, internet companies and other principals on data protection law, IT and intellectual property matters (both contentious and non-contentious).

HENGELER MUELLER

Hengeler Mueller is universally recognised to be one of Europe's pre-eminent law firms. It is dedicated to absolute quality of legal advice, the highest standards of service, and to delivering the most creative and efficient solutions designed to optimise clients' business objectives. The prerequisite: an independent partnership of professionals; entrepreneurial both in thinking and practice; international both in education and training.

Hengeler Mueller is a long-term market leader in banking and financial regulatory law in Germany with about 15 partners in its banking and finance department. Hengeler Mueller is the first contact for clients facing complex legal issues. Partners of Hengeler Mueller have broad experience in advising all types of financial market actors and frequently advice service providers domiciled outside of Germany with respect to their access to the German market.

The firm advises on all major M&A transactions for financial as well as strategic investors.

Chapter 10

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 within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Hong Kong has been steadily making efforts in recent years to become a fintech hub.

It was one of the early adopters of "stored value facilities" (prepaid instruments with monetary value). Currently, there are 13 non-bank licensees authorised to operate stored value facilities in Hong Kong, including Tencent, Alipay, Paypal and Octopus cards, with two banks issuing or facilitating stored value facilities. The last round of licences was granted in November 2016, demonstrating a continuing interest to further develop the stored value facilities landscape.

In November 2016, the Hong Kong Applied Science and Technology Research Institute ("**ASTRI**") published a whitepaper commissioned by the Hong Kong Monetary Authority ("**HKMA**") on the application of distributed ledger technology ("**DLT**" or "block chain") to financial services in Hong Kong. ASTRI will publish a second whitepaper on DLT in the latter half of 2017.

The HKMA has also recently spearheaded other initiatives to encourage the development of fintech, including (amongst others):

- the 'Fintech Innovation Hub' (a collaboration between the HKMA and ASTRI), which was announced in September 2016 and intends to be a platform for the banking and payment industries to conduct proof of concept trials of products and services through new technologies. It also gives regulators an opportunity to provide early input into the trials before their implementation; and
- the 'Fintech Supervisory Sandbox', which allows banks to conduct testing and trial of new technologies without full compliance with HKMA's usual supervisory requirements. Its purpose is to permit banks to collect data and feedback in a controlled environment before the final launch.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

No particular fintech businesses are prohibited or restricted (except that fintech businesses in the gambling sector are effectively prohibited under Hong Kong gambling legislation).

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 below 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?

While not specifically tailored to fintech businesses, the government's Innovation and Technology Fund offers various funding programmes, including a HK$2 billion Innovation and Technology Venture Fund for co-investment with private funds in local technology start-ups and a HK$500 million Technology Voucher Programme, under which local SMEs are encouraged to make use of technological solutions to improve productivity and business processes. HK$10 billion has been earmarked in the 2017 Budget for developing the technology sector, with fintech being a key focus area.

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

Listing conditions depend on whether a business intends to list on the Main Board or the Growth Enterprise Market ("**GEM**") Board of The Stock Exchange of Hong Kong Limited ("**SEHK**").

Weighted voting rights, a common feature in technology companies, are not currently permitted by the SEHK. However, the SEHK

reportedly plans to consult the market on the launch of a third board in a bid to attract more technology companies to list in Hong Kong – whether alternative voting structures will form part of the consultation remains to be seen.

Main Board

For a listing on the Main Board, an applicant 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$200 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.

Minimum Market Capitalisation

At least HK$200 million at the time of listing.

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$50 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, with the key differences being:

Financial Requirement

The applicant must have a trading record of at least two financial years comprising:

1. positive cashflow of at least HK$20 million in aggregate immediately preceding the issue of the listing document which is generated from ordinary course of business; and
2. market capitalisation of at least HK $100 million at the time of listing.

Minimum Market Capitalisation

At least HK$100 million at the time of listing.

Public Float

The same 25% public holding applies, but with market capitalisation of at least HK$30 million in public hands.

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 many high profile exits by founders of fintech businesses in Hong Kong thus far, two noteworthy fintech IPOs are anticipated in 2017.

Lufax, one of China's largest p2p lenders, is reportedly preparing for a Hong Kong IPO before the end of 2017.

Ant Financial, the operator of Alipay and an affiliate of Alibaba, is considering a Hong Kong IPO in the first half of 2017. In April 2016, it secured funding of US$4.5 billion, the world's largest private fundraising round for an internet company at the time.

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 Securities and Futures Commission ("**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.

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 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 ("**ICO**")

  The ICO provides no person shall carry on any class of insurance business in or from Hong Kong unless authorised to do so.

3.2 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?

Financial regulators and policy-makers in Hong Kong are receptive to fintech. The government established the Steering Group on Financial Technologies in April 2015 to advise on Hong Kong's development into a fintech hub. Banking, securities and insurance regulators have each set up dedicated fintech offices to deal with regulatory enquiries, as well as a cross-regulatory collaboration group with representatives from each of the three fintech offices.

The HKMA's supervisory approach to fintech is risk-based and technology neutral. It has established a Fintech Facilitation Office ("**FFO**") to act as an interface between market participants and the HKMA, creating a platform for exchanging fintech initiatives and initiating research in potential application and risks of fintech solutions. Four major projects have been launched by the FFO thus far:

- the Cybersecurity Fortification Initiative launched in May 2016 has developed three key pillars: (i) the Cybersecurity Resilience Assessment Programme; (ii) the Cybersecurity Intelligence Sharing Platform; and (iii) the Professional Development Programme (the initiative is further discussed at question 4.4);
- a comprehensive study on DLT as noted in question 1.1 above;
- the Fintech Innovation Hub as noted in question 1.1; and
- the Fintech Supervisory Sandbox as noted in question 1.1.

The SFC's approach to fintech is also technologically neutral. It is open-minded about licensed corporations and new entrants deploying technologies that achieve the right results under its rules and standards. It has established a Fintech Contact Point and has recently broadened its focus to include "regtech".

The Office of the Commissioner of Insurance ("**OCI**") has established a Fintech Liaison Team to enhance communication with businesses involved in the development and application of fintech. It facilitates the fintech community's understanding of the current insurance regulatory regime and act as a platform for exchanging ideas of fintech initiatives among key stakeholders.

3.3 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 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 ICO 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 also 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'.

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 or 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 cyber security 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.

The HKMA recently launched several significant measures to strengthen cyber resilience in the banking sector, putting Hong Kong on par with international standards. The "Cybersecurity Fortification Initiative" aims to raise the level of cybersecurity among banks in Hong Kong and will provide an improved framework for banks to evaluate risk exposure to help ensure better prevention and detection of cyber security incidents. 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 recently 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.

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 at question 3.1 above, the AMLO imposes on financial institutions (including licensed corporations, banks and others authorized institutions and insurance companies) customer due diligence and record-keeping requirements, while DTROP, OSCO and UNATMO require 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 unions 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?

There is a statutory minimum hourly wage (at HK$34.5 with effect from 1 May 2017) which applies to most workers in Hong Kong.

The 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.

Note 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.

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.

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 tests.

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 are 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. The international registration of marks under the Madrid Protocol does not currently apply to Hong Kong.

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 Companies Registry within a month in order to protect against creditors.

Acknowledgment

The authors would like to acknowledge their colleagues Peter Lake and Roger Cheng for their invaluable contribution to the preparation of this chapter.

Peter Lake is a Partner in our Hong Kong office. He 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 2017 edition of *Who's Who Legal Banking: Finance* in Hong Kong, and as a leading lawyer in the *IFLR 1000 Asia Pacific 2017* for Banking and Finance in Hong Kong. He is recommended in *Chambers Asia-Pacific 2017* for Banking & Finance, and Financial Services: Non-contentious Regulatory (Hong Kong-based international firms, China).

Peter co-authored the Hong Kong chapters of 'The Asset Management Review' 2015 edition, 'The Banking Regulation Review' 2015 edition and 'The Lending and Secured Finance Review' 2015 edition.

Tel: +852 2521 0551 / Email: peter.lake@slaughterandmay.com.

Roger Cheng is a Partner in Slaughter and May's Hong Kong office. He has been involved in general corporate financing and commercial work, including mergers and acquisitions, securities transactions, joint ventures and corporate borrowings.

Tel: +852 2521 0551 / Email: roger.cheng@slaughterandmay.com.

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, corporate finance transactions, 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. Benita is listed as a top tier lawyer in *Chambers Asia-Pacific 2017*, *The Legal 500 Asia Pacific 2017* and the *IFLR 1000 2017* for Capital Markets and Corporate/M&A.

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 20 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) in *Chambers Asia-Pacific 2017*, the *IFLR 1000 Asia Pacific 2017* for Private Equity, and is recommended in *the Legal 500 Asia Pacific 2017* for Investment Funds.

Jason co-authored: the Hong Kong chapters of The Asset Management Review 2015 edition, The Mergers and Acquisitions Review 2015 edition, the European Lawyer publication Hedge Funds Jurisdictional Comparisons 2013 edition; and The Practitioner's Guide to the Listing Rules of the Hong Kong Stock Exchange. 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 and Hong Kong.

SLAUGHTER AND MAY

Slaughter and May has a long-standing presence in Asia and we opened our office in Hong Kong in 1974. We have extensive experience of a wide range of work involving Hong Kong, the People's Republic of China and Asia.

In particular, we are familiar with the challenges facing clients in the fintech sector, having been involved in various transactions for financial institutions, global technology companies, trading platforms, investors and start-ups. Our experience includes advising: Zhong An Online P&C Insurance (China's first internet insurance company which was co-founded by Alibaba Group Holdings, Tencent Holdings and Ping An Insurance) 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 investment in, and O2O joint venture with, Intime Retail (Group) Limited and its acquisition of SCMP Group Limited.

India

Kosturi Ghosh

Trilegal

Preethi Srinivas

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 within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

The fintech sector in India has grown rapidly in the past few years. What started as a small foray into mobile payments, has now become a vibrant and innovative market. Reports indicate that the fintech sector in India is set to touch around USD 2.4 billion by 2020 from the current USD 1.2 billion. The industry covers e-wallets, insurance, banking, security and biometrics, and peer-to-peer lending. Blockchain is still in its nascent stages in India but is slowly gaining momentum. There has been a major uptick in the e-payments space after demonetisation of 83% of India's currency. Reports indicate that the use of digital payments has increased by up to 300% after demonetisation.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

Currently, there are no express prohibitions or restrictions on the fintech businesses generally. However, 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, companies, that are owned and controlled by residents can make an application to set up payment banks in India.

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 funding are generally available for new and growing businesses in India. Given the current business landscape, venture capital, private equity and venture debt are the preferred equity and debt funding options. Angel investors also fund start-ups in this space. External Commercial Borrowing can also be availed from a non-resident lender. Public offerings could also be made to raise funds from the market. Crowdfunding is an unconventional method of funding. Incubators have begun to play a particularly important role for start-ups in this space. Reports indicate that approximately USD 4 billion was invested in Indian start-ups in 2016.

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 has launched the 'Start-up India' initiative to develop an ecosystem which is conducive for growth of start-ups and to provide assistance in funding. The Government has launched various tax relief schemes which include three years of income tax exemption for start-ups. A National Credit Guarantee Trust Company has also been set up to provide funding for 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.

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

The Securities and Exchange Board of India (**SEBI**), the Indian capital markets regulator, has, in addition to the general rules for capital raises, also prescribed regulations for issue of specified securities by small and medium enterprises (**SME**) 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 1.5 million or whose post issue face value capital is more than approximately USD 1.5 million and up to approximately USD 3.7 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 issue made by SMEs should be one hundred percent underwritten and the minimum application size in terms of number of specified securities should be at least INR 100,000 (USD 1,520).

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 few acquisitions in the fintech space where the founders have exited their company. One notable transaction is where PayU, an online payments company, acquired Citrus Pay for around USD 130 million in cash, leading to one of the biggest cash exits in the payments sector. Another notable transaction was the acquisition of Momoe, a mobile based payments firm by ShopClues, an online marketplace, in a cash and stock deal. Chennai based Financial Software and Systems Private Limited's plans to undertake an IPO was deferred due to the unpredictable market conditions after demonetisation.

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 Reserve Bank of India (**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 network and pre-paid instruments (wallets). Regulations are now being developed and modified by the regulators for fintech businesses which include peer-to-peer lending and blockchain.

3.2 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?

The regulators and the policy makers are generally cautious when it comes to any change in the heavily regulated financial services sector. However, realising the importance and the need for innovation and technology, especially concerning cyber security, they 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 RBI has recently set up an inter-regulatory working group to, *inter alia*, (a) study and understand fintech innovations, (b) assess the opportunity and the risk to the financial systems on use of financial technology, and (c) realign the regulatory framework for increasing fintech opportunities and managing risk.

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 the customers without involving the physical movement of cash. Further, the Government is making efforts to promote non-cash transactions in India and this is also reflected in the initiatives proposed by the Government 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.

3.3 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 its 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 from 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?

The Information Technology (Reasonable Security Practises and Procedures and Sensitive Personal Data or Information) Rules, 2011 (**Privacy Rules**), regulate body corporates or any persons 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*' has been defined to mean personal information that contains information relating to passwords; financial information; physical, physiological and mental health condition; sexual orientation; medical history and records and biometric information. Further, any use or transmission of the 'Unique Identification Number' (**UIN**) which is treated as sensitive personal information would also be subject to the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (**Aadhaar Act**) and the corresponding regulations.

With the boost to digital transactions by the Government, the Ministry of Electronics and Information Technology felt the need to regulate the various PPIs operating in India and has issued draft Information Technology (Security of Prepaid Payment Instruments) Rules, 2017, for public comments. It is now proposed that the issuers of PPIs will have to, *inter alia*, disclose their privacy policy

on their website or mobile app, ensure end-to-end encryption of data exchanges and undertake customer identification and authentication.

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. 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 a 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 been also made punishable with imprisonment for a term extending to three years or with fine extending to approximately USD 8000, 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 or penalty amount will be approximately USD 400.

The Aadhaar Act, *inter alia*, prescribes penalty for disclosing identity information. If a person intentionally discloses, transmits, copies or otherwise disseminates any identity information collected in the course of authentication to any person not authorised under the Aadhaar Act, he will be punishable with imprisonment of a term of three years or with fine of approximately USD 150 or, in the case of a company, with a fine of approximately USD 1,500. Further, any contravention of the Aadhaar Act for which a specific punishment is not provided under the Aadhaar Act, is punishable with imprisonment which may extend to one year or with a fine of approximately USD 400 or, in the case of a company, with a fine of approximately USD 1,500.

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) hacking a computer system, data alteration, (b) sending offensive material through communication service, (c) violation of privacy, and (d) cyber terrorism. 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 frauds, 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. The CERT-In currently operates as (i) 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.

Further, the draft Information Technology (Security of Prepaid Payment Instruments) Rules, 2017, require 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 or 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. Per the PMLA, a 'Reporting Entity' is required to maintain records of, *inter alia*, clients, transactions and furnish information to the authorities. 'Reporting Entity' includes a banking company, financial institution and intermediaries such as investment advisor and merchant bankers. If a fintech company qualifies as a 'Reporting Entity' under the PMLA, all the obligations imposed on such entities must be met. In addition to the above, the financial regulators also prescribe certain additional know your customer requirements and mandate entities regulated by them to have adequate information and data security infrastructure to prevent and detect fraud.

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, the applicable tax and exchange control regulations whilst operating in India. Exchange control regulations in India govern all transactions between persons resident in India and persons resident outside India, including minimum capitalisation requirements and 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 applicability of most employment statutes varies depending on several factors which include, the number of employees in an establishment, nature of activity carried out by the organisation, type of workforce engaged by the establishment and the wages earned by the employee. As many labour legislations cater to the concept of a 'workman', it is important to identify if any employee falls under the definition of a workman as it plays a vital role for a variety of reasons, such as, determining termination compensation, changing terms and conditions of employment, formulating employment policies, etc. The Industrial Disputes Act, 1947 defines a 'workman' to mean 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 managerial or supervisory capacity. Further, several labour legislations require employers to obtain various licences to operate, e.g. every commercial establishment is required to obtain a licence from the state Shops and Establishments Acts.

As regards to termination, statutory minimum notice periods on termination of employment, and a number of statutory severance payments such as gratuity, retrenchment compensation, payable at the time of termination are prescribed under labour legislations. Courts in India do not normally recognise the concept of 'at will' termination of employment as termination should be for a 'reasonable cause'. Some state Shops and Establishments Acts expressly require an employer to provide a 'reasonable cause' for the termination. 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, (c) by mutual agreement, (d) upon the employee's retirement/superannuation, and (e) on expiry of the term of the contract.

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

Indian social security legislations primarily address contingencies that may arise due to stoppage or reduction on earnings, maternity, employment injury, occupational diseases and death. The social security legislations cover 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 fund. Non-contributory labour statues 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 the case of death or disablement of employee. Labour statues in India also cover leave and holidays. Certain establishments must also comply with the maternity benefit laws which, *inter alia*, prescribes conditions regarding maternity leave and imposes restriction 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 Patent 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 new form of known substance, (iii) mathematical, business method, computer program or algorithm, (iv) performing mental act or method of playing 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. Since computer programmes are *per se* not patentable, they can be protected as 'literary work' under the Copyright Act, 1957 (**Copyright Act**) as long as they are original.

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

The legislative framework in India protects trade marks, patents, copyright, designs and layout designs. Patents need to be registered under the Patents Act. Copyright does 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 was 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 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) Trade marks protect brands names, logos, sounds, colours and 3D shapes.

b) Patents protect patentable inventions.

c) Copyright protects original literary, dramatic, musical work, computer program, artistic work, cinematographic film, sound recordings.

d) Designs protect the shape, configuration, pattern, and appearance of products.

e) Layout designs protect the layout design of semi-conductor 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 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 addition to the courts, IP tribunals have been set-up to hear cases for rectification and cancellation of registered IP.

An unregistered trademark is protected under common law. A claim for passing-off can be initiated in the courts for protection of unregistered trademarks and designs. The courts have recognised trans-border reputation in passing-off actions concerning trademarks. Private parties can also resolve their disputes regarding IP through the WIPO arbitration and mediation centre.

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 should 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 license 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 license agreement must be registered with the patent office. Any unregistered assignment or license agreement cannot be used as evidence of transfer of title. The Government may also grant compulsory licence under various situations which include national emergencies. The Copyright Act also stipulates certain conditions for assignment and license 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 license of IP is regulated under the foreign exchange regulations on current account transactions and capital account transactions 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 4699
Email: Kosturi.Ghosh@trilegal.com
URL: www.trilegal.com

Kosturi Ghosh is Partner at Trilegal and Deputy Head of the corporate practice group of the firm. 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.

Preethi Srinivas
Trilegal
The Residency, 7th Floor
133/1, Residency Road
Bengaluru
Karnataka 560025
India

Tel: +91 80 4343 4699
Email: Preethi.Srinivas@trilegal.com
URL: www.trilegal.com

Preethi Srinivas is an Associate in the Bangalore office of Trilegal and is part of the Firm's corporate practice group.

Preethi focuses on regulatory, joint ventures, and other corporate and commercial matters. She has been involved in advising companies on structuring investments in India, conducting due diligences, drafting and reviewing transaction documents and advising private companies on general corporate matters.

TRILEGAL

Trilegal is one of India's top-tier law firms with offices in five of India's major cities – Mumbai, New Delhi, Gurgaon, Bangalore and Hyderabad. We represent clients on a large number of the most complex and high-value transactions in India, leading to our key practices winning 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

David Dawborn

Hiswara Bunjamin & Tandjung
(in association with Herbert Smith Freehills LLP)

Vik Tang

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 within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

The fintech sector in Indonesia is relatively new and still very much developing. That said, Indonesia is widely perceived as an untapped market for fintech opportunities. This is largely due to its population of over 250 million people and growing mobile smart phone and internet penetration. With only about 25% of the population possessing bank accounts, innovative fintech services are seen as being in line with the Indonesian Government's long-term policy goals of promoting financial inclusion and the development of small and medium-sized enterprises. The rise in the number of fintech start-ups in Indonesia over the last few years, particularly in the online payment services space, is closely tied with the growth of the Indonesian e-commerce sector.

Indonesian fintech start-ups remain at an early stage of development, but cover a broad range of activities including (i) payment, (ii) lending (including peer-to-peer), (iii) financial aggregation and comparison services, (iv) accounting, (v) point of sale services, (vi) crowdfunding, (vii) investment, (viii) cryptocurreny, (ix) personal finance, and (x) insurance.

Most Indonesian fintech businesses are engaged in payment services, including e-money, e-wallet and payment gateway. Financial comparison services form the second largest segment, followed closely by lending services (which comprises peer-to-peer lending platforms and marketplaces for financial products).

Importantly, we are currently also beginning to see traditional banks and telecommunications companies exploring new ways of providing digital financial services (such as mobile banking and unsecured lending based on data analytics) which are giving rise to new regulatory challenges.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

There are currently a number of restrictions and/or requirements in the fintech sector, including the following, which are chiefly aimed at:

- protecting customers – through the application of adequate prudential and risk management principles. For example, under Bank Indonesia ("**BI**") Regulation No.18/40/PBI/2016 on Operators of Payment Transactions Processes ("**BI Regulation 18**"), fintech companies engaged in "payment system services" business activity (e.g. e-wallet, e-money, payment gateway services providers) are required to have sufficient internal policies on and a team responsible for risk management. Further consumer protection measures are expected as financial regulators say stricter policies are needed to protect the public from fraud and ensure their personal data is not sold or shared without their consent;
- anti-money laundering requirements – through the requirement to have a face-to-face KYC verification process for on-boarding new clients in certain areas of financial services products (e.g. credit cards and e-money), although this is gradually liberalising for certain business platforms; and
- supporting the growth of the local fintech businesses – through foreign ownership limitations imposed on certain fintech sectors. For example, the foreign ownership for fintech "lending operators" (i.e., peer-to-peer lending) is set at a maximum of 85%. In the payment sector, a maximum foreign ownership limitation of 20% applies to companies performing the roles of "principals", "switching operators", "clearing operators", and "final settlement operators".

BI Regulation 18 also prohibits payment system providers to process payment transactions using crypto or virtual currencies. Note that BI does not, through this regulation, prohibit the use of virtual currencies, but rather prohibits payment system providers, who are licensed by BI, to *process* payment transactions using virtual currency. BI does not recognise cryptocurrencies (such as Bitcoin) as valid currency in Indonesia. Nevertheless, while the uptake has been slow compared with other jurisdictions, Bitcoin providers and users do exist in Indonesia and therefore it remains to be seen whether the prohibition to process payment using cryptocurrencies will remain in place (and be strictly enforced) or the restriction will be slowly relaxed 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)?

In general, there are several types of funding available to growing fintech companies in Indonesia including equity injections or debt instruments. In practice, we are seeing venture capital investors, local conglomerates and banks/telcos currently investing in this sector.

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, no. Current Indonesian regulations in the fintech sector do not provide for any special incentive schemes. But given that the fintech sector in Indonesia is relatively new and still developing, it is possible for such schemes to be implemented in the future.

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

There are two listing boards on the IDX: (1) main board (*papan utama*); and (2) development board (*papan pengembangan*). In brief, the key listing requirements in Indonesia are:

a. Main board:
- be an Indonesian limited liability company (*perseroan terbatas*);
- have three-year track record in the current core business;
- have audited financial statements for the last three financial years, with the last two years and any interim period having received an unqualified auditor report; and
- have net tangible assets of at least IDR 100 billion.

b. Development board:
- be an Indonesian limited liability company (*perseroan terbatas*);
- have one-year track record in the current core business;
- have audited financial statements covering at least 12-month period and any interim period having received an unqualified auditor report; and
- have net tangible assets of at least IDR 5 billion.

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, not yet. As mentioned, the fintech sector in Indonesia is relatively new and still very much developing. Indonesian regulators are starting to catch up with developments on the ground by issuing new regulations and guidelines. Existing regulations and guidelines are also being fine-tuned to suit market conditions. We have seen increased activities by both local and foreign start-up fintech companies seeking to obtain the necessary licences (or amendment of their existing licences) to carry out their business in Indonesia.

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 sector in Indonesia is very much still in its infancy, with developments in the sector itself outpacing the ability of regulators to regulate the various activities that fall under the umbrella term "fintech". At the time of writing, regulators have issued specific 'fintech regulations' in relation to the use of e-money activity, e-wallet, payment services providers (e.g., payment gateway) and peer-to-peer lending services only.

E-money

E-money activity has existed in Indonesia for around 10 years and was first regulated by BI under BI Regulation No. 11/12/PBI/2009 on Electronic Money, which was most recently amended by BI Regulation No. 18/17/PBI/2016 in August 2016 (collectively, the "**E-Money Regulation**"). In 2016, BI also issued two circular letters providing further guidance on the E-Money Regulation. The E-Money Regulation defines, among other things, the roles of service providers that make up the E-Money process (i.e. principals, issuers, acquirers, clearing processors and final settlement operators) and sets out the risk management and prudential principles applicable to each category (as well as foreign investment restrictions, where applicable).

Online payment

In November 2016, BI issued BI Regulation No. 18 and Circular Letter No. 18/41/DSKP on online payment transactions providers. BI Regulation 18 complements existing BI regulations regulating payment, clearing, and settlement activities by both banks and non-banks and focuses on, among other matters, the regulation of operators providing electronic wallet (or "**e-wallet**") services and payment gateway services.

Lending

The December 2016, IT Lending Regulation is the most recent fintech regulation to be issued in Indonesia and relates to peer-to-peer lending. The IT Lending Regulation focuses on marketplace lending, governing matters such as foreign ownership limit, lending platform operation, the requirement to have a data centre in Indonesia, and the indirect restriction to use the financed shareholders arrangement to establish fintech lending operators.

3.2 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?

Fintech regulatory developments are still at a relatively early stage in Indonesia. However, the broad outlines of the institutional landscape for the proposed fintech regulatory framework are already beginning to take shape. In general terms, the main regulator in this area is likely to be the Financial Services Authority (or OJK), with the exception that issues relating to payment are likely to be regulated primarily by the Indonesian central bank (or BI). It is also important to bear in mind the regulatory role played by the Ministry of Communication and Informatics ("**MOCIT**"), which in broad terms regulates telecommunications and information technology-related matters. Accordingly, certain aspects of the fintech industry may fall under MOCIT's regulatory remit. The Indonesian Foreign Investment Coordinating Board ("**BKPM**") is also likely to have a role in this space in certain situations involving foreign investors, as BKPM regulates foreign investment generally (with certain notable exceptions, for example, in the financial services sector).

Indonesian regulators are broadly receptive to fintech innovations and new technology-driven entrants as they see these innovations as being in line with the government's long-standing policies of promoting financial inclusion and promoting small and medium-sized enterprises. In the last six months or so, the regulators have publicly expressed their intention to provide a comprehensive set of regulations governing the sector, as it is recognised that such regulatory framework is necessary in order to underpin consumer and investor confidence in the sector (although this currently remains a work in progress). This is manifested through the various regulations which have recently been issued by OJK and BI, which primarily relates to peer-to-peer lending and payment system operators.

Given the existence of multiple regulatory bodies with potentially overlapping functions, we envisage that in the immediate future the evolving regulatory framework is likely to be complex and hence a case-by-case analysis is advisable when considering the regulatory framework applicable to new products and business platforms in this fast-evolving sector in Indonesia. That said, there is reason to be optimistic that the regulators in Indonesia will eventually find a workable balance between promoting a nascent (but rapidly growing) industry which has the potential of significantly addressing Indonesia's long-term financial inclusion policy objectives, and at the same time addressing the need to create a sound regulatory framework which takes into account prudential corporate governance principles in the financial services sector (including risk management and consumer protection aspects).

3.3 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?

BKPM, as the main regulator of foreign investment in Indonesia, generally requires all business activities conducted in Indonesia to establish a foreign owned company in Indonesia. However, based on current regulations, if a fintech business is operated entirely from offshore (i.e., no employees, no office space in Indonesia, no revenue paid into an Indonesian bank account, and no physical marketing activities within the territory of Indonesia, etc.) then it is unlikely that such activity will attract scrutiny from BKPM under current regulations (although tax may still be an issue – see below).

One noteworthy development in this regard is the release of the Draft OTT Regulation by MOCIT in April 2016. We understand from recent statements of MOCIT officials that, under the draft regulation, offshore entities which provide services over the internet (including entities with no physical presence in Indonesia) and gain revenue from transactions performed in the territory of Indonesia may be required to (i) incorporate a company in Indonesia, or (ii) appoint an Indonesian company as its representative to conduct all of its activities in Indonesia on its behalf ("**Onshore Requirement**"). There is very little detail on the nature of this requirement including (i) whether certain revenue threshold must be reached for the Offshore Requirement to apply, and (ii) whether there will be any exemptions (the Draft OTT Regulation is very broadly drafted). Furthermore, it is unclear when the Draft OTT Regulation will come into force and whether or not the Onshore Requirement will be retained in the final version of the official OTT Regulation. The Draft OTT Regulation is driven in part by the Indonesian government's recent drive to increase the overall tax revenues of the government, and foreign entities deriving Indonesia related revenue from outside Indonesia is seen as tax leakage from the government's perspective.

Note also that from the perspective of the Indonesian financial services regulator ("**OJK**"), any regulated activity in the financial services sector (including for example peer-to-peer lending) will be required to be licensed in Indonesia. Likewise, from the perspective of the Indonesian central bank ("**BI**"), activities relating to certain types of payment services and e-money or e-wallet may require to be licensed in Indonesia. This is quite a complex and evolving area at the moment and a case-by-case approach is advisable.

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, there is no single umbrella data protection law in Indonesia. However, there is currently a bill waiting to be passed by the legislature. Under the bill, a commission to supervise the management of personal data will be established by the government, and transmission of personal data to outside Indonesia is restricted unless the designated countries can be deemed as having a similar level of protection towards personal data as Indonesia.

In the meantime, data protection is regulated under a number of piecemeal laws and regulations. One of the more significant legal instruments is Law No. 11 of 2008 on Electronic Information and Transaction as amended by Law No. 19 of 2016 ("**Law 11/2008**"), which is further implemented by, among others, Government Regulation No. 82 of 2012 on Management of Electronic System and Transaction ("**GR 82/2012**") and MOCIT's Regulation No. 20 of 2016 on Data Protection in Electronic Systems ("**MOCIT Reg 20/2016**"), collectively referred to as "EIT Regulations".

The provisions of the EIT Regulations apply to "electronic system operators" ("**ESOs**"). The definition of ESO is very broad and, in our view, could capture fintech companies. The EIT Regulations impose various data protection obligations on ESOs including that personal data must be protected and used in accordance with the consent of the personal data owners.

The IT-Based Lending Regulation and BI Regulation 18 (referred to above) also impose similar obligations on Fintech Lending Companies, payment gateway operators, and e-wallet operators. These regulations also provide for data centre localisation requirements.

Note that banking regulations also provide a separate data protection regime as it applies to banks.

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 wording of the EIT Regulations is not restricted to domestic application. Therefore, at least in theory, the data privacy measures set out under the EIT Regulations could apply to overseas organisations. However, based on current regulations, as mentioned above, if a fintech business is operated entirely from offshore (i.e. no employees, no office space in Indonesia, no revenue paid into an Indonesian bank account, and no physical marketing activities within the territory of Indonesia, etc.) then it is unlikely that such activity will attract regulatory scrutiny for failure to comply with data privacy measures set out in the EIT Regulations. Note, however, that if an online platform operated by an offshore entity becomes prevalent in the Indonesian market it will likely attract increasing attention from local regulators.

We note also that Article 22 of MOCIT Reg 20/2016 requires that any transfer of personal data outside of Indonesia to be coordinated with the Minister or the relevant government bodies. It currently remains unclear how this will be implemented in practice.

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

Article 36 of MOCIT Reg 20/2016 provides for administrative sanctions ranging from written warning to temporary suspension of operational activities. In addition to the sanctions provided by MOCIT Reg 20/2016, under the IT-Based Lending Regulation and BI Regulation 18, non-compliance with data privacy obligations may result in the imposition of sanctions ranging from written warning to revocation of business licence.

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

Broadly speaking, Indonesia's current cyber security framework is regulated under the EIT Regulations mentioned above under question 4.1. There are currently no other Indonesian laws or regulations which deal specifically with cyber security. In 2010, the Indonesian government introduced the Bill on Information Technology Crimes, but this has never been passed into law. In January 2017, media outlets reported comments from Indonesia's Coordinating Minister for Political, Legal, and Security Affairs General Wiranto that establishment of a National Cyber Agency is "all but certain" and will take place in the near future. There is currently little additional detail as to the nature and mandate of this proposed agency.

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

Both the IT-Based Lending Regulation and BI Regulation 18 prohibit fintech businesses from being involved in money laundering, terrorism, and/or other financial crimes. The regulations require that fintech businesses prepare an internal standard anti-corruption and bribery operating procedure ("**ABC Internal Procedure**"). There is, however, very little detail provided under the regulations as to the form and substance required for a company's ABC Internal Procedure.

The IT-Based Lending Regulation and BI Regulation 18 do not provide specific criminal sanctions. However, failure to comply with the obligations to provide ABC Internal Procedure may subject the company to a range of administrative sanctions from written warning to revocation of business licence.

Other than the above, banks who are considering entering the fintech sphere should also note the AML and anti-terrorism financing requirements set out in BI Regulation No. 14/27/PBI/2012 on Implementation of AML and Prevention of Terrorism Funding by Commercial Banks and its implementing circular.

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

At the time of writing, the fintech regulations mentioned above are the only regulatory measures aimed specifically at fintech businesses.

However, broadly speaking BKPM foreign investment registrations, MOCIT regulations may be applied to certain types of fintech business in certain situations. Note also that, certain aspects of financial services regulations (administered by OJK) as relates to banks (and other regulated entities under the financial services regulatory regime) may also be applicable depending on the regulated entity in question. In addition, certain central bank regulations (administered by BI) which relate to payment services and e-money/e-wallet, may also be applicable in certain situations for both banks and non-banks.

Indonesian regulators are also continuously assessing the landscape and the need for additional or more specific regulations. Accordingly, this sector must be monitored closely and new business models should be considered on a case-by-case basis.

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 Indonesia, employment-related matters are primarily governed by Law No. 13 of 2003 on Manpower ("**Manpower Law**") and its related regulations. In broad terms, the Indonesian employment regime is favourable with respect to employees and in general it is difficult to dismiss employees.

The following key points are commonly considered by both foreign and local employers:

a. Hiring of employees

   (i) probationary period – while indefinite employment agreements can provide for a probationary period, it is not allowed under fixed-term employment agreements. The probationary period cannot be more than three months; and

   (ii) fixed-term employment – fixed-term employment agreements can be entered into for one-time or temporary work, short-term work (not more than three years), seasonal work, or work involving new products or activities or products that are still being tested. They must satisfy certain requirements (e.g. in writing in Indonesian language). The Minister of Manpower and Transmigration Regulation No. Kep. 100/MEN/VI/2004 on Implementation of Fixed-Term Employment Agreement ("**MOM Reg 100/2004**") also provides that fixed-term employment agreements must be registered with the relevant manpower office where the employer is domiciled.

b. Dismissal of employees – dismissal of an employee under Indonesian law must be voluntarily agreed by the employee, unless in cases where the employee is still serving his probation or has committed a serious violation (e.g. fraud or embezzlement). There are also certain reasons that cannot be used by an employer to dismiss an employee, e.g. sickness of less than 12 consecutive months or marriage. When dismissing an employee, the employer must also pay severance package in accordance with the requirements set out in the Manpower Law (the terms of which are generous).

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

The Manpower Law provides for the following mandatory benefits:

a. at least 12 days of annual paid leave to employees who have worked for 12 consecutive months; and

b. the Manpower Social Security Programme (*Program Jaminan Sosial Ketenegakerjaan*) and Health Social Security Programme (*Program Jaminan Sosial Kesehatan*) – every employee, including expatriates, who has worked for more than six months in Indonesia must be registered

as a participant of these programmes. Both employees and employer contribute to these programmes, with the percentages of their contributions set by the government (and subject to change from time to time).

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 foreign nationals who wish to work for fintech businesses in Indonesia. Therefore, the requirements under the relevant manpower regulations relating to expatriates would apply. Some of the requirements are:

a. work permit – the employer must first obtain an approval and permit to employ an expatriate. Once that is satisfied, the employee then has to apply for a temporary residential permit;

b. expatriate to Indonesian employees ratio – the current regulations are silent on the permissible ratio. Prior to 23 October 2015, the permissible ratio was 1:10. Although the current regulations are silent, based on our experience, the Ministry of Manpower may apply its own unwritten internal policies on a case-by-case basis, and hence an employer planning to hire expatriates is well advised to have prior discussions with the MOM; and

c. restrictions on position and employment period – expatriates cannot be employed to hold certain positions (e.g. human resources director) and cannot be employed as permanent employees.

In general, the process of bringing in foreign employees into Indonesia is not straightforward and takes time. Hence, advance planning in this regard is advisable.

6 Technology

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

Innovations and inventions are protected in Indonesia by different intellectual property rights, including trademarks, copyright, patents, trade secrets and industrial designs. These rights are regulated under a set of Intellectual Property Rights regulations.

Indonesia joined the World Trade Organization (WTO) in 1994 when it ratified the Agreement on Trade-related Aspects of Intellectual Property (TRIPs Agreement). To date, Indonesia has also ratified most major international IP agreements, including the Paris Convention and the Berne Convention.

In relation to fintech, copyright arguably extends to computer code, user interface features, audio, video guides, and other works. The technology brand may include a word mark, logo, or icon protected as trademarks. Industrial designs can be used to protect the 'look and feel' of physical articles such as electronic cards, transaction machines, as well as computer interfaces and icons. The underlying core technology may also be protected by a combination of patent and trade secret rights.

Each fintech company and each innovation need to be assessed on a case by case basis to determine the appropriate mix of intellectual property protections.

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

Trademark, patent, and industrial design rights are secured by way of registration with the Indonesian Directorate General of Intellectual Property Rights ("**DGIPR**").

Trade secrets and copyright do not have to be registered. Trade secrets are automatically the subject of legal protection provided that the information in question meets certain requirements (i.e. it is not known by the public, has economic value when used in business activities, and its confidentiality is maintained by its owner). Copyright protection also arises automatically upon the creation a copyrightable 'work', but it is still recommended to register copyrights with the DGIPR for stronger protection.

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)?

A national right needs to be owned to be protected under the IP laws and regulations in Indonesia. Indonesia does not recognise 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?

Parties can monetise IP in Indonesia by way of licensing arrangements. There are no restrictions regarding royalty arrangements. However, the licencing agreement must not (i) create any economic loss in Indonesia, (ii) inhibit the development of technology, or (iii) contravene prevailing laws, public order, or morality.

***

David Dawborn
Hiswara, Bunjamin & Tandjung
23rd Floor, Gedung BRI II
Jl. Jend. Sudirman Kav 44-46
Jakarta 10210
Indonesia

Tel: +62 21 574 4010
Email: david.dawborn@hbtlaw.com
URL: www.hbtlaw.com

David is a Herbert Smith Freehills (HSF) Partner heading the firm's specialist Indonesian practice. He is seconded to HSF's associated Indonesian law firm, Hiswara Bunjamin & Tandjung in Jakarta and leads a team of HSF lawyers dedicated to Indonesian transactions, financial and securities sectors and projects. He has practised in Jakarta since the early 1990s and is consistently ranked by global legal directories as one of the leading foreign lawyers practising in Indonesia. He is fluent in Bahasa Indonesia, both spoken and written. He advises a broad range of cross-border, corporate and financial transactions. He also has extensive experience advising on employment and manpower matters for foreign investors. In addition, David regularly supports the firm's specialist Indonesian disputes resolution practice in relation to strategic and commercial aspects of regulatory investigations and dispute proceedings based on his long involvement and experience with Indonesian matters.

Vik Tang
Hiswara, Bunjamin & Tandjung
23rd Floor, Gedung BRI II
Jl. Jend. Sudirman Kav 44-46
Jakarta 10210
Indonesia

Tel: +62 21 574 4010
Email: vik.tang@hbtlaw.com
URL: www.hbtlaw.com

Vik is a Partner at Herbert Smith Freehills on a permanent secondment arrangement to Hiswara Bunjamin & Tandjung in Jakarta. He graduated with a first class degree in law from Oxford University. Prior to joining Herbert Smith Freehills, Vik worked for nine years at a 'magic circle' firm in London and specialises in public and private M&A, private equity and joint ventures. Prior to Jakarta, Vik spent four years in Herbert Smith Freehills Singapore office working on South East Asia cross-border M&A transactions. He has broad experience in cross-border transactions involving the UK, Europe, Asia and the Middle East, with particular specialisation in Indonesia. He has also been seconded to Morgan Stanley (for a year) in London. Vik is fluent in Bahasa Malaysia, and has a good working knowledge of Bahasa Indonesia (both spoken and written).

HISWARA BUNJAMIN & TANDJUNG

in association with HERBERT SMITH FREEHILLS

Hiswara Bunjamin & Tandjung ("**HBT**") is a leading commercial and corporate law firm in Indonesia. It currently has seven partners, one Senior Counsel and around 60 associates, as well as several international counsel from our associated international firm, Herbert Smith Freehills LLP ("**Herbert Smith Freehills**"), who are permanently seconded to HBT.

We regularly advise some of the largest corporations and financial institutions in relation to a wide range of Indonesian matters, including banking regulatory issues, financing, employment, disputes, capital markets, and M&A. We are a leading law firm in the technology and fintech sector and have been regularly receiving instructions on fintech-related matters in the past few years from start-ups, financial institutions, investors, and telecommunications companies.

We provide high quality, innovative legal services of an international standard based on informed and commercially relevant local knowledge. All of our partners are experienced Indonesian corporate and commercial lawyers with many years of experience in advising clients across all major Indonesian market sectors.

Chapter 13

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 within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Dublin is now a "*booming FinTech hub*". Change in the financial services sector in Ireland is being driven by digitalisation in consumer banking and disruptive technology. New entrants to this sector are developing innovative business models that are testing the parameters of the current financial services framework. These include services relating to electronic money, intermediation of payments and payment channels, the aggregation of financial services data, raising capital through peer-to-peer platforms and crowdfunding, financial cyber security, the facilitation of price comparisons in connection with retail financial products and the emergence of blockchain technology. 2016 saw particular disruption in the payments sector with established institutions being bypassed through the use of technology-driven payment processes such as PayPal, Stripe and TransferMate. Recent lending innovations include alternative credit models, use of non-traditional data sources and the emergence of data analytics and auto being used to price risks and reduce operating costs.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

There are no prohibitions or restrictions that are specific to fintech businesses in Ireland.

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

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 over €100 million in the first three quarters of 2016. Irish financial services organisations have set up venture funds and a number of fintech incubation and acceleration projects which offer funding in return for an equity percentage (see our answer to question 2.2).

Debt

In addition to the traditional lending from financial institutions for small and medium businesses, there are increasing 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 the Grid. The speed at which funds can be raised makes this a particularly attractive option.

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 attractively low corporate tax rate in Ireland of 12.5% is a major incentive for start-ups or companies looking for a location for their business investments. Some other attractive features of Ireland's IP tax code include the R&D tax credit regime, the stamp duty exemption on IP transfers, the key employee reward mechanism, the double taxation agreement network (which will be phased out in 2020) and the 6.25% tax rate, under Ireland's knowledge development box, on profits arising from certain IP assets which are the result of qualifying R&D activity carried out in 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-Up Fund (CSF)**: This fund offers €50,000 equity investment in return for a 10% equity stake. Calls are made throughout the year for specific sectors, and in May 2016, a specific fintech CSF was announced which was open to companies in payments, banking, regtech, security, insurtech and other fintech solutions leveraging blockchain, internet of things, artificial intelligence and data intelligence.
- **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.

Other Government-backed schemes include:

- the **StartUP Refunds for Entrepreneurs (SURE)** initiative, which 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; and
- the **Employment and Investment Incentive (EII) Scheme**, which 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 and this essentially depends upon the scale of the business and the funding required by the company. The precise listing rules differ in respect of the different markets. The Irish Stock Exchanges (**ISE**) offers four markets: the Main Securities Market (**MSM**), 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 Enterprise Securities Market (**ESM**), which suits smaller companies (minimum market capitalisation of €5,000,000) in the early stages and therefore 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 the MSM (the principal market in Ireland) include:

- 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 as least €1,000,000 for shares and €2,000,000 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 €115,000,000 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 2017 will see increased M&A activity within the fintech space. In particular, 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 Central Bank of Ireland (**CBI**) to conduct business. If authorised, the firms will be subject to Irish legislation and various ongoing CBI requirements.

Payment institutions, electronic money institutions (**EMIs**), investment companies and money transmission businesses are examples of business models which may require authorisation. The legislation which is most likely to apply to fintech businesses is the Payment Services Regulations 2009, which governs payment institutions, and the Electronic Money Regulations 2011, which authorises an undertaking to issue E-money.

Fintech business may also be subject to consumer protection legislation, and CBI codes of conduct, as well as anti-money laundering and data protection legislation, depending on the services that they are offering.

3.2 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?

The CBI is becoming increasingly aware of the positive impact financial services can have on a country as a whole and the regulatory environment surrounding this area is therefore positive. The CBI encourages fintech development, but does recognise and warn against the potential to blur lines between regulated and unregulated activities and the challenges this may present.

The CBI's focus is on the risks to consumers from fintech developments and on protecting consumers where activity is not yet regulated. In its 2016 Consumer Protection Outlook Report, the CBI observed that the lack of consumer-faced culture was a major challenge. The CBI has encouraged fintech companies to focus on this aspect as they offer a great opportunity to steer innovation in financial services towards an improved consumer experience. The CBI's Director of Consumer Protection has recently said that "there is an exciting opportunity for Fintech firms to contribute in a positive way to protecting consumers and enabling greater access and availability of financial products and services".

In 2015, the Irish Government launched its strategy for Ireland's International Financial Services Sector for the following five years (**IFS2020**), which seeks 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 Irish Government Industrial Development Authority (**IDA**) is working with its clients to determine what role Ireland can play as they plan their future technology requirements. Furthermore, the start-up rate for Irish-owned fintech companies is accelerating rapidly, and in 2016, 10% of Enterprise Ireland's start-ups were involved in the fintech sector.

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. Multinational corporations (**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 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, for example the Accenture fintech Innovation Lab which is now in its third 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.

The IDA, Enterprise Ireland, the CBI and the Department of Finance participate in a working group 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).

3.3 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 activities 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.

- Firms wishing to establish a 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. A board of directors should meet in Ireland quarterly. A business must have at least two directors, one of whom is an EU resident. The CBI will require at least one independent non-executive director and 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 the applicant to be adequately capitalised. The amount will vary depending on the activity being authorised. 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 activities. These exemptions can be general or apply to a specific area.
- Alternatively, a fintech business authorised to provide regulated activities in another EU member state can notify the CBI 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 Acts 1988 and 2003 (**DPA**) govern the control and processing of personal data in Ireland. The DPA implement the EU Data Protection Directive 95/46/EC. The DPA regulate the processing of personal data and apply to data controllers if (i) they are established (e.g. as a body incorporated, branch or agency) in Ireland and process in the context of that establishment, or (ii) if the data controller is neither established in Ireland or the EEA but makes use of equipment in Ireland for processing data.

In addition, the e Privacy Regulations 2001 (S.I. 336 of 2011) which implement the e Privacy Directive 2002/58/EC (as amended by Directive 2006/24/EC and 2009/136/EC) (the **e Privacy Regulations**) deal with data protection issues in relation to phone, email, SMS and internet use.

General Data Protection Regulation 2016/679 (GDPR)

The DPA will be superseded by the GDPR from 25 May 2018. The GDPR, as a regulation, will be directly applicable in Ireland and broadly will not require national implementing measures. The Government's Spring/Summer 2017 Legislation Programme, however, includes publication of the heads of a Data Protection Bill to "give full effect" to the GDPR. The Data Protection Bill is expected to include a mechanism for fines imposed by the Office of the Data Protection Commissioner (**ODPC**) under the GDPR to be confirmed by a court. The profile and influence of the ODPC will increase under the GDPR as it is expected to become the lead data protection regulator for many of the world's largest multinational tech companies under the GDPR's one stop shop mechanism.

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 DPA apply to organisations not established in the European Economic Area (**EEA**) but who use equipment to process personal data in Ireland.
- The DPA restrict 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; or

- 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 in the context of the ODPC's application to the Irish High Court to make a reference to the Court of Justice of the European Union as to the validity of this mechanism (*Data Protection Commissioner v. Facebook Ireland Limited & Maximillian Schrems Record Number 2016/4809P*). For the time-being, however, the Model Clauses remain valid for data transfers outside the EEA.

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

Regulatory Action

The ODPC is responsible for the enforcement of the DPA and the e Privacy Regulations. The ODPC has a proactive approach to identifying data protection issues and regularly engages with public and private-sector organisations on those issues. The ODPC has, for example, a specific unit which focuses on issues arising for Irish-based tech multinationals.

The ODPC currently has no power to issue administrative fines but has broad investigative and enforcement powers including the power to:

- carry out announced and/or on the spot audits;
- compel compliance with the DPA, require the deletion of data and/or prohibit the transfer of personal data from the State; and
- prosecute – the ODPC has actively pursued prosecutions in respect of electronic marketing in recent years.

Criminal liability can arise for breach of specific provisions of the DPA. These include: (i) failure of a data controller or data processor to register; (ii) disclosure of personal data which was obtained without authority; and (iii) failure to comply with an enforcement notice. Persons found guilty of offences under the DPA may be liable on summary conviction (before a district judge sitting alone) to a fine not exceeding €4,000; or on conviction on indictment (before a judge and jury), to a fine not exceeding €100,000. The e Privacy Regulations also prescribe criminal liability for failure to report data breaches, inadequate security measures and sending of unsolicited communications (spam) with regard to electronic communication networks and services.

Damages

Damages may be recovered by a data subject for a breach of their data protection rights. In order for a data subject to be awarded compensation, it must be shown that the data subject suffered loss or damage arising from the breach. To date, the Irish courts have held that actual damage must be proved and damages for distress are not recoverable unless extreme distress results in actual damage, such as a recognisable psychiatric injury.

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 DPA require data controllers and data processors to take "appropriate security measures" to protect personal data and to ensure that staff and "other persons at the place of work" are aware of, and comply with, security measures.
- **Criminal Law**: It is an offence under the DPA to access or obtain and disclose to another person personal data without the prior authority of the data controller or data processor. The Criminal Damage Act creates two basic computer crime offences: that of causing criminal damage to a computer; and that of unauthorised access. The unlawful operation of a computer with the intent of making gain is a criminal offence under the Criminal Justice (Theft and Fraud) Offences Act 2001.
- **Duty of Care**: A duty of care may arise in relation to data compromised during a cybersecurity incident. Both data controllers and processors owe individuals whose data they process an express statutory duty of care under the DPA. As such, they may be subject to a claim for damages where a cybersecurity incident arises in connection with a breach of that duty.
- **Regulatory Guidance**: In June 2015, guidance on internet payments and the necessary security required were published by the European Banking Authority and the CBI would expect any authorised firms to comply with these. Fintech businesses regulated by the CBI need to comply with the CBI's 2016 cross-industry guidance in respect of IT and cybersecurity risks (available at: https://www.centralbank.ie/publications/Documents/Cross%20Industry%20Guidance%20Information%20Technology%20Cybersecurity%20Risks.pdf).
- **Proposed Legislation**: The Second Payments Directive will also enhance regulation in this area by creating new legal obligations to be complied with, such as all payment transactions requiring customer authentication. The EU's Network and Information Systems Directive sets out legal measures to boost the overall level of cybersecurity in the EU, including imposing security requirements and incident notification obligations on banks and other "operators of essential services" together with certain digital service providers. This Directive must be enacted into Irish law by May 2018. The Criminal Justice (Offences relating to Information Systems) Bill 2016 is progressing through the legislative process. When enacted it will create a number of new offences including unauthorised access of information systems, interference with information systems or data and use of tools to facilitate commission of these offences.

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 the Criminal Justice Act 2010 (**CJA 2010**). Designated persons under the CJA 2010, including all financial institutions authorised by the CBI or businesses conducting certain activities, have statutory obligations to comply with the CJA 2010's provisions. The CJA 2010 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 2010 is an offence.

The EU Fourth Anti-Money Laundering Directive is due to be implemented in June 2017. This will establish a stricter regime than in place currently, and a more detailed analysis of a business from this AML perspective may be required.

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

Employers must comply with equality legislation not only in the context of existing employees but also in all aspects of recruitment including job advertisement 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 travelling community). The maximum compensation available to non-employees who bring a claim in relation to a job application is €13,000.

Dismissing Staff

The Unfair Dismissals Acts 1977–2015 (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. The UD Acts apply to employees who have obtained one year's service (there are limited exceptions to the one years' service rule). Employees may also bring a claim for discriminatory dismissal under 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 years' 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.

Redundancy

In a redundancy situation, fair procedures require employers to consult with employees on the proposal prior to deciding to go ahead with the change with a view to looking for alternatives to the redundancy.

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, and a week's pay is capped at €600 per week. It is the practice in many redundancies for the employer to make a severance payment greater than the statutory level to the employees.

Employers also have certain statutory obligations in respect of consultation when effecting a collective redundancy. A collective redundancy will arise where an employer dismisses a specified number of employees within a 30-day consecutive period.

Notice Period

Employees are entitled to certain minimum statutory notice periods depending on length of service. An employee who does not receive this notice period may bring a claim for wrongful dismissal and loss of earnings during the notice period.

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**: the statutory minimum annual leave entitlement for full time employees is four working weeks.
- **Rates of Pay**: the minimum wage for employees in Ireland is €9.15 per hour. However, this rate may vary in certain sectors of employment.
- **Pension**: an employer in Ireland is not required to contribute to a pension for an employee; however, it is required to provide their employees with access to a pension scheme.
- **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 pay the basic 26 weeks' entitlement to employees.
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 pay the basic 24 weeks' entitlement to employees.
Paternity Leave	Up to 2 weeks' leave (paid by the State).	No obligation to pay. However, many employers pay the entitlement to employees.
Carer's Leave	Up to a maximum of 104 weeks' unpaid leave.	No obligation to pay.
Parental Leave	18 weeks' unpaid leave per child.	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 Jobs, Enterprise and Innovation (the **DJEI**).

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 multinational company 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 and 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 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 belongs 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 owner 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 must be notified to the Controller of Patents, Designs and Trade Marks (the Controller).

Assignment: In general, assignment of IP must be in writing. Assignment of patents, trade marks and designs must be registered with the Controller. Copyright may be freely assigned 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. Registration within 21 days is required with the Irish Companies Registration Office (**CRO**). Security interests granted over patents, trade marks and designs must also 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

Elad Wieder

Ariel Yosefi

Herzog Fox & Neeman

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 within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Israel, the "Start-Up Nation", had been a fertile ground for disruptive financial technologies long before the term fintech achieved its current prominence. Today, with innovation centres established by Citibank and Barclays (each boasts its own accelerator programme), local R&D centres of international giants like of Visa, PayPal and Intuit (many of which were initially established by acquiring an Israeli start-up company), and support of the prominent local financial institutions (including "The Floor" hub at the Tel-Aviv Stock Exchange, sponsored by internationals including HSBC, RBS, Santander, and Deutsche Bank) – Israel is leading the fintech innovation scene worldwide.

With more than 400 fintech start-ups located in Israel, and more than 500 million dollars of capital raised in 2016, Israeli technology is on its way to wallets and accounts around the world, in the same manner as it became part of every Intel or Apple device. In some cases, ventures which were seeded in Israel reach maturity in other, bigger markets; Lemonade, Payoneer, eToro, Forter and Credorax would be a few of such examples.

While Israeli fintech companies are to be found in each and every sub-sector (as can be seen in the excellent chart compiled by Carmel Ventures (http://www.slideshare.net/violanotes/israeli-fintech-companies-created-by-carmel-ventures), recent focus is mainly put on AI and technologies relating to all aspects of Big Data: novel algorithms for analysis of enormous amounts of aggregate data from various sources, are used to provide faster, better results for actuarial, pricing, underwriting, fraud prevention, customer retention and engagement, and other challenging tasks in today's financial markets.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

Currently, there are no prohibitions or restrictions that are specific to fintech businesses in Israel. A pending legislative initiative is aimed at prohibiting the activity of offering binary options on trading platforms, both to Israeli and non-Israeli customers.

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)?

Israel's highly developed and sophisticated funding infrastructure for technology companies is equally accessible for the fintech industry. Start-up companies of all sizes and stages of growth, from early seed company to late stage development have taken advantage of such funding, and almost all venture capital firms in Israel have investments in this field, some more than others. Equity financing through venture capital is available on customary standard terms and conditions.

Specialised venture capital funds and corporate venture capital investors which invest only or primarily in fintech companies have now entered this competitive space. Alongside the well-established legacy funds such as Carmel Ventures, which has a broad range of fintech companies in its portfolio, some newcomers have emerged, such as Moneta Seeds a micro fund specialising only in the fintech field. Another prominent trend is equity financing by multinational banks and corporate investors looking to invest in Israeli companies, such as The Standard Bank of South Africa and Visa.

The large commercial banks in Israel are also heavily involved in financing start-up companies in Israel in various manners. In addition to the special terms of debt financing offered to technology companies in general, some of the large commercial banks have also started special programmes in which a blend of equity and debt along with a "Proof of Concept" platform is offered, allowing start-ups in the field to enjoy both financing and design partnership programmes.

Very early stage programmes are available for start-ups in the field, through specialty "acceleration" and incubation programmes in which the companies may enjoy initial convertible debt products as first financing, along with design and development support through the programmes and "acceleration", into the market and the general financing platforms.

A recent amendment to the Israeli Joint Investment Trust Law, which is the primary legislation governing mutual funds in Israel, authorises the establishment of designated closed-end mutual funds, listed for trading on the TelAviv Stock Exchange (TASE), which will specifically invest in high-tech companies (including, potentially, fintech companies).

Finally, some peer-to-peer (P2P) debt and equity financing platforms have emerged in recent years which offer technology companies the ability to finance through debt, where such investment is syndicated through the platform among many individuals lenders. This is very early stage financing in most cases.

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 August 2010, the Government of Israel, through the Office of the Chief Scientist in the Ministry of the Economy (recently re-branded as the Israel Innovation Authority), enacted Directive 8.17, aimed at assisting multinational financial institutions in setting up R&D centres in Israel. The programme provides direct participation in financing of R&D centres in Israel by such multinationals, and is uniquely tailored to R&D in the fintech field. Two large R&D centres have been established in Israel under this programme operated by Citibank and Barclays. All of the Government's funding opportunities offered through the Israel Innovation Authority are available to all fintech companies, to the extent that they meet the criteria for each available programme.

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

The Tel-Aviv Stock Exchange (TASE) recognises the need of high-tech companies to raise capital in their early stages. Therefore, the TASE has laid down rules to enable R&D companies, including (potentially) fintech companies, to offer shares to the public on particularly lenient terms. An "R&D company" is a company that has invested at least ILS 3 million in research and development over the last three years, including investments using funds received from the OCS.

R&D companies are not required to show a specified period of activity or level of shareholders' equity prior to IPO. The minimum public-float rate is relatively low (ILS 16 million), making it easier for R&D companies to raise capital on the TASE at an early stage in their life cycle, with relatively little dilution of the founders' holdings.

An IPO on the TASE can serve as a convenient stepping-stone to an additional issuance on NASDAQ and other stock markets, as the company matures. The Dual-Listing Law on NYSE, NASDAQ, AMEX or the London Stock Exchange enables companies that initially issued shares on the TASE and later listed in the U.S.A. or U.K. to report according to U.S. or U.K. reporting rules, so that they are not required to report under two different sets of rules.

The TASE's Tel-Tech index helps to increase the exposure of technology companies traded in Tel-Aviv to the investing public.

Further reliefs and benefits for R&D companies include tax benefits for both investors and founders/controlling-shareholders, support of the TASE with free analysis of selected high-tech companies by Edison or Frost & Sullivan, easing of the reporting obligations for R&D companies included in the Tel-Tech index, and more.

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

Notable exits in the past few years include, Actimize (bought by Nice Systems), Check (bought by Intuit), Trusteer (bought by IBM), Superderivatives (bought by Intercontinental Exchange) and Billguard (bought by Prosper Markets).

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.

While there is no specific regulatory framework under Israeli law which applies to fintech businesses as such, the provision of financial products or services in Israel may fall within the scope of one (or more) of the existing financial regulatory frameworks:

(i) the Bank of Israel (BoI) regulates banking business, payment systems (including merchant acquirers) and credit data;

(ii) the Israel Securities Authority (ISA) regulates (*inter alia*) securities exchanges, trading platforms, investment advice and portfolio management; and

(iii) the Capital Markets, Insurance and Savings Authority regulates insurance companies and agents, pension and provident funds, pension advisors, money service businesses, non-bank lending (including by issuance of credit cards), credit unions and services for comparison of financial costs.

Recent regulatory initiatives, some of which are still pending, address specific aspects of the above regulatory frameworks which are typically relevant to fintech activities. These include (a) regulation of P2P platforms by the Capital Markets Authority, (b) a new regulatory framework for payment service providers by the BoI, (c) crowd-funding for corporations, under the ISA's remit, and (d) investment advice/management by use of technological means (algo-trading and robo-advisory), also under supervision of the ISA.

3.2 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?

All of the Israeli financial regulators and policy-makers are very receptive to fintech and financial innovation. Their support is clearly shown in the recent regulatory reforms and initiatives which are aimed at opening the regulated financial services markets to new entrants, mainly by technology-driven means (such as online platforms, alternative payment means, etc.).

Having said that however, turning this sentiment into actual developments, and adapting the licensing and supervisory methodologies of the various regulators is proving more challenging. Most of the regulatory initiatives relating to developments in the fintech space have yet to come into force.

3.3 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?

Provision of regulated financial services in Israel usually requires a licence, permit or registration; various exemptions apply, and specific legal advice should be sought in each case.

Israeli legislation does not generally specify the territorial scope of application of a particular law or regulation (whether any set of rules will apply cross-border or globally). In many cases, an analysis is required to determine whether cross-border financial services

will entail sufficient "nexus" to be subject to Israeli jurisdiction. Accordingly, different operational models may have significant consequences in that regard, and specific legal advice should be sought in light of the relevant circumstances.

Non-Israeli banks, insurers and investment advisors/managers may apply for an Israeli licence based on their foreign licence (with reduced requirements and obligations); foreign entities may also apply for registration as insurance agencies and money service businesses (until June 2018). Other licences (including for money service businesses from June 2018 onwards) require incorporation as an Israeli entity.

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 Protection of Privacy Law, 1981 and the regulations enacted thereunder (the "**Privacy Law**") regulate the matter of protection of privacy in general, and the matter of protection of privacy in computerised databases in particular (including with respect to the collection, use and transfer of such personal data). Fintech businesses which collect, use, process or transfer personal data pertaining to natural persons will be required to comply with the provisions of the Privacy Law. This may include, *inter alia*, matters such as registration of a database with the Israeli Data Protection Authority, providing privacy notifications to data subjects, maintaining security of the database, ensuring review and access rights to data subjects, direct marketing activities, and so on.

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 Law is territorial in nature and therefore may apply in cases where the activity has a nexus to Israel (for example, where personal data is collected from Israel, servers containing personal data are located in Israel, processing of personal data is performed within Israel, and so on).

The Protection of Privacy Regulations (The Transfer of Data to a Database Outside the State Borders), 2001 (the "**Transfer Regulations**") prohibit the transfer of personal data outside of Israel, unless the receiving country in question ensures a level of protection of data which is not lower than the level of protection provided under the Israeli law. The Transfer Regulations set out exceptions to this rule: for example, consent of the data subject for the transfer is in place, data is being transferred to a corporation under the control of the owner of the Israeli database, the data is being transferred to someone who has undertaken in an agreement with the owner of the Israeli database to fulfil the conditions laid down in Israel for the maintenance and use of the data, the data is being transferred to a database in a country which receives data from member states in the European Union under the same conditions of receipt, and so on.

In addition, under the Transfer Regulations, the owner of the database must ensure (by way of a written obligation from the recipient) that: (i) the recipient is taking steps to ensure the privacy of the data subject; and (ii) the recipient undertakes that the data will not be transferred to any person other than himself/herself, whether that person is in the same country or not.

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:

- ***Administrative sanctions*** – administrative fines might be imposed in cases of breach of the terms of the Privacy Law with respect to databases (such as a breach of a duty to register a database, a breach of a duty to use a database only for the purpose for which it was registered, a breach of a duty to provide data subjects with a privacy notice, and so on). The fines range between approx. US$545–US$1,370, and when the offender is a corporate entity, the fines imposed are five times this level.
- ***Criminal sanctions*** – breach of privacy in general (by willful misconduct) or breach of privacy in databases may amount to a criminal offence (punishable by imprisonment or fine). However, in practice, criminal prosecution is pursued only in extremely severe cases of breach of privacy.
- ***Civil claims*** – statutory damages of up to approx. US$16,350 may be imposed by the court in cases of infringement of an individual's privacy without his/her consent. Individuals may also be entitled to compensation under tort claims for damages (without limitation in amount, subject to proving damage) caused by the breach of Privacy Law.

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

Fintech companies which process or store personal information are subject to privacy and cyber security legal requirements. Under the Israeli Protection of Privacy Law 5741-1981, businesses which own or store personal information in a database are subject to legal requirements, including an obligation to safeguard the database in a reasonable manner. Moreover, the new Privacy Protection Regulations (Data Security), 5777-2017 (enacted in March 2017) present a wide range of binding regulatory arrangements aimed at ensuring cyber related obligations, including with respect to adaptation of technological, organisational and physical security measures and notification obligations in case of data breach.

In addition, fintech businesses may be subject to sector-specific cyber regulations when offering their services to financial institutions, insurance companies and banks. These entities are subject to strict cyber regulations (such as Directive 361 on Cyber-security Management and Risk Management in Cloud Computing Environment Guidelines issued by Supervisor of Banks at the Bank of Israel, and the Circular on Cyber Risk Management of Financial Institutions, issued by the Director of Capital Markets, Insurance and Savings) which impose various cyber-risk management obligations that may apply to services and technologies which such financial institutions, insurance companies and banks may wish to introduce.

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

The Prohibition of Money Laundering Law, 2000, the Prohibition of Terror Financing Law, 2005 and various orders promulgated under these Laws set various requirements applicable to financial institutions, money service businesses and potentially other fintech businesses. These requirements include client identification, identity verification, reporting and record keeping obligations. Anti-money laundering (AML) supervision is entrusted with the respective

regulators of each type of financial institution/business, with certain authority to tailor necessary adjustments and exemptions to the standard rules set in the respective AML orders.

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

Possible regulatory regimes that may apply include:

- ***Consumer Protection legislation*** – the Consumer Protection Law, 1981 and the regulations enacted thereunder (the "**CPL**") regulate the protection of a "consumer" ("a person who purchases a product or a service from a dealer within the framework of the dealer's business, mainly for personal, home or family use"). Consequently, to the extent that fintech businesses sell products or services to Israeli consumers, they may have to comply with various principles and requirements set out in the CPL. These include, *inter alia*, the prohibition on misleading consumers with respect to any matter which is material; certain disclosure requirements; requirements with respect to marketing and promotions; requirements relating to transactions carried out from a distance; rights of cancellation of transactions and so on.
- ***Spam law*** – Israeli law prohibits the sending of marketing material to recipients, by means of email, automated telephone message, facsimile or SMS/MMS, without the recipient's explicit prior consent, or, under certain specific circumstances, if the recipient has given his or her details in the past to the advertiser.
- ***Standard Contracts*** – the provisions of the Standard Contracts Law, 1982 (the "**Standard Contracts Law**") might apply if the relationship between the fintech business and its customers or clients or business partners) is governed by certain contractual terms which are pre-determined by the fintech business. In such case, the terms may be regarded as a standard contract, in which case the Israeli court might strike out unfairly prejudicial terms within the standard contract.

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, subject to the provision of mandatory employment benefits (as detailed hereunder), the employer and employee can agree on their contractual engagement terms.

Prior to a decision to employ a candidate, an employer is entitled to perform some background checks with respect to the candidate, subject to the certain limitations such as the candidate's basic right for dignity and privacy, nondiscrimination and general good faith obligations. Criminal background checks are, in general (and subject to certain exceptions), prohibited.

In principle (and subject to certain exceptions), Israeli law does not require that an employment contract be in writing. However, each employer is required to provide all new employees with a formal written notification (in a form as set out under applicable law) regarding certain employment terms, and to update all such employees in writing of any changes in those terms. If all terms of such notification are included in the employee's employment contract, there is no need to provide formal notification. There is no requirement that employment contracts be written in any specific language, as long as the employee understands the language.

As a general rule, either party to an employment contract is entitled to terminate the employment contract, subject to providing the other party with prior written notice as required by law.

Employers should exercise their right to terminate employees in good faith and for valid reasons. Valid reasons for dismissal may include performance-based, redundancy and disciplinary reasons.

There are categories of employees whose employment cannot be terminated without obtaining a special permit (such as pregnant employees and employees undergoing fertility treatment) or at all, such as employees on maternity leave.

Notice Period – both employers and employees are required to give prior written notice when ending their employment relationship. The minimum notice period required by law to be given by both employer and employee depends on the seniority of the employee. Longer notice periods may be set out by any additional binding source applicable between the parties, such as an employment agreement.

A collective bargaining agreement applicable on the parties may impose additional terms and requirements with respect to hiring and termination.

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

The main mandatory benefits which should be provided to employees are as follows:

Wages: an employer is required to pay its employees at least the minimum wage according to law. Currently, the minimum monthly wage for an adult employee is approximately NIS 5,000 per month (currently, equivalent to approx. US$ 1,400).

Annual Leave: The Annual Leave Law – 1951 requires employers to provide employees with a minimum number of paid annual leave days on which the employees shall receive their full salary.

Public Holidays: Non-Jewish employees are entitled to choose whether to be absent from work on their religious holidays or on Jewish holidays.

Sick Leave: According to applicable regulations and prevailing industry customs.

Recuperation Pay: An employee is entitled to an additional annual payment referred to as "recuperation pay". The name of this payment is historical.

Travel Expenses.

Pension: Almost all employees in Israel are entitled to pension insurance. There are some limited exceptions to this rule.

Employers are required to contribute, on their own account, a percentage of the employee's salary (up to the average market salary) to pension insurance, and to also deduct a certain percentage from salary as the employee's contributions to the pension fund. A more beneficial pension entitlement may apply pursuant to any collective agreement, personal employment agreement or other binding source. Currently, the mandatory required employer's contributions are as follows: 6.5% of the salary towards the saving and risk component and 6% of the salary towards the severance component (this can be increased to 8.33%). The employee contributes 6% of his or her salary (deducted by the employer).

Severance Pay: As a general rule, an employee who is dismissed after completing at least one year of service is entitled to statutory severance pay. Severance pay is calculated based on the employee's last monthly base salary multiplied by the number of years of service. Any amounts accumulated in the employee's severance fund (a component of his

pension arrangement) are on account of the employee's entitlement to severance pay, unless a special arrangement has been adopted. Under Israeli law, severance pay will only be denied under extreme circumstances of misconduct on the part of the employee.

The severance component deposited in the employee's pension arrangement is taken into account when calculating the amount of severance pay to which the employee is entitled (if at all).

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 employ a foreign employee in Israel, an employer must obtain a work permit. In general, work visas for the employment of foreign nationals are granted in the following fields of the economy: (1) construction; (2) agriculture; (3) nursing; and (4) industry.

A special category of permit within the "industry" sector has been created for "foreign experts". A foreign expert visa is granted based on a list of criteria, such as holding a managerial position or special expertise that cannot be found in Israel. Most of the foreign expert permits are conditional upon the employer undertaking to pay the foreign expert a monthly salary of at least twice the average salary in Israel.

Once the employer obtains a foreign expert permit, it is then eligible to employ the specific employee. The employee may only work for the employer that obtained the permit and only after obtaining a work visa, which is stamped in his or her passport.

Generally speaking, the employment of a foreign expert in Israel is subject to the same legal framework as applies to every foreign worker in Israel. A foreign expert work permit can be issued for a period of 45 days, three months, one year or two years. However, a work visa will only be issued for up to one year. In general, a work permit can be extended, subject to the discretion of the Immigration Authority, for additional periods up to a maximum of five years and three months.

Notwithstanding the above, the Foreign Workers Regulations (Exempt Employers of Foreign Experts), 2007 (the "**Regulations**"), determine that the employers will be exempt from certain obligations set out in the general law relating to foreign workers. In this regard, there is no special route for fintech employees.

In principle, a foreign employee is entitled to the same benefits and entitlements as an Israeli employee and in addition, is entitled to the following main entitlements: (a) an employer of a foreign worker is required to purchase private health insurance for the employee throughout the entire employment period; and (b) employers must provide suitable housing for foreign workers. Such housing must meet the conditions set out in Regulations. These (and other related) obligations will not apply to an "Exempt Foreign Expert", such as a manager, senior representative or senior employee in a position that requires a high degree of personal trust in a foreign corporation or an international company.

6 Technology

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

Israeli law generally protects innovations and inventions by means of patents under the Patent Law, 1967 (the "**Patent Law**") and trade secrets, which are governed by the Commercial Torts Law, 1999 (the "**Commercial Torts Law**"). Patents have a term of 20 years from the date of application, subject to certain exceptions, and there is no limitation on trade secret protection, as long as the information remains secret and does not enter the public domain.

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

The general rule under Israel law is that the creator of the right is the first owner, except in employer/employee relationships, where the first owner is the employer.

Patents: The first owner of rights in an invention is the inventor, except where the invention is created by an employee in the course of employment (defined as a Service Invention). In the absence of any agreement to the contrary, the employer owns all Service Inventions (although it is nonetheless customary to include a broad "assignment of IP" clause in employment agreements, as well as an express waiver of any right to royalties on Service Inventions, so as to avoid claims by employees).

Copyright: Israel's Copyright Law, 2007 protects the economic and moral rights of authors. The author of a literary, dramatic, musical or artistic work, or the producer of a sound recording, is the first owner of copyright in the work or sound recording respectively (unless otherwise agreed, for example in the case of a commissioned work, where the parties may agree that the principal is the first owner of the copyright rather than the creator of the work). As an exception to this rule, the first owner of a work created by an employee in the course of his or her employment is the employer, unless otherwise agreed between the parties.

Software is protected as a literary work.

Moral rights refer to the right of attribution and to the right to prevent detrimental changes to the work. The rights are personal and non-transferable (although it is generally accepted that they can be inherited). In an employment relationship, moral rights remain with the employee; it is customary in employment and contracting/consulting agreements to require a waiver of moral rights, although this has not been tested in Israeli courts.

There is no moral right in software.

Trademarks: the registered owner of a trademark is presumed to be the owner.

Trade Secrets: Trade secrets are defined as any business information which is not publicly known and which cannot readily and legally be discovered by the public, the secrecy of which grants its owner an advantage over his or her competitors, provided that its owner takes reasonable steps to protect its confidentiality.

The person in possession of the information is usually the owner of the trade secret. This is a question that is largely governed by case law, mainly in the context of employment and non-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)?

Generally speaking, IP rights in Israel are territorial, and it is necessary to own a local/national right in order to be protected, but there are cases in which international treaties grant protection to the owners of foreign rights. International treaty obligations are not self-executing under Israeli law, but some provisions incorporated into Israel law are closely based on the language of the applicable international treaty obligations.

Under the Berne Convention for the Protection of Literary and Artistic Works, no discrimination is permitted on the basis

of whether the author is a foreign national or a national of the jurisdiction in which the right is being asserted. This provision has been implemented by the Copyright Law. Infringement of copyright (or a violation of moral rights) in Israel is a civil tort, and the available remedies include, *inter alia*, injunctions, monetary awards, statutory damages and the seizure and disposal of infringing materials.

Israeli law protects unregistered well-known marks in accordance with the Paris Convention for the Protection of Industrial Property and the Agreement on Trade-Related Aspects of Intellectual Property Rights (the "**TRIPS Agreement**").

With respect to enforcement, injunctive and monetary relief are available for trademark infringement. In addition, statutory damages for passing off under the Commercial Torts Law 1999 can serve as a complementary claim to trademark infringement.

Furthermore, the Copyright Law, the Trade Marks Ordinance, and the Customs Ordinance [New Version] each contain sections stating that the customs authorities are authorised to suspend the release of imported goods suspected of being infringing copies.

Patents are only protected on a national level. If the patent is not registered in Israel, it is not protected under Israeli law. In case of patent infringement, injunctive and monetary relief are available. No statutory damages are available.

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 in Israel can be assigned, licensed or used as collateral.

The right can be sold/assigned on its own or together with the corresponding business.

Both exclusive and non-exclusive rights are recognised. Patent and trademark licences must be recorded with the registry in order to be valid against third parties.

A security interest in IP rights must be recorded at the relevant registry. In the case of unregistered rights (copyrights, trade secrets and unregistered trademark right, if any), the only required registration is either with the Registrar of Companies (if the debtor is an Israeli company) or with the Registrar of Pledges in all other cases.

Under Section 90 of the Patent Law, a security interest against a patent is also required to be recorded on the Patent Registry, in addition to the Companies Registry or the Pledges Registry. This recordal is constitutive and the lien/charge will not be effective against third parties if it is not so registered.

While the Trademarks Ordinance [New Version], 1972 does not require the recordal of a security interest against a registered trademark, it has become common practice for the Commissioner of Trademarks to record a note of the lien/charge against the trademark in question at the request of one of the parties, by way of courtesy. This is not constitutive.

The Patent and Design Ordinance, 1924, which is the law applicable to industrial designs, does not require the recordal of any security interest against a registered design, but we believe these should be treated the same way as trademarks and that a note may be entered against the design upon request.

Please note there are different tax implications to each of the means of monetisation.

We note further that in certain cases the Government may provide incentives to different companies and projects. For example, the Israel Innovation Authority encourages innovation by providing a variety of incentives to Israeli companies and entrepreneurs. There are tax and fiscal incentives for, *inter alia*, R&D. Such incentives can impose various conditions on the IP created, including with respect to freedom to use and transfer the IP outside of Israel.

Elad Weider
Herzog Fox & Neeman
Asia House, 4 Weizmann St.
Tel Aviv 6423904
Israel

Tel: +972 3 692 5521
Email: wiedere@hfn.co.il
URL: www.hfn.co.il

Elad Wieder is a partner in HFN's Banking and Finance Department. Elad has experience in a wide range of legal issues within the financial industry, with a particular emphasis on technology. This includes online platforms, digital payment solutions and other innovative products and services. Elad's knowledge of alternative payment mechanisms means that his expertise is invaluable to credit card companies, online payment processers and others concerned with payment methods in the 'post-money' age. As part of his specialisation, Elad advises major financial institutions as well as innovative start-ups, on matters of cross-border compliance, international anti-money laundering and sanctions regimes and other regulatory & licensing topics.

While working at HFN, Elad has spent time on secondment at Allen & Overy in England and Barclays in Tel Aviv.

Ariel Yosefi
Herzog Fox & Neeman
Asia House, 4 Weizmann St.
Tel Aviv 6423904
Israel

Tel: +972 3 692 2871
Email: yosefia@hfn.co.il
URL: www.hfn.co.il

Ariel Yosefi co-heads HFN's Technology & Regulation Department. He is highly-regarded for his prominent global practice and experience in advising startups, multinational companies, mobile app and software developers, internet vendors and disruptive technologies on various technology compliance, regulatory and commercial matters.

Ariel's multidisciplinary expertise covers numerous areas, including Adtech and online advertising, telemarketing and e-marketing, quality media and traffic, content, social networks and User-Generated-Content platforms, monetisation, mobile and other app marketplaces, Insurance Technology, Health Technology, Fintech, Cybersecurity, Internet of Things, computer and software protection e-Commerce, privacy and data protection.

Ariel has unique experience with the increasing volume of related regulations, enforcement actions and legislative trends across a myriad of jurisdictions, as well as with the industry's best practices and leading self-regulatory guidelines.

HERZOG FOX & NEEMAN
LAW OFFICE

Herzog Fox & Neeman is one of Israel's largest law firms and has earned a reputation as a market leader – evident by its recognition as '2016 Israel Law Firm of the Year' by Mergermarket, *IFLR*, *BDI Code and Dun & Bradstreet*, and its consistent top-tier rankings in both international and Israeli legal ranking directories. HFN is the most diverse law firm in Israel with over 300 lawyers, of whom more than 115 are partners. The firm has expertise in all aspects of corporate, commercial and administrative law and serves many of Israel's and the world's best-known companies.

Along with an international network of expert advisers, HFN provides an interdisciplinary, global regulatory advisory service to the fintech industry. We keep abreast of the rapidly changing landscape of the industries in which our clients operate, to ensure that we provide them with a current and comprehensive understanding of the laws and regulations that govern their activities.

The Fintech team provides a fully coordinated range of services to our clients, including licensing, regulatory, tax, commercial and e-payments, as well as coordinating and assisting in the implementation of public offerings and other exit strategies.

Italy

Federico Vezzani

Tommaso Faelli

BonelliErede

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 within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

A wide variety of fintech businesses are currently active in Italy and operate in almost every sub-sector of the fintech industry. According to the most recently available information, almost 150 fintech companies are based in Italy, and this number continues to grow. Crowdfunding is the largest sub-sector, with 51 active companies followed by payment services and other sub-sectors, including asset management, blockchain, virtual currencies, insurance and peer-to-peer lending. A wide range of innovative fintech solutions have recently been developed in the payment service sector, mainly through apps that provide alternatives to the traditional banking channel. Insurance and asset management sectors are also very aware of and interested in fintech solutions. For example, an Italian based start-up is currently developing an application to sell short-term, highly customised insurance policies. Banks have also recently started seeing fintech as a way to innovate their everyday business and therefore planning consistent investments that take advantage of fintech solutions.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

In Italy no specific provisions prohibit or restrict the types of fintech business that a company is entitled to carry out. However, the Bank of Italy has discouraged Italian banks and other supervised entities from buying or selling virtual currencies following the recent scandals involving bitcoins (i.e., the bankruptcy of the well-known Japanese exchange facility MtGox). The Bank of Italy has also highlighted that several non-regulated entities are involved in the disposal of virtual currencies and, as they are not subject to Anti-Money Laundering regulations (AML), their activities may pose some risks.

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 wide range of financing tools are available for new and growing businesses, including both equity and debt financing. A useful tool for raising finance is issuing so-called mini-bonds. These bonds are designed for SMEs and can be admitted to trading in a dedicated segment of the Italian regulated market reserved for qualified investors, with fewer formal requirements than a standard admission to trading. Moreover, fintech start-ups can be financed by non-bank entities such as venture capitalist, business angels and business incubator and may use 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?

The Italian legislation provides for several measures aimed at supporting investments in research, development and technological innovation: the main ones applicable to fintech businesses are (i) the "innovative SMEs and start-ups" regime, (ii) the R&D tax credit regime, and (iii) the Patent Box regime. The measure in favour of innovative SMEs and start-ups consists in a vast and diversified package of measures that includes more flexible corporate management tools, tax incentives for investments in innovative SMEs and start-ups (deduction for income tax purposes of the 30% of the amount invested up to €1m or €1.8m 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 SME Guaranteed Fund). The R&D tax credit regime provides for a tax credit, up to €20m per year, equal to the 50% 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.

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 in the Italian regulated market must meet the following requirements: a) 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) publish a prospectus approved by Consob (the Italian authority in charge of supervising the financial sector and listed companies). Start-up companies (i.e. companies that have been in business for less than three financial years) are also required to disclose additional information (e.g., profit estimates and forecasts) to have a prospectus approved. Companies may also list their shares on a

non-regulated market reserved for professional investors with less 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?

No notable IPO or sale of business has taken place in Italy.

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. In any case, as a general rule, specific authorisation should always be requested for activities that could qualify as reserved activities under applicable Italian law regardless of the (technological) means used to carry them out. For instance, peer-to-peer lending may fall within the scope of the payment services regulation, thus requiring the Bank of Italy's authorisation. Similarly, robo-advice can be considered an investment service, in which case Consob authorisation may be required. Moreover, Consob issued a specific regulation for crowdfunding activities (Regulation No. 18592 of 26 June 2013, as amended) and subsequently last December the Bank of Italy and the Italian banking association (ABI) signed an agreement to work together to improve cyber security for data used by banks when providing their services.

3.2 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?

Although cyber society and technological developments are currently in the spotlight, Italian regulators and policymakers have yet to issue any regulations in this respect. However, Consob has launched different initiatives in cooperation with some of the most prestigious Italian universities, including research programmes concerning robo-advice, block-chain and, more generally, the relationship between fintech businesses and more traditional financial activities.

3.3 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 via branch or under the regime of 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 in case of incorporation of a branch). In this respect it is worth highlighting that in 2016, one of the few peer-to-peer platforms with banking licence worldwide and core-business in consumer credit entered into the Italian market via branch. One of the main regulatory hurdles for non EU companies carrying out reserved activities to overcome is obtaining the necessary administrative authorisations.

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?

Until the GDPR enters into force, Legislative Decree no. 196 of 30 June 2003 ("Data Protection Code" or "DPC") sets 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. Consent of the data subjects is not required in specific cases, such as when processing is necessary to comply with legal obligations or contractual obligations, or to exercise a right. Consent of the data subjects is normally necessary when direct marketing, profiling or geolocation is envisaged. Limitations and conditions apply to the appointment of outsourcers, communication of the data to third parties, data transfer to non-EU entities and authorities. Duty to file data breach information with the Italian Data Protection Authority ("Italian DPA") applies to certain sectors, such as banking and telecommunications.

In addition, the Italian Data Protection authority issued Guidelines for the Banking Sector, which are binding on whomever operates in this 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?

The law applicable to data processing is that of the EU Member State in which the data controller is established (i.e. DPC applies to entities established in the Italian territory). If the data controller holds establishments in more than one European country, the data protection law applicable in each country must be complied with. DPC also applies to data controllers established outside the EEA processing personal data through means or equipment located in the Italian territory. For example, DPC applies when a data controller is located outside the EEA but avails itself of servers located in Italy. GDPR will change this approach to one based on the geographical target of the processing.

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 non-EU country, approved by the EU Commission; c) consent of the data subjects; and d) adoption of Binding Corporate rules.

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

Italian DPA may issue blocking orders of non-compliant personal data processing (and therefore prevent further use of the data) and administrative fines, among which the most frequent are due to lack of adequate information on data subjects (fine up to €36,000), lack of data subject's consent (fine up to €120,000), and lack of minimum security measures (fine up to €120,000). Repeated

breaches for large amount of personal data increase fines up to €300,000 and fines can further increase by up to four times if the initial fine amount is considered ineffective based on the offender's economic status. In a recent case of early 2017 regarding severe violations of five companies in the money transfer sector, the Italian DPA issued fines totalling about €11 million. Criminal sanctions apply if there is gain or intent to cause harm (imprisonment up to 18 months or in most severe cases up to 24 months) or for lack of minimum security measures (imprisonment up to 24 months, which can, however, be avoided if the data controller promptly remedies the breach).

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

DPC sets forth minimum security measures for processing data with electronic means also aimed at preventing cybersecurity incidents. Companies of specific sectors (e.g. banking, health and telecommunications) must adopt further and stronger measures (e.g. encryption/double encryption, segregation of databases, careful risk assessment for cloud services, etc.). The Italian criminal code also sets forth specific computer crimes, such as computer fraud or unlawful access to a third party IT platform. Changes are expected with the implementation of the NIS (Network and Information Security) directive.

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

If a fintech business falls within the scope of a reserved activity (e.g. banking activity, payment or financial services) an authorisation from the competent national authorities is required. Carrying out a reserved activity without the relevant authorisation is a criminal offence and may result in the application of criminal sanctions.

Moreover, if the company carrying out a fintech activity is subject to AML regulations, any breach of such regulations may result in an administrative or criminal sanction depending on the offence committed. Recently an Italian fintech company dealing mainly with virtual currency publicly disclosed its intention to voluntary comply with the AML regulation.

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. 36 months). The employment is regulated by law, national collective bargaining agreement (NCBA – if applied) and individual contract. To dismiss an open-ended employee, the employer must:

(i) fulfil specific formal requirements; and

(ii) find grounds for the dismissal on 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 24 monthly salaries (in particular, two months' salary per each year of seniority).

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…). 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 a NCBA results in increased costs for the employer. Nevertheless, NCBAs are actually applied by companies on a voluntary basis (since it makes more comfortable the management of the employment contracts).

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% 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 to the principle of territoriality, must pay social contributions to INPS (with the 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 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 programmes, which are likely to flourish in the fintech industry, can be patented only if technical effects can be demonstrated according to EPO's guidelines on software patentability; otherwise, software programmes are eligible for protection under copyright law, which only covers the code and not the logic behind.

(ii) Trade secrets, either of 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 will likely lead to a detailed regulation of specific aspects but will not change the main legal framework.

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 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 the ownership of the employer (not the employees) or the client (not the provider or contractor) unless otherwise was 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 can be exploited though 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 which is equally eligible for the Patent Box regimes 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.

Acknowledgment

The authors would like to acknowledge the assistance of their colleagues Giuseppe Rumi (Partner – Regulatory) and Jacopo Liguori (Managing Associate – IP/IT/Privacy) in the preparation of this chapter.

Giuseppe Rumi (giuseppe.rumi@belex.com) – LinkedIn URL: https://www.linkedin.com/in/giuseppe-rumi-84637744/.

Giuseppe (partner since 2007) is an expert in banking and finance regulatory matters and founded the Financial Regulatory Department within the firm.

Giuseppe advices major national and international banks and investment firms on the Italian rules governing banking and investment services, including the impact of all types of transactions on licences and authorisations and of the new internal organisation regulations on the processes, policies, and rules of banks and investment firms.

Member of the Italian Bar is also admitted to practice before the Italian Supreme Court (*Corte di Cassazione*).

Jacopo Liguori (jacopo.liguori@belex.com) – LinkedIn URL: https://it.linkedin.com/in/jacopo-liguori-bb612617.

Jacopo (managing associate since 2017) has a wealth of experience in assisting multinational companies with privacy compliance plans: he recently assisted a fashion company in implementing a CRM plan in more than 20 countries. He also focuses on new technologies, contracts and on intellectual property, particularly on global brand protection strategies.

Jacopo holds master's degrees in business and IP law, and attained a Ph.D. in IP law at the University of Parma.

He is lecturer for the master's courses of Il Sole 24 Ore in IP and privacy Law.

Federico Vezzani
BonelliErede
Via Michele Barozzi
1 - 20122 Milano
Italy

Tel: +39 02 771131
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;
- 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. He recently advised one of the most important Italian banks in investing in fintech funds.

Tommaso Faelli
BonelliErede
Via Michele Barozzi
1 - 20122 Milano
Italy

Tel: +39 02 771131
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 at masters in IP and cyber risk.

BonelliErede

BonelliErede is one of the largest independent law firms in Italy, with offices in Milan, Rome, Genoa, London, and Brussels. BonelliErede has also two outposts in Africa: one in Cairo, in cooperation with Kosheri, Rashed & Riad, and one in Addis Ababa, in cooperation with Teshome Gabre-Mariam Bokan Law Office.

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 **62** partners, **3** local partners, **20** of counsel, **300** associates supported by about **150** staff employees. Among its **380** lawyers, it boasts **15** university professors.

Japan

Taro Awataguchi

Ken Kawai

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 within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Although Japan is not a global leader in fintech innovation, nevertheless, recent government reforms supported by initiatives by the financial industry are driving the establishment of fintech companies to progress at a faster pace and compete with the advanced countries. According to Accenture, the investment in this sector in Japan grew, by 230 percent from the previous year, to approximately USD 154 million in 2016. Among these, the investment in payment services including those related to cryptocurrency accounted for 40 percent and the investment in wealth and asset management services including robo-adviser gained ground. That being said, compared to fintech companies in other countries such as the United States, fintech ventures and startups in Japan are more likely to coordinate with traditional financial institutions rather than fight with them and disrupt existing financial services, partly because of the nature of Japanese society and the relative difficulties in procuring massive funding for fintech ventures in Japan. Notable sub-sectors are listed below.

- Money transfer:

  Traditionally, only banks and certain other depository institutions handling deposits licensed under applicable laws (collectively, the "Banks") were able to provide money transfer services. In April 2010, however, a part of such restriction was deregulated by the promulgation of the Payment Service Act (the "PSA"). Under the PSA, companies other than Banks are allowed to provide a service of money transfer not more than JPY one million if they are registered under the PSA. Since then, entrance into this sub-sector by non-banking companies has been steadily increasing.

- Electronic-money ("E-money"):

  Prepaid-type E-money is very popular in Japan. Mobile wallets for E-money installed in the mobile phone have been used since 2004 in this country. Recent developments in this sub-sector include so-called biometric payment service. For instance, a fintech startup provides the service with which people can make payment at shops only by scanning their fingers on a small fingerprint sensor machine.

- Crypto-currency:

  Although Japan experienced bankruptcy of the Mt. Gox, which is a Japanese company, trading volume of bitcoin and other crypto-currencies in this country has been increasing rapidly and it is often reported that Japan is the second largest market for bitcoin trading in the world. Japan is becoming crypto-currency-friendly country not only for trading but for payment and settlement as well since consumption tax will basically become inapplicable to buying crypto-currencies effective from July 1, 2017. Nikkei, the leading business newspaper in Japan, reported recently that more than 260,000 shops are expected to adopt bitcoin payment by summer 2017.

- Cloud-Computing Accounting and Personal Wealth Management:

  Sub-sectors that have gained much attention are the sectors of cloud-computing accounting and personal wealth management ("PFM"). The main function for these sub-sectors are accumulating and aggregating a user's financial accounts data that are separately held by several financial institutions in which the user has its accounts.

- Asset management:

  In this sub-sector, several fintech startups as well as traditional investment advisory/management companies provide investment advisory/management services based on the technology of artificial intelligence (the "Robo-advisers").

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

There are, at present, no prohibitions or restrictions that are specific to fintech businesses in Japan.

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/or friends are commonly utilised. Funding through bank loans tends to be difficult in these stages. Japan Finance Corporation and municipalities provide a certain lending systems to support start-ups up to a certain maximum amount. Angel investors would 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.

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 the angel investors with the following tax incentives: (i) reduction of the income tax (the amount invested to the target company which have not made profits in three years from the establishment will be reduced from the gross income); or (ii) reduction of the capital gains from transfer of shares in the target company (the amount invested to the target company of less than 10 years old will be reduced from the capital gains).
- The research and development ("R&D") tax incentive system has been adopted and often revised in Japan with the aim of maintaining and strengthening the R&D initiatives, which support Japan's global competitiveness.
- Unlike some of the European countries, the patent box scheme (which allows companies to apply a lower rate of corporation tax to profits earned from patented inventions) has not been adopted in Japanese tax system, though the adoption has been continuously proposed by the Japanese industry.

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") by which the company will be examined to list its stock encompassed: "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; (vii) number of consecutive years of business operation, and so forth. 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?

There are many fintech start-ups aimed at exits such as IPO, though completion of the IPO is yet to be reported. In addition, given the deregulation of the Banking Act which enabled the bank holding company to make investment to fintech business companies upon a respective approval by the Financial Services Agency of Japan ("JFSA"), such investment may increase.

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 crypto-currency (the "Virtual Currency Regulations"), there is no specific regulatory framework for fintech businesses, which are subject to the existing body of Japanese financial regulations. If the services provided by the fintech companies are subject to existing financial regulations, they are required to comply with these regulations including 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 JFSA or one of the Local Financial Bureaus that is delegated a part of the authority from the JFSA. Please note that solicitation for using its services from abroad to residents in Japan is basically considered as undertaking its activities in Japan.

Money transfer services are regulated under Banking Act and acts applicable to other depository institutions, which requires those who wish to enter into this business to obtain a licence from the JFSA, provided that service of money transfer of not more than JPY one million can be provided if a firm obtains the registration of the "Funds Transfer Service Provider" under the PSA.

As with 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 get registration, provided that they have 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 the payments to other entities that are designated by the issuer, then the issuer is required to obtain the registration of the "Issuer of Prepaid Payment Instruments" under the PSA.

Regulations on crypto-currency came into force on April 1, 2017. The amended PSA defines "Virtual Currency" and requires a firm that wishes to provide "Virtual Currency Exchange Services" to get registration of "Virtual Currency Exchange Service Providers". The term "Virtual Currency Exchange Services" means any of the following acts carried out as a business: (i) sale/purchase of Virtual Currency or exchange for other Virtual Currency; (ii) intermediary, agency or delegation for the acts listed in (i) above; or (iii) management of users' money or Virtual Currency in connection with its acts listed in (i) and (ii).

Please note that an online payment instrument can be considered either as a part of "Funds Transfer", a "Prepaid Payment Instrument", a "Virtual Currency" or something else. As the boundary of each definition is not easy to distinguish, a consultation of specialists is recommended if an entity wishes to undertake business related to online payments in Japan.

In March 2017, the bill to amend the Banking Act for regulating "Electronic Payment Intermediate Service Provider" and facilitating open API was submitted to the Diet in Japan. If the bill passes the Diet, this amended act will come into force within a period not exceeding one year from the day of promulgation. An intermediary between financial institutions and customers, such as an entity engaged in the communication of payment instructions to Banks through IT based on the entrustment from its customers or an entity providing its customers information of their financial accounts held by Banks through IT may fall under the definition of Electronic Payment Intermediate Service Provider.

3.2 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?

Yes. Financial regulators and policy-makers in Japan are receptive to fintech innovation and technology-driven new entrants in to the regulated financial services markets.

The Financial System Council (the "FSC"), the advisory body for the Japanese government, published its "Final Report: Strategies for Reforming Japanese Payment System" in December, 2015. The report emphasised that both public and private sectors in Japan should recognise how influential the innovation as well as structural changes and globalisation of payment services in conjunction with technological innovation would be in the field of financial services and should make efforts in a timely manner in the respective field to progress in the following direction:

- applying IT innovation and renovating the payment services sector;
- securing of payment system stability along with information security;
- promoting innovation and ensuring user protection; and
- demonstrating leadership in international trends concerning payment systems.

In August 2016, Japanese cabinet approved its action plan for 2016 to 2017, and named it "Japan Revitalization Strategy 2016". The Action plan includes the Japanese government's commitment to creating environment (FinTech ecosystems) to ensure development of fintech companies in Japan.

Since 2015, JFSA has been introducing several pro-fintech policies and measures, aimed at enhancing financial innovation through fintech:

- in September 2015, the JFSA published its first "Strategic Directions and Priorities" paper, which designated fintech as one of the areas that has top strategic priorities for the agency;
- in December 2015, the JFSA established "FinTech Support Desk" as a one-stop contact point for inquiries and opinions pertaining to businesses involving fintech; and
- in June 2016, the JFSA established a "Payments Council on Financial Innovation", aiming to set up a framework in which members from financial sector, industry, consumer and government could work together and follow up on the progress of the action plan agreed by the aforementioned Working Group and deliver payment system reforms and payment service innovations continuously.

3.3 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 basically required to obtain the same authorisation or registration that Japanese companies need to obtain to carry out such regulated activities from the relevant authorities in Japan. 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 other jurisdiction that wishes to provide its service to residents in Japan is 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. In connection to this, in March 2017, the JFSA made a series of announcements supporting fintech companies from other jurisdictions to enter the Japanese market which are as follows:

- the JFSA and the UK's Financial Conduct Authority jointly announced that they exchanged letters on a co-operation framework to support innovative fintech companies in Japan and the UK to enter each other's market by providing a regulatory referral system. The JFSA and the Monetary Authority of Singapore ("MAS") jointly made the similar announcement; and
- the JFSA announced the launch of the "Financial Market Entry Consultation Desk" to give advice on Japan's financial regulations to foreign financial business operators (e.g. asset management firms) which plan to establish a business base in Japan. The JFSA's Financial Market Entry Consultation Desk closely cooperates with the Tokyo Metropolitan Government's "Financial One-Stop Support Service" to support foreign financial business operators planning to set up offices in Tokyo.

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 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The Act is applicable to all private businesses including fintech businesses. Based on the requirements of the APPI, each governmental ministry issued administrative guidelines that are applicable to specific industry sectors under its supervision. Fintech businesses should basically comply with the "Guidelines on Personal Information Protection in the Financial Industry". In September 2015, the amendment to the APPI was promulgated and will be 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 utilisation of de-identified information, (iii) establishment of Personal Information Protection Commission (already established), and (iv) setting restrictions on transferring personal data to foreign jurisdictions and rules of Introducing restrictions on transferring personal data to foreign jurisdictions.

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 does not have exterritorial reach. However, the amended APPI will be applicable to certain acts that are performed in a foreign country. More specifically, many of the provisions of the amended APPI will be applicable to the owner of personal information regardless of the owner's location, if the owner uses or processes such personal information of 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 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 cyber security. Under the 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 the 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 Provider and Virtual Currency Exchange Service Provider are specified as the Specified Business Entities under the APTCP, while Issuer of Prepaid Payment Instruments is not designated under Specified Business Entities.

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 is aimed specifically at 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 either of hiring and 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 the 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 of the definite term employment contract or without delay of such expiration date, deemed to be renewed as an employment contract with an indefinite term under the same terms and conditions of employment as the definite term employment contract if a certain condition is met. Please also note that a definite term contract employee whose contract periods total over five years by renewals may convert the employment contract to an indefinite term employment contract by requesting 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 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 employment contract. The employer must abide by a 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 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 the dismissal, practically, the employers sometimes offer a certain monetary package that would induce an employee 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 a general rule, (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 percent 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, the 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 organization 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 organization 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) grant of the 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 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 working of the patent, the employer's burden and contribution to the invention and 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 the 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 to the author.

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.

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 rights, the formalities of these transactions are different.

Rights in registered patents can be assigned to any party upon registration of the assignment. Copyright and neighboring 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 its registration, which is required in order for the pledge to be valid and enforceable. Copyright and neighboring 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.

Taro Awataguchi
Anderson Mōri & Tomotsune
Akasaka K-Tower, 2-7, Motoakasaka
1-chome, Minato-ku
Tokyo 107-0051
Japan

Tel: *+81 3 6894 1073*
Email: *taro.awataguchi@amt-law.com*
URL: *www.amt-law.com/en*

Taro Awataguchi has extensive experience in the field of banking, financing and insolvency, and is recognised by *Best Lawyers* (banking and financing law). He also advises clients on legal matters of FinTech and virtual currencies. He was appointed by the Japanese court as the trustee in bankruptcy proceedings of a bitcoin related company where various disputes related to bitcoin were involved. He is a frequent lecturer on finance matters and spoke on "Cryptocurrencies" at the American Bar Association (ABA) Section of International Law 2016 Fall Meeting held in Tokyo. He is also noted for successful creditor representations in various cross-border collection/insolvency matters.

Ken Kawai
Anderson Mōri & Tomotsune
Akasaka K-Tower, 2-7, Motoakasaka
1-chome, Minato-ku
Tokyo 107-0051
Japan

Tel: *+81 3 6894 2053*
Email: *ken.kawai@amt-law.com*
URL: *www.amt-law.com/en*

Ken Kawai has extensive experience advising financial institutions, investors and corporate clients on litigation, complex finance and financial regulatory matters.

Ken's focus has been on derivatives. He counsels global banks, broker-dealers and investors on regulatory matters and best practices regarding derivatives and related products. His in-depth understanding of the actual practices derives from his 17-year career at The Bank of Tokyo Ltd./The Bank of Tokyo-Mitsubishi (presently The Bank of Tokyo-Mitsubishi UFJ Ltd.), where he mainly engaged in derivatives trading and marketing.

Ken has also been very actively advising fintech companies, financial institutions and self-regulatory organisations on fintech legal issues including those of payments, personal financial managements, cryptocurrencies and blockchain.

ANDERSON
MŌRI &
TOMOTSUNE

Anderson Mori & 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

Dominic Rebelo

Sonal Sejpal

Anjarwalla & Khanna 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 within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Kenya is experiencing a surge in investments in fintech business, driven mainly by the penetration of mobile telephony and the receptiveness to innovations in the technological arena. The MPESA mobile money transfer platform, which started in Kenya, received global acclaim and has been subsequently launched in a number of countries across the globe. This innovation has enabled 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; and mobile payment systems.

Other notable fintech businesses in the process of being rolled out in the country include peer-to-peer lending and payment platforms, business-to-business lending and payment platforms, online payment systems, online trading, online foreign exchange platforms, online procurement and the more recent blockchain applications.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

There are currently no prohibitions on fintech businesses in the country and the regulator of the financial sector, the Central Bank of Kenya (**CBK**), appears to be receptive to these innovations. For instance, in 2007, the CBK gave a letter of no objection to Safaricom Limited, the mobile operator which sought to operate the first mobile e-money transfer platform in Kenya (**MPESA**), at a time when there was no regulatory framework in place and allowed MPESA to proceed under the oversight of the CBK pending a complete regulatory framework. Since then, the National Payment Systems Act (Act Number 39 of 2011 of the Laws of Kenya) (the **NPS Act**) has been enacted, which governs payment service providers in Kenya. The Communications Authority of Kenya is also receptive to these innovations.

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 considers that virtual currencies are not legal tender and, as such, no protection is available if the system collapses.

Despite the CBK declining to grant licences to deal with bitcoins, there are fintech businesses dealing with bitcoins in the country. It remains unclear how the CBK will deal with these businesses as they are currently unregulated and we are not aware of any proposed regulations on virtual currencies.

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 or equity financing. Equity financing is preferred as it avoids front loading often associated with debt financing. Early stage fintech business operations are often financed by convertible debt or issuance of preference share to investors.

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 for fintech businesses in the country. However, foreign investors investing at least USD 100,000 may apply for registration with the Kenyan Investment Authority (KenInvest) which can assist investors in obtaining tax registration, government permits and authorisations including work permits.

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

Listing on the Nairobi Stock Exchange (**NSE**) must be approved by the Capital Markets Authority on satisfaction of various listing requirements. These requirements include the need to ensure that the companies' memorandum and articles of association conform with the guidelines on corporate governance for listed companies and the rules regarding immobilised securities. There must be at least three non-executive directors in the company and the chairperson of the board must not hold a chair position in more than two listed companies. The companies must also meet the capital requirements depending on their investment segment: 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 who will ensure that listing requirements are satisfied. For a company listing on 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.

The GEMS market allows companies without a profit history to list and access public funds.

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 major exits or sales of fintech businesses in the country. 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.

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 and this 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) and the **NPS Act**. 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.

Regulations and guidelines have also been passed to enhance financial regulation including the Money Remittance Regulations which require the licensing of all persons intending to offer money remittance services in the country.

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. In this instance, an approval and licences issued by the Communications Authority of Kenya may be required.

Public issuance of shares is regulated by the Capital Markets Act, CAP. 485 (A) of the laws of Kenya (the **CMA Act**). Companies selling shares through public placements or offers will be required to seek approval from the Capital Markets Authority (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.

3.2 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?

The CBK has, in the past, shown that it is receptive to the development of fintech businesses in the country that deepen financial penetration in the country. The classic example in this respect is the CBK allowing the implementation of a mobile money transfer service while the country did not have legislation governing this innovation. This has been a critical decision that have enabled the development of financial services in the country and served as the basis for the growth of fintech business innovations.

Conversely, the CBK recently issued a public notice to discourage against the use of virtual currencies such as bitcoins which are not considered legal tender. It also noted that it had not licensed any person to deal with bitcoins as virtual currencies are presently unregulated.

The law generally follows technology, with policymakers generally seeking to catch up with technological developments. This generally provides a space for fintech companies to innovate prior to being regulated.

3.3 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 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 and/or IRA depending on the type of business that they wish to carry on before accessing customers in Kenya.

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?

Kenya does not have a statute specifically dealing with handling of personal data, but there is a bill pending before Parliament – the Data Protection Bill – which seeks to regulate the collection and use of personal data. This bill is modelled to give effect to the constitutionally guaranteed right to privacy. This right is also reiterated in various international instruments that form part of Kenyan law. Currently, there is no specific legislation on data transfers or protection beyond the broad protections enshrined in the Constitution of Kenya, 2010 (the **Constitution**). The Constitution provides that every person has the right to privacy which, *inter alia*, includes the right not to have information relating to their family or private affairs unnecessarily required or revealed.

Generally, there is no prohibition on the collection, use and transmission of personal data, provided that the consent of the owner of the data has been provided and the person has been informed of the reasons for which the data is being collected. Disclosure of personal data without the owner's consent may be considered to be infringement on the right to privacy, save for where Kenyan law expressly provides for the disclosure.

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?

Kenya's data privacy laws apply to organisations established in other jurisdictions in respect of data collected in the country. Organisations are required to give due regard to the right to privacy of the owner when handling this data. However, the enforcement of orders against organisations found to be in breach of this right may be challenging where they have not established a legal presence in Kenya and there no reciprocal enforcement of judgments between Kenya and the country where the organisation is based.

There are no restrictions on the transfer of data outside the country, provided it is done within the remit of the right to privacy. Consent of the owner should be sought where applicable before transferring or storing such data outside the country.

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

Presently, the data privacy laws in the country are founded on the Constitution and a breach constitutes an infringement of the right to privacy. The remedies available include: a declaration of the right to privacy; restriction of the conduct infringing on the right; or an order for compensation. The remedy and quantum is dependent on the circumstances of the case.

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

Kenya is currently developing a legal framework on cyber security through the Cyber Crimes Bill and the Cyber Security and Protection Bill. The two bills are pending in Parliament and it is unclear when they may come into force.

The provisions of the Kenya Information and Communications Act on electronic transactions are relied upon when dealing with cyber security issues. It is expected that once the bills are in force, there will be a robust framework of cyber security laws in the country.

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 (Act Number 9 of 2009 of the Laws of Kenya) is the principal statute on money laundering and provides for ongoing reporting requirements for financial institutions. The Proceeds of Crime and Anti-Money Laundering Regulations, 2013 (the **Anti-Money Laundering Regulations**) also regulate money laundering activities in Kenya. Financial institutions are required to report suspicious transactions and any cash transaction of USD 10,000 or more to the Financial Reporting Centre. In addition, the identity of the customer identity should be verified (Know Your Customer – KYC).

The National Payment System (Anti-Money Laundering Guidelines for the provisions of Mobile Payment Services) Guidelines, 2013 has been promulgated which applies to mobile payment service providers. The provisions of these regulations would apply to fintech businesses which are considered to be reporting institutions under the principal statute.

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

The main regulatory frameworks for fintech businesses are the legal frameworks governing the financial sector and the telecommunications sector. There are other regimes that may also be applicable, including consumer protection law, which is based on the Consumer Protection Act and Competition Act, 2010.

Fintech businesses should adhere to general laws, regulations, rules and guidelines that apply to all businesses generally.

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 laws in Kenya are founded on the Employment Act, 2007, which sets out the relationship between the employer and employee. An employment contract 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 Kenya Shillings. Whilst this statutory provision is clear, we are aware of businesses that pay their staff in hard currency.

An employee may be terminated from employment on account of redundancy, by summary dismissal without notice on certain grounds or by termination by notice for fair reason.

In general, the employment courts in Kenya 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, whose contributions are on a graduated scale based on the pay;
2. a pension scheme through the National Social Security Fund, which has standard contribution;
3. reasonable housing or sufficient allocation to afford reasonable housing;
4. wholesome water; and
5. sufficient medicine during illness and medical attention for serious 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?

The Kenya Citizenship and Immigration Act, 2011 (**KCIA**) requires that foreigners who wish to work in Kenya must obtain a work visa and a work permit to work in the country. In addition, they must also obtain all other documentation that is required by a Kenyan employee. Under the KCIA, an employer is required to procure work permits for its non-Kenyan citizen employees. It is an offence under the KICA to employ a person who requires a work permit and

does not have one. The penalty is a fine not exceeding five hundred thousand shillings (KES 500,000) or imprisonment for a term not exceeding three (3) years, or both. A similar fine is also placed on employees who work illegally.

Foreign investors whose businesses are registered with KenInvest may be entitled to certain work permits.

6 Technology

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

Kenya has an intellectual property regime that guarantees the protection of innovations and inventions as follows:

1. patents, industrial designs, and utility models – Industrial Property Act;
2. trade marks receive protection under the Trade Marks Act;
3. copyright receives 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.

The registered legal owner of 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. An IP holder has the right to alienate, assign or licence the IP rights held in respect of an innovation or invention.

The IP rights only apply within 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)?

One does not need to have local/national registrations in order 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 (**ARIPO**)'s Harare Protocol on Patents and Industrial Designs. The Protocol Relating to the Madrid Agreement Concerning the International Registration of Marks (the Madrid Protocol) also has the force of law in Kenya and therefore trade mark rights may also be registered and enforced in Kenya under its provisions.

Kenya is also a party to the Patent Co-operation Treaty (**PCT**) which provides for an international filing mechanism, but the rights that are yielded at the end of a patent process initiated through the PCT are actually national rights. The PCT therefore grants no substantive rights, but only offers a system of international filing of patent applications.

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.

Dominic Rebelo
Anjarwalla & Khanna Advocates
The Oval, 3rd Floor
Junction of Ring Rd. Parklands & Jalaram Rd.
Westlands, Nairobi
Kenya

Tel: *+254 203 640 000 / +254 703 032 000*
Email: *djr@africalegalnetwork.com*
URL: *www.africalegalnetwork.com/kenya*

Dominic Rebelo is a partner in A&K's Corporate Department. He has wide-ranging experience in corporate mergers and acquisitions, private equity, capital markets and natural resources. 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. He has also assisted a variety of foreign investors in the energy sector in setting up operations in Kenya. Dominic has extensive experience advising tech start-ups, with a focus on fintech, and recently collaborated with FSD Africa on examining the regulatory and public landscape that governs crowdfunding in Kenya. Prior to joining A&K, Dominic was a partner at a prominent Kenyan law firm.

Dominic is ranked as a leading lawyer in Kenya by *Chambers Global*.

Sonal Sejpal
Anjarwalla & Khanna Advocates
The Oval, 3rd Floor
Junction of Ring Rd. Parklands & Jalaram Rd.
Westlands, Nairobi
Kenya

Tel: *+254 203 640 000 / +254 703 032 000*
Email: *ss@africalegalnetwork.com*
URL: *www.africalegalnetwork.com/kenya*

Sonal has been a full-time Director with A&K for over 18 years. Sonal is also a Director at ATZ Law Chambers in Tanzania. Prior to joining A&K, Sonal was a partner at Franks Charlesly & Co. in London. She is a Solicitor of the Supreme Court of England and Wales with considerable experience in banking and finance, natural resources, company commercial and employment law.

Sonal is a regular speaker on various aspects of banking and commercial law and has contributed to a number of publications, including the Kenyan chapters for Aircraft Finance: Registration Security and Enforcement and Aircraft Liens & Detention Rights published by Sweet & Maxwell. In addition, Sonal sits on the Board of Directors of Liberty Life Insurance Company and Heritage Insurance Company. She is the Vice Chairperson of the British Business Association of Kenya.

Sonal is ranked as a leading lawyer in Kenya in *Chambers Global*, *IFLR 1000*, *The Legal 500*, *Euromoney Guide to the World's Leading Project Finance Lawyers*, and *PLC Which Lawyer?*

A&K | ALN
ANJARWALLA & KHANNA

Anjarwalla & Khanna (A&K) is generally considered the leading corporate law firm in Kenya and is one of the largest full-service corporate law firms in Africa outside of South Africa with over 90 lawyers. Our client base is made of both local and international clients. We regularly act for several of the largest and most sophisticated players in the region. A&K has offices in both Nairobi and Mombasa, and sister firms in Dar es Salaam, Tanzania (ATZ Law Chambers) and Dubai, UAE (Anjarwalla Collins & Haidermota). A&K has been named "African Law Firm of the Year" three times in four years at the African Legal Awards. A&K is the founding member of ALN, Africa's widest and most integrated legal alliance of independent top-tier firms. 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 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 big-data-based asset management. The most notable fintech innovation trends are electronic payment services led by major Korean major IT companies and financial institutions. These new electronic payment services tailored to Korean consumers have been generally well accepted in Korea. New banking platforms in the form of internet-only banks, such as K-Bank and Kakao Bank, have been introduced in Korea. These internet-only banks have also been developed by major Korean IT companies and financial institutions, or through a consortium of major IT companies and financial institutions.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

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 licencing requirements, please refer to our answer in question 3.1 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)?

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 Financial Investment Services and Capital Markets Act (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 700 million per year through crowdfunding. To raise funds that exceed KRW 700 million, conventional means of financing should be utilised. Moreover, under the FSCMA, the issuance of equity for crowdfunding is permitted for non-listed small to mid-sized companies with less than seven years of business operations.

Debt

New and growing business may borrow through P2P lending in Korea. The Korean P2P lending industry has grown significantly in recent years. For example, the total amount of loans outstanding in the P2P lending industry in the fourth quarter of 2016 increased more than four times when compared to the first quarter of 2016. Due to the sharp increase in P2P borrowing in Korea, the Korean financial regulatory authorities published a P2P Loan Guideline on February 2017 to better regulate the P2P lending industry. For ordinary individual investors who are P2P lenders, the P2P Loan Guideline sets a monetary limit between KRW 5–40 million, which varies depending on the income of the ordinary individual investor. Whereas, the P2P Loan Guideline does not set a monetary limit for P2P lenders who are either corporate investors or individual expert investors. However, there is no loan amount limit for borrowers in P2P lending under the P2P Loan Guideline.

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.

- The 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 its business income.
- Those companies identified as a "venture business" by the Korean Government, which many fintech companies may

qualify, may receive 50% corporate tax relief even though they are located in highly populated cities in Korea.

- Research and development (R&D) tax deduction is available for certain R&D costs (including labour costs and material costs) that satisfy certain legal requirements, which may be relevant to tech/fintech businesses or small/medium-sized businesses with R&D activities.

These special incentives are not specific to the tech/fintech sectors or small/medium sized businesses as they 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 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 large companies with equity capital of KRW 30 billion or more); (ii) the KOSDAQ (for stocks issued mainly by small to medium-sized but rapidly growing companies with equity capital of KRW 1 billion or more); and (iii) the KONEX (for stocks issued mainly by small to medium-sized start-up companies).

The KONEX market was introduced to provide small to medium-sized companies with IPO opportunities as an alternative to the KOSPI or KOSDAQ market. The KRX does not apply the rigorous financial requirements, when compared to the KOSPI and KOSDAQ, for a KONEX market listing so that start-up companies in the early stages of a business can list in the Korean securities market. As a result, the KONEX market has opened IPO opportunities for start-up fintech and/or small to medium-sized companies, which may find it difficult to meet the KOSPI or KOSDAQ listing requirements.

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 all electronic financial transactions in Korea. Specifically, the EFTA includes: (i) the 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 Financial Services Commission (FSC), the above types of electronic financial businesses must be registered with the FSC and are subject to supervision 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 intends to undertake regulated activities in Korea, such as banking or credit card businesses, should review whether it is required to obtain appropriate authorization (license or registration) from the relevant Korean regulatory authorities such as the FSC or the FSS.

3.2 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?

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. In 2015, 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. As a result of the Korean Government's initiatives in the fintech sector, innovative business models, such as internet-only banks and online payment services tailored to Korean consumers, have entered the Korean market, and an increasing number of information and communications technology companies, both foreign and domestic, expanded into financial services in Korea.

3.3 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 Korea, it will need to obtain authorisation from the relevant Korean financial regulatory authority (as discussed in our answer to question 3.1 above). Typically, the standard to determine the applicability of Korean laws to foreign fintech businesses is whether the foreign fintech businesses targeted Korean customers (e.g., Korean website) or allowed 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 general 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 the 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 Use and Protection of Credit Information Act (Credit Information Act) and the Act on the Promotion of IT Network Use and Information Protection (Network 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 may also 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 taken 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 Interior (MOI) is responsible for enforcing the PIPA. The Korean Communications Commission (KCC) is responsible for enforcing the Network Act. The FSC, the FSS and the Ministry of Science, ICT and Future Planning (MSIP) 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 prosecutor's 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?

Since cyber security is mainly an issue in the context of privacy and data protection, the main statutes in the context of cyber security that may apply to fintech businesses are the PIPA and the Network Act. The PIPA and the Network Act prescribes 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 regime in Korea is generally governed by the Act on Reporting and Using Specified Financial Transaction Information (also know as Financial Transaction Reporting Act or FTRA) and the Act on Regulation and Punishment of Criminal Proceeds Concealment (also known as Proceeds of Crime Act or POCA).

The FTRA regulates money laundering activities committed 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 those financial institutions that are licensed

under the Korean financial regulations, and therefore fintech businesses that are regulated 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 others, they became aware that transacted assets are criminal proceeds or that the counterparty is engaged in the crime of concealment of criminal proceeds.

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 issuance or dealing of foreign exchange and payment, collection and receipt between the Korea and a foreign country.
- Act on Consumer Protection in e-Commerce, which regulates online retailers, any person who is 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 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 (i.e., layoff). However, in each such case, unilateral termination would require that the company meet 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 6,470 per hour (about US$5.70 per hour) as of 2017, pursuant to 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 all 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 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 to be 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, 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. 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 substantial 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 on the patent register 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 of 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 rights 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 licenced through an exclusive or non-exclusive agreement for royalties or may be licenced 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 practice 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 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 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, 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. Lee is also licensed to practice 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 foreign attorney at Kim & Chang. He practices primarily focuses on general regulatory compliance for financial institutions and high-tech/internet companies. 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 receipient 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. We provide legal advice of the highest quality. Our successful track record and relentless dedication to our clients have set us apart since our founding in 1973. Many of the world's largest companies have turned to us for smart and innovative solutions to their most difficult challenges. Today, more than 1,200 professionals work seamlessly together on a task force basis to achieve outstanding results. We are home to lawyers licensed in Korea, U.S., China, France, Germany, U.K., Canada, Australia, New Zealand, Belgium and in the Netherlands.

Malaysia

Timothy Siaw

Shearn Delamore & Co.

Elyse Diong

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 within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

The Securities Commission Malaysia ("SC") has recognised the rise of peer-to-peer ("P2P") financing and crowdfunding platforms in Malaysia in recent years.

In 2015, 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.

In 2016, the SC introduced the regulatory framework for P2P lending, allowing small and medium-sized companies access to this avenue for debt funding.

The Malaysian Islamic Financial Services Board is seeing a growing demand for financial technology in the Malaysian financial services system.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

There are currently no 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)?

Apart from funding from financial institutions, the Malaysian Government provides financing schemes to assist small and medium enterprises start or grow their businesses such as guarantee schemes, Government special funds and micro-finance schemes.

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.

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. The main incentives are Pioneer Status, Investment Tax Allowance, Reinvestment Allowance, Accelerated Capital Allowance and Industrial Building Allowance.

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

All companies seeking listing on Bursa Malaysia are required to obtain the approval of the SC and the main listing requirements can be found at:

http://www.bursamalaysia.com/misc/system/assets/15741/listing_requirement_main_market_consolidated_010317.pdf.

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.

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 activities which entail banking, banking, insurance or takaful, money changing, and remittance, operating a payment system or issuing payment instruments will come under the purview of the Malaysian Central Bank, Bank Negara Malaysia ("BNM"). The Financial Services Act 2013 ("FSA") provides for the regulation

and supervision of financial institutions, payment systems and other relevant entities and the oversight of the money market and foreign exchange market.

In 2016, BNM launched the Financial Technology Regulatory Sandbox Framework ("the 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 Framework provides for innovation by fintech companies to be deployed and tested in a live environment, within specified parameters and timeframes. The Framework is applicable to the following fintech entities:

(a) a fintech company which collaborates with a financial institution; and

(b) a fintech company intending to carry on:

(i) an authorised or registered business as defined in the FSA; and

(ii) an authorised business as defined in the Islamic Financial Services Act 2013 ("IFSA"); or

(iii) a money services business as defined in the Money Services Business Act 2011 ("MSBA").

Upon completion of the testing, BNM will decide 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 FSA, IFSA and MSBA.

Furthermore, the SC has introduced the regulatory framework for P2P lending and set out the requirements for the registration and obligations of a P2P operator in its revised Guidelines on Recognised Markets in April 2016. The P2P framework enables sole proprietorships, partnerships, incorporated limited liability partnerships, private limited and unlisted public companies access to market-based financing to fund their projects or businesses via an electronic platform. The P2P framework places obligations on the P2P operators to:

(a) ensure there is efficient and transparent risk scoring system in place relating to the Investment note or Islamic investment note;

(b) carry out a risk assessment on prospective issuers intending to use its platform;

(c) monitor and ensure compliance with its rules;

(d) carry out investor education programmes;

(e) ensure that the issuer's disclosure documents lodged with the P2P operator are verified for accuracy and made accessible to investors through the platform; and

(f) have in place processes to monitor anti-money laundering requirements.

Parties who are interested to operate a P2P platform may submit their application to the SC and they must be locally incorporated and have a minimum paid-up capital of RM 5 million.

3.2 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?

BNM, the SC as well as Malaysia Digital Economy Corporation ("MDEC") are all supportive of providing an environment which is conducive of fintech innovations and deployment. 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 ("ICT") industry, and the adoption of digital technology amongst Malaysians.

The Financial Technology Regulatory Sandbox Framework was launched in October 2016 by BNM only after having taken into account the comments and suggestions from numerous fintech companies, financial institutions and fintech associations.

In 2015, the SC launched the "Alliance of FinTech Community" or "aFINity@SC", an initiative to provide to catalyse greater interest towards the development of emerging technology-driven innovations in financial services, whether existing or prospectively developing in Malaysia.

3.3 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 question 3.1.

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 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. "Commercial transactions" is defined to include 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 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. The PDPA allow applied to data users not established in Malaysia, but use equipment in Malaysia to process personal data otherwise than for the purposes of transit through Malaysia.

A data user may transfer personal data outside of Malaysia under the following conditions:

(a) data subject has given consent to 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 this Act; and

(g) the transfer is necessary in order to protect the vital interests of the data subject; or the transfer is necessary as being in the public interest in circumstances as determined by the Minister.

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.

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

The following cyber security laws or regulations which have general application in Malaysia:

(a) Communications and Multimedia Act 1998;

(b) Communications and Multimedia Commission Act 1998;

(c) Malaysian Communications and Multimedia Content Code (Version 6, published in 2012);

(d) Computer Crimes Act 1997;

(e) Digital Signature Act 1997;

(f) Copyright Act 1987;

(g) Electronic Commerce Act 2006;

(h) Consumer Protection Act 1999; and

(i) Consumer Protection (Electronic Trade Transactions) Regulations 2012.

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

The Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 provides that it is a money laundering offence in Malaysia to do the following:

(a) engage directly or indirectly in a transaction that involves proceeds of an unlawful activity or instrumentalities of an offence;

(b) acquire, receive, possess, disguise, transfer, convert, exchange, carry, dispose of or use proceeds of an unlawful activity or instrumentalities of an offence;

(c) remove from or bring into Malaysia proceeds of an unlawful activity or instrumentalities of an offence; or

(d) conceal, disguise or impede the establishment of the true nature, origin, location, movement, disposition, title of, rights with respect to, or ownership of, proceeds of an unlawful activity or instrumentalities of an offence.

Upon conviction, a person may be liable to imprisonment of a term not exceeding 15 years and shall also be liable to a fine of not less than five times the sum or value of the proceeds of the unlawful activity or instrumentalities of an offence at the time the offence was committed or five million ringgit, whichever is higher.

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

Please see question 3.1.

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?

The following legislations are 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 RM 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 period 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 Malaysia Digital Economy Corporation ("MDEC"). Companies

with MSC Status are eligible to apply for special employment passess and exemptions to employ foreign knowledge workers.

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.

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

Copyright

Under the Copyright Act 1987, the copyright shall vest initially in the author of the copyrighted work except:

(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;

(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; and

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 Mark

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.

Patent

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, employees of 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; and

(b) industrial designs created by an employee in the course of employment, the employer is the original owner; and

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, 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.

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.

Timothy Siaw
Shearn Delamore & Co.
1 Leboh Ampang
Wisma Hamzah Kwong-Hing
Kuala Lumpur 50100
Malaysia

Tel: *+603 2027 2660*
Email: *timothy@shearndelamore.com*
URL: *www.shearndelamore.com*

Timothy Siaw has degrees in science and law from Monash University, Australia and has been admitted as a Barrister and Solicitor of the Supreme Court of Victoria, Australia and as an Advocate and Solicitor of the High Court of Malaya. He is a partner in the IP and Communications & Technology practice groups in Shearn Delamore & Co.

Elyse Diong
Shearn Delamore & Co.
1 Leboh Ampang
Wisma Hamzah Kwong-Hing
Kuala Lumpur 50100
Malaysia

Tel: *+603 2027 2669*
Email: *elysediong@shearndelamore.com*
URL: *www.shearndelamore.com*

Elyse Diong has a LL.B. (Hons) from the University of London and is a legal associate of the IP and Communications & Technology practice groups in Shearn Delamore & Co.

Shearn Delamore &co.

Established in 1905, Shearn Delamore & Co. is today one of the largest full-service law firms in Malaysia with 50 partners, around 52 legal associates and around 280 support staff. Our firm has garnered numerous accolades and awards and recently, the Malaysian Law Firm of the Year at the Chambers Asia Pacific Awards 2017 and many of our partners have consistently been recognised as leaders in their areas of practice. We are focused on providing and delivering a full range of legal solutions promptly and effectively. At Shearn Delamore & Co. we value quality, integrity and practicality.

Malta

Dr. Andrew J. Zammit

Dr. Michael Grech

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 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 having 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 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.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

Whilst no specific types of fintech businesses are prohibited in Malta, the Malta Financial Services Authority ("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.

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 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, 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.

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.

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.

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 establishing a presence on the island, and this has seen significant growth in the Maltese economy, particularly over the past seven years.

In addition to the corporate tax incentives, fintech businesses regulated by the MFSA may also attract top talent to Malta through the 15% personal tax rate that is granted to qualified expatriates working in key positions with fintech and other financial services operators in Malta, which is known as the Highly Qualified Persons programme. This measure, which applies both to EU and non-EU nationals, 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.

Venture capital financing is not available in Malta and most entrepreneurs seeking to base their businesses in Malta invariable source financing for their business from 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 EU Prospectus Directive.

- Shareholders' funds less intangible assets must be of at least €585,000.
- 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 €1,165,000 (not being Preference Shares).
- At least twenty-five percent (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.

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 Malta Financial Services Authority, also referred to as the MFSA, is the regulatory authority charged with the power to regulate, monitor and supervise all 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 witnessed technological developments that have created innovative fintech business propositions although admittedly payment related services have seen the most innovation over recent years.

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. One would therefore find laws such as the Banking Act, the Financial Institutions Act, the Investment Services Act and the Insurance Business Act. Therefore fintech activities would be regulated in the same way that the corresponding non-fintech businesses (that is more traditional bricks-and-mortar operations) would. There has, however, been significant focus on the part of the MFSA to introduce regulations, rules and policies which serve to address specific risks and concerns that are relevant for fintech models, revolving principally around security and technological standards.

3.2 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?

The MFSA is receptive to fintech innovation and technology-driven financial services operators and takes up 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.

3.3 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 provide cross-border services or to establish a branch in Malta. If a branch is established 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 440 of the Laws of Malta) ("DPA") and its subsidiary legislation provide for the protection of individuals against the violation of their privacy by the processing of personal data. The provisions of this statute implement the provisions of the EU's Data Protection Directive.

The processing of data effectively refers to the processing (whether automated, mechanical, manual or otherwise) of a person's data in a filing system, or in what is intended to form part of a filing system.

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?

Maltese Data Protection Law applies to:

- Data controllers established in Malta.
- Data controllers in a Maltese Embassy or High Commission outside Malta.
- Equipment used for processing and situated in Malta, even where the Controller is established outside the EU.

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

Penalties for non-compliance with the Data Protection Act 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 Courts of Malta may impose the following penalties:

- Level 1: Fine of between €120 and €600, imprisonment of not more than one month.
- Level 2: Fine of between €250 and €2,500, imprisonment of between one and three months.
- Level 3: Fine of between €2,500 and €23,300, imprisonment of between three and six months.

The Data Protection Commissioner may impose the following fines without recourse to a court hearing:

- Level 1: Fine of between €120 and €600, or a daily fine of between €20 and €60.
- Level 2: Fine of between €250 and €2,500, or a daily fine of between €25 and €250.
- Level 3: Fine of between €2,500 and €23,300, or a daily fine of between €250 and €2,500.

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 does deal 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 is also signatory to the Council of Europe Cybercrime Convention since 2001, which 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's status as a full member of the EU and 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 talent to Malta, including 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 in 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 approx. 420,000). 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.

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 usual tax and social security registration and a notification procedure intended for statistical purposes. Citizens of other countries 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 difficulty, although such permits can involve a waiting time of up to 90 days until approved.

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 is 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 6*bis* 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 to 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.

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. Michael Grech
GVZH Advocates
192, Old Bakery Street
Valletta
Malta

Tel: +356 2122 8888
Email: michael.grech@gvzh.com.mt
URL: www.gvzh.com.mt

Dr. Michael Grech is a partner at GVZH Advocates, heading the intellectual property department at GVZH Advocates. His practice focuses on all aspects of intellectual property law including the representation of several multi-national clients in all aspects of IP law, including brand protection and anti-counterfeiting.

Michael also assists the firm's commercial and corporate department and is part of the firm's team on privatisation matters, advising the Government of Malta as well as private clients. He sits on the boards of a number of local companies including three publicly listed companies.

Michael is the Chairman of *Teatru Manoel*, Malta's national theatre, and a member of the Boards of *Governors of Fondazzjoni Patrimonju Malti* and St. Edward's College. He is a Knight of Magistral Grace of the Sovereign Military Order of Malta.

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

Mariana Islas

Claudio Kurc

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 within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

While Fintech is a nascent industry in Mexico, according to Fintech Radar Mexico's website (http://www.finnovista.com/fintech-radar-mexico), the main fintech business models identified in Mexico are: payments and Remittances; Lending; Enterprise Financial Management; Personal Financial Management; Crowdfunding; Wealth Management; Insurance; Financial Education and Savings; Scoring, Identity and Fraud Solutions; and Trading and Markets.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

There is no fintech-specific regulation in Mexico. However, some of the fintech business activities fall on one or more restricted activities (e.g., under banking, securities market, mutual funds, insurance companies and other statutes regulating activities of similar import). Generally speaking, issuance of currency, solicitation of money deposits, public offering of securities, acting as 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 start-ups would generally not qualify. Venture capital and private equity are also available to new 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?

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.

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 must convert into SAB 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 IPO, according to Expansion Magazine's article issued on March 2017, there have been several notable investment rounds on fintech businesses in the past few years. Kueski, a lending platform, announced a USD 35 mm debt and equity round, currently the largest funding in the Mexican fintech market. Konfio, another lending platform, raised USD 8 mm in an equity round; Clip, a payment processor platform, raised USD 8 mm in an equity round; and Kubo Financiero, a P2P

lending platform, raised USD 7.5 mm in an equity round (TOLAMA, Jimena, *et.al*. Expansión, *El Huracán Fintech*, 2017).

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 currently no regulatory framework applicable to fintech businesses operating within the Mexican jurisdiction. Therefore, no fintech activities are explicitly regulated. However, as mentioned in question 1.2, certain fintech activities are subject to financial (non-fintech) regulation.

3.2 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?

Mexican financial regulators and policy makers are very receptive to fintech innovation. Despite there being no regulatory framework for fintech businesses, throughout the past year, the federal government has been working on a fintech law and has had copious interaction with entrepreneurs and high-ranking officers of various fintech startups. For example, on June 2016, Mexico announced the National Policy for Financial Inclusion which has as main axis to use technology innovations to increase the scope and depth of financial products and services, through a regulatory framework that provides a secure environment for both fintech startups and its clients. On May of 2016, the then Minister of Finance visited Silicon Valley to meet with fintech entrepreneurs and investors, to better understand the industry. The Ministry of Finance and Public Credit has recently announced that a draft bill to regulate fintech has been shared with the private sector for feedback.

3.3 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?

Current restrictions on the provision of financial services are generally territorial. This means that, with some exceptions, the activity would need to be carried out within Mexican territory to be the subject matter of regulation. By its nature, fintech defies the territorial limitations encountered by traditional *brick-and-mortar* businesses. This phenomenon allows some fintechs to find a way around the regulation, simply by not having a physical presence in Mexico or not specifically targeting Mexican residents. However, for other fintechs this lack of clarity entails a level of uncertainty that undermines their business models. The specifics of each case make it hard to derive general rules on how to overcome local regulatory hurdles.

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. These statutes are applicable to anyone that collects personal data pertaining to individuals (other than credit bureaus, which are exempt from these statutes).

Fintechs, as any other business, must provide 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.

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 personal data is processed by an establishment of the controller 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 via the privacy notice the personal data subject to international transfers, the purpose of the transfer and the third party to whom the data will be disclosed. Said transfers ordinarily only require the data owner's consent. However, such consent is not necessary under certain conditions, such as when it is established in an international treaty or whenever such transfer is made by virtue of an agreement. The terms and conditions governing the transfers must be established in contractual clauses, stating that the recipient of the data shall assume the same obligations regarding the protection of the personal data as the issuer that collected the data subjects' personal information.

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, comply with legal restrictions to transfer personal data, among other actions. Fines go up to USD 0.3 mm 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?

Banking regulations require entities that use electronic means to perform financial services and operations to have cryptographic safeguards and develop policies to protect information stored, processed or transferred through such means.

Cyber-attacks, hacking, virus infection and other cyber-crimes constitute punishable criminal offences. The National Security Program (2014–2018) includes among its objectives the creation of a regulatory framework applicable to cyber security.

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 fintech businesses, as well as by any person involved in lending activities. Among the AML requirements that fintech businesses have to comply with are the following:

- Verify client's identity.
- Identify the beneficiaries of transactions.
- Give notice of suspicious transactions.
- Have internal manuals.
- Register with the AML overseer.
- File monthly reports.

In addition, fintech businesses registered as a regulated entity (e.g., a licensed bank, non-bank bank, thrift, broker-dealer, etc.) are subject to specific AML provisions. Among the additional obligations are:

- 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 to Blocked Persons and Politically Exposed Persons.

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

Besides the regulatory framework established in this chapter, there are a number of additional regulations applicable to fintech businesses in Mexico; for example: the General Law on Commercial Corporations, or in some cases the Securities Market Law, determines 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. 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 and the Federal Law on Consumer Protection, both of which determine certain information that must be available to consumers, such as product information and fees. Such regulations also establish the safeguards available to clients whenever the service provider fails to comply witch 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.

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?

As a general rule, employment relationships in Mexico are for an indefinite period of time. 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 employee's dismissal, the Law provides employers may terminate an employment relationship at any time so long as the termination is based on a limited number of causes. An employee terminated without legal cause may demand reinstallation or severance.

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

Employee benefits mandated by the Law are the following:

- Salary, which cannot be lower than the minimum wage at force at the time.
- Working schedule, which shall not require more than 48 working hours per week and shall contemplate at least one day of rest.
- Annual vacations that shall be equivalent to six days in the first year of employment and shall increase annually in proportion to the years of seniority of the employee.

- Vacation premium of at least 25%.
- Christmas bonus equivalent to 15 days of salary to be paid no later than December 20th of each year.
- Payment of profit sharing equivalent to 10% of the employer's pre-taxes annual profits.

The Law also regulates the payments that must be made in the event of overtime.

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. No special route for obtaining permission for individuals who wish to work for fintech businesses are available.

6 Technology

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

In Mexico, most of 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 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 (twenty) years; industrial designs have a protection of 15 (fifteen) years, and utility models have a protection of 10 (ten) 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) patrimonial rights over a computer program shall be protected for a term consisting of the life of the author plus 100 (one hundred) years after his death. Moral rights protection do 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 transferring, 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 it. The assignment of computer programs is not subject to any time limitations generally found in other copyrights.

Mariana Islas
Galicia Abogados, S.C.
Av. Ricardo Margain, No. 440, Piso 9
Despacho 901, Valle del Campestre, 66259
San Pedro Garza García, N.L.
Mexico

Tel: +52 81 9689 9030
Email: mislas@galicia.com.mx
URL: www.galicia.com.mx

Mariana Islas' professional practice focuses on M&A, contracts and corporate matters. She has participated in several cross-border transactions and corporate restructures for companies in the manufacturing industry. She also has experience regarding foreign investment, real estate and environmental matters.

Prior to joining Galicia Abogados, she worked at Basham, Ringe y Correa. She studied law at Instituto Tecnológico y de Estudios Superiores de Monterrey where she graduated with honours, and imparted a diploma course on Corporate Law at her alma mater.

Claudio Kurc
Galicia Abogados, S.C.
Blvd. Manuel Ávila Camacho #24
7º Piso, Col. Lomas de Chapultepec, 11000
Mexico City
Mexico

Tel: +52 55 55 40 92 00
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, 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.

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 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.

Netherlands

Bart van Reeken

De Brauw Blackstone Westbroek

Björn Schep

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 within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Over the last few years, trends in the Netherlands included 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 types 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 denominators such as InsurTech, BigTech, PensionTech and RegTech.

Besides new initiatives from start-ups, established financial companies in the banking and insurance sector are also very active with regard to innovation. Various large banks in the Netherlands have set up internal innovation platforms and because the Dutch insurance market is under a lot of pressure due to low interest rates, a saturated market and low margins, insurers are focussed on developing new innovative business models.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

There are no specific rules and regulations that prohibit or restrict fintech business in the Netherlands. However, the financial services sector is a heavily regulated area. Therefore, there is a substantial risk that fintech businesses are confronted with established financial regulatory policies, rules and regulations. In the case that the fintech business provides a regulated financial service, such as the offering of consumer credit, payment services or insurance services, it has to comply with the relevant rules and regulations, even if the business is more "tech" than "fin".

If the fintech business provides a regulated financial service, such as the offering of consumer credit, payment services or insurance services, it has to comply with the relevant rules and regulations.

The Dutch Central Bank ("DNB") and the Netherlands Authority for the Financial Markets ("AFM") are aware of the fact that current rules do sometimes not fit well with the proposed fintech solutions and are increasingly adapting a positive and constructive attitude towards innovation in the financial services sector.

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 an increasingly popular listing venue, Euronext Amsterdam, which are accessible to fintech businesses above a certain size.

Whilst 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 or expanding fintech businesses in Europe. This is, amongst other things, the result of the absence of withholding taxes on interest and royalties and the possibility to often repatriate profits derived from European activities with no, or minimal, tax leakage. In addition, the following tax incentives may be available to fintech businesses:

Innovation box

The innovation box regime provides for profits derived from certain qualifying self-developed intangibles (e.g. software) being taxed at an effective rate of 5% 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 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 up to 30% during a maximum period of eight years. The foregoing effectively results in only the remaining 70% being subject to income tax.

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 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 that will allow the 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?

Although the Netherlands has become a global fintech hub, it has yet to see its first fintech business IPO or big sale of business. The trend in the fintech sector is to collaborate with venture capital firms or to partner up with incumbents, rather than selling a fintech business in its entirety.

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. Most fintech activities pertain to the 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 the relevant regulated financial entity.

Regulated activities are amongst others offering consumer credit, acting as an intermediary in financial products (e.g. insurances, consumer credit), acting as a bank, offering insurance and providing payment services.

The Netherlands adheres to a functional supervisory model (twin-peaks model). In this model DNB is charged with the supervision of prudential rules (e.g. capital adequacy), whereas the AFM oversees compliance with market conduct rules (e.g. KYC).

3.2 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?

The financial regulators and policy makers in the Netherlands are very receptive to fintech businesses and try to facilitate fintech businesses as much as possible.

Financial regulators

To support businesses that seek to implement innovative financial business models or products, but are unsure about the specific relevant rules, in June 2016, DNB and the AFM set up the InnovationHub. The InnovationHub offers new businesses and incumbents the opportunity to submit questions about regulations directly to DNB or the AFM, regardless of whether they are currently subject to a regulatory framework. Following the successful introduction of the InnovationHub, to further facilitate innovation and to enable businesses to launch their innovative financial products without unnecessary (regulatory) hindrance, DNB and the AFM have created a regulatory sandbox from 1 January 2017. 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 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 therefore expected to hugely support innovation in the financial services sector. The regulatory sandbox is open for start-ups as well as established financial companies active in the Netherlands.

Policy-makers

In March 2016, the Dutch Minister of Economic Affairs and the Dutch Minister of Finance briefed the Dutch Parliament on the opportunities and risks that fintech business offer to the Dutch economy. To ensure that the described opportunities can be seized, the Dutch policy-makers and financial regulators proposed to implement the following three policy lines:

- to remove potential impediments (e.g. difficulties in obtaining a licence);
- to safeguard the financial sector (e.g. improving the knowledge of the financial regulators with regard to applied technologies); and
- to seize opportunities (e.g. improving the profile of the Netherlands as a centre of financial innovation).

3.3 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 customers in the Netherlands will likely trigger Dutch financial regulatory law. In those cases, offering the financial services or financial products is in principle subject to prior authorisation by the relevant Dutch regulator (either through a national application for a licence, notification of the relevant regulator or through 'passporting' an EU-Member State authorisation). There are various exemptions and exceptions to this main rule. However, it depends on specific circumstances (e.g. the regulated activity) whether a fintech business may rely on such an exemption or exception. Regulators do, however, 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, in case the financial company will have a large client base in the Netherlands, there is a risk that the relevant Dutch regulator will take the view 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?

The Dutch Data Protection Act (*Wet bescherming persoonsgegevens* – DDPA) regulates the processing of personal data in the Netherlands. The DDPA is the national implementation of the European Data Protection Directive 95/46/EC. As of 25 May 2018, the DDPA will be replaced by the General Data Protection Regulation (GDPR), which will be directly applicable in all EU-Member States.

Fintech businesses that want to collect and use personal data effectively need to determine if they are subject the obligations set out in the DDPA. The DDPA regulates the processing of personal data by organisations established in the Netherlands which determine the purpose and manner in which personal data is processed. Such organisation is defined as a "data controller". Primarily the DDPA requires data controllers to:

- collect personal data only for specified, explicit and legitimate purposes;
- process personal data only if there is a legal basis, such as consent or a legitimate interest; and
- store and process personal data only to the extent necessary for the purpose of the processing.

Furthermore, the DDPA requires data controllers to (i) notify the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*, DPA) before carrying out any automatic processing, (ii) appropriately secure personal data, and (iii) to enter into processing agreements when engaging third party data processors.

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 DDPA applies to the processing of personal data by any controller, whether or not established in the EU, when it uses automated or non-automated means established in the Netherlands. Such non-EU controller must designate an organisation within the Netherlands that acts on his behalf in accordance with the DDPA. Fintech businesses providing a mobile application to users in the Netherlands may be subject to this requirement.

The transfer of personal data within the European Economic Area (EEA) is permitted, since all countries within the EEA provide an adequate level of protection. Data transfers outside of the EEA are only allowed if, amongst other exceptions:

- the EC has recognised this third country as providing adequate protection (i.e. Andorra, Argentina, Canada, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay);
- in case of transfer to the United States: the US recipient adheres to the Privacy Shield Framework (please note that this exception is heavily criticised);
- the data subject (the person whose personal data are processed) gives his explicit consent;
- the transfer is necessary for the conclusion or performance of an agreement to which the data subject is party;
- the controller and the receiving party have entered into a contract that is either (i) based on EU model contracts (Standard Contractual Clauses), or (ii) licensed by the Minister of Justice; and
- binding Corporate Rules are adopted by the controller and its group.

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

In case of infringement of the DDPA, the DPA has both investigative and punitive powers. Investigative powers include the right to order an organisation to provide information to the DPA. Punitive powers include the right to impose administrative sanctions such as orders subject to a penalty and fines of up to EUR 820,000 or 10% of the company's annual net turnover. The DPA may decide to publish a sanction it imposes. Some violations, such as failure to comply with an order to provide information, might also trigger enforcement under other sector specific laws, such as the Dutch Act on Economic Offences (*Wet Economische Delicten*) or trigger civil claims.

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

Under the DDPA, companies must take 'technical and organisational' security measures to protection personal data. This general requirement aims to protect personal data against loss or unlawful processing. A risk-based approach is to be taken. This means that additional security measures may be required for high risk data, such as financial data. Furthermore, data controllers must notify the DPA within 72 hours in the event of a data breach.

Fintech businesses may also be subject to financial markets regulations in place (see question 3.1). These regulations may also require fintech businesses to take appropriate measures to secure any personal data. Finally, fintech businesses products and services of which the availability and reliability are considered vital to Dutch society, may be subject to additional notification and security requirements.

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 (*Wetboek van Strafrecht*, DCC) and the Act for the Prevention of Money Laundering (*Wet ter voorkoming van witwassen en financieren van terrorisme*, WWFT).

Money laundering under the DCC is a wide concept. It entails, amongst 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 six years imprisonment or a fine of up to EUR 82,000.

Secondly, under the WWFT, specific financial institutions are required to undertake certain customer due diligence before they establish business relationships. It depends on the regulated activity of the fintech business whether it will fall in scope of the WWFT. Risk-based due diligence must be conducted, for example, when the company has any doubts on the correctness 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. Other requirements from the WWFT are the duty to report unusual transactions and the requirement to hold sufficient recordkeeping. Failing to comply with these rules is punishable under the Economic Offences Act (*Wet Economische Delicten*, WED). Penalties upon infringement could result in a maximum of two years' imprisonment or fines up to EUR 20,500. In addition, the Dutch Minister of Finance may impose an order for incremental penalty payments and administrative fines with a maximum of EUR 4,000,000 per infringement.

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 that is aimed specifically at the fintech-sector. Fintech businesses providing 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 out 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. The employment agreement has no prescribed form and can be for a definite or an indefinite term. However certain restrictive provisions (e.g. probationary period, non-compete clause, unilateral changes clause, penalty clause) must be agreed to in writing.

Under Dutch law, there are two ways in which the employment agreement can be unilaterally terminated by the employer:

i. giving notice after having obtained a dismissal permit from the Employee Insurance Agency; and

ii. requesting the court to 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 (i) there is a reasonable ground (i.e. the conditions of at least one of the limited grounds have been fully met), and (ii) it is not possible to reassign the employee within a reasonable period of time to a suitable alternative position within the company.

In practice, employment agreements are usually terminated by means of a mutual agreement.

In certain situation, the dismissal of an employee is prohibited, among others during the first two years of illness.

An employee who has been employed for 24 months or more is entitled to a transition payment if the employment is terminated on the initiative of 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 77,000 gross (2017 figures), or one annual salary if the annual salary of the employee exceeds the amount of EUR 77,000 gross (2017 figures).

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

Members of staff are entitled to at least:

i. the applicable 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 (generally 20 vacation days per year on the basis of a full-time contract).

During the first two years of illness the employee is entitled to at least 70% of their salary (unless 70% of their salary is less than the statutory minimum wage, in which case the employee is entitled to the statutory minimum wage). During this period, the employer and employee must work together on the reintegration of the employee. After this two-year period, the obligation to pay the salary ends unless the Employee Insurance Agency is of the opinion that 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 with a maximum of one year.

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 company is obliged to recruit first from within the European Economic Area (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.

The above does not apply in case of highly-skilled migrants. In order to bring highly-skilled migrants to the Netherlands, the employer must be recognised by the IND 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.

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

can, depending on the type of invention, to a certain extent also be protected by other intellectual property rights such as copyrights (software), data base rights and utility models. Technical information and know how 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 of industrial application. A Dutch patent may be applied for at the Dutch Patent Office. Dutch patents are not preliminary 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. It is expected that a European patent with unitary effect will be introduced in the course of 2017 as part of the EU patent package. The European patent with unitary effect is not a bundle of patents but can be directly enforced in all participating EU Member States, amongst which the Netherlands, through the Unified Patent Courts.

Trade secrets

Information is protected to the extent that it (i) is kept secret, (ii) has commercial value because it is secret, and (iii) has been subject to reasonable steps to keep it secret. This follows from Article 39 TRIPS. Because Article 39 TRIPS is not implemented in national legislation, it cannot be relied upon directly. It is, however, deemed to be incorporated in Dutch tort law. The "proprietor" has the possibility of preventing the information from "in a manner contrary to honest commercial practices" being (1) disclosed, (2) acquired, or (3) used by others without its consent. Trade secrets are protected for as long as the conditions under (i) through (iii) are satisfied.

More specific trade secret legislation is expected in the course of 2018 as a result of implementing the EU Trade Secrets Directive.

Copyrights, data base rights, utility models

Except for the protection of source code of software, copyrights, which under Dutch law arise by operation of law, play a limited role in protecting innovations and inventions since (purely) technical information regarding functional aspects is exempt from copyright protection. A (*sui generis*) data base is protected insofar as the data base 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.

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

In principle, a Dutch patent will be owned by the applicant of the patent. Any party (other than the applicant) that claims that it is entitled to the patent, can initiate court proceedings claiming entitlement to a patent.

If an invention has been 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. In case of inventions made during training or by employees of educational or research institutions, the employer and the institutions, respectively, are generally entitled to the patent. This is not mandatory law, however. Employment agreements therefore generally contain arrangements to ensure that all inventions and related rights will be 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 and the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). More specifically applicable for patents are the European Patent Convention (EPC), the Patent Cooperation Treaty (PCT) and the upcoming Unitary Patent Regulation and other corresponding regulations, under which a European patent with unitary effect may be directly enforced in the Netherlands (see under question 6.1). 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.

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 infringe, 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 5% applies for profits and losses resulting from patented inventions.

Bart van Reeken
De Brauw Blackstone Westbroek
Claude Debussylaan 80
1082 MD Amsterdam
The Netherlands

Tel: +31 20 577 1599
Email: Bart.vanReeken@debrauw.com
URL: www.debrauw.com

Bart van Reeken heads De Brauw's information, communication and technology practice. He regularly assists companies in reaching agreement on outsourcings, information technology projects and joint ventures.

Bart's primary focus is structuring effective business relations between companies, both nationally and internationally. Bart is experienced in setting up joint development, mutually integrated production and joint marketing arrangements. He negotiates in a way which contributes to the success of the relationships. In the area of information technology, his work covers a broad spectrum, ranging from regularly assisting in negotiating and drafting outsourcing agreements, software development agreements, software licences, implementation agreements, and telecom agreements, to handling IT-related disputes. He represents both IT suppliers and corporations.

Bart has worked for most of the larger Netherlands-based banks, the largest insurance companies and a few fintech startups.

Björn Schep
De Brauw Blackstone Westbroek
Claude Debussylaan 80
1082 MD Amsterdam
The 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. He regularly advises insurers, banks, investment firms and financial services providers on applicable financial regulatory requirements such as license requirements, prudential requirements and market conduct requirements.

Björn was seconded to Slaughter and May in London in 2012, where he worked in the Financial Regulation group.

Björn is currently following the Executive Master Insurance Studies / Enterprise Risk Management at the Amsterdam Business School and anticipates graduating in August 2017.

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 a few fintech startups, mostly advising them on market access issues.

DE BRAUW
BLACKSTONE
WESTBROEK

De Brauw is the largest law firm in the Netherlands, with offices in Amsterdam, Brussels, Frankfurt, London, New York, 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.

Nigeria

Yinka Edu

Udo Udoma & Belo-Osagie

Tolulope Osindero

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 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 subsector is 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, 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 Unstructured Supplementary Service Data ("USSD") services for payments by bank and non-bank operators and the use of artificial intelligence via chatbox. Licensed banks have also adopted the use of USSD service for payments and transfer services. The competition among the various participants has resulted in new and simplified solutions for funds transfer and payments services. A total transaction value of =N=163.3 billion was processed through mobile money operators in Nigeria during January and February 2017 according to the Electronic Payment Fact Sheet of the Nigerian Interbank Settlement Systems.

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 individual loans and loans for small companies. At interest rates between 40%-70% per annum and with loan size of up to =N=2,500,000 (equivalent of US$8,200), these lenders are gaining on the market share of micro finance banks and other personal banking divisions of traditional banks.

Personal Finance: several fintech businesses and some banks now offer personal savings solutions which are available on mobile phones.

Blockchain: one company that utilises blockchain technology for payments commenced operations in Nigeria in 2016. There are also bitcoin exchanges and other bitcoin wallet providers in Nigeria.

Reward and Donation Crowdfunding are also prevalent in Nigeria.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

There are currently no express regulations restricting or prohibiting any fintech business in Nigeria.

Having said this, section 22(5) of the Companies and Allied Matters Act, Laws of the Federation of Nigeria ("LFN") 2004 and Section 67 of the Investment and Securities Act, 2007 prohibit private companies from offering their securities, whether shares or debentures, to members of the public. The Securities and Exchange Commission (the "SEC"), based on its interpretation of the current regulations, do not permit crowdfunding and 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. Every company limited by shares is required to have share capital under Nigerian law so this makes equity funding the most common type of funding. 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 such as the Aliko Dangote Fund, the Tony Elumelu Entrepreneurial Foundation, the National Information Technology Development Agency ("NITDA") Fund, etc.

As part of its development objectives, the Bank of Industry ("BOI") makes funding available to small businesses generally at more friendly rates through the Youth Entrepreneurship Support Fund and the National Youth Service Fund which are available to technology businesses. The BOI also partners with venture capital funds to provide funding to technology companies. In 2015, the BOI provided funding to mobile based payments company in Lagos State.

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 in Nigeria. We have discussed below some of the incentives that are generally available in Nigeria.

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 of that company.

Pioneer Status: Companies classified as pioneer industries or engaged in the production of pioneer products are entitled to apply for pioneer status, and when granted, 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. Currently, the basis for the grant of this incentive is being reviewed and no companies are being granted pioneer status.

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:

a. accelerated capital allowance for equity investment by a Venture Company in a Venture Project for the first five years of their investment;

b. reduction of withholding of tax on dividends declared by Venture Projects to Venture Companies for the first five years from 10% to 5%;

c. export incentives such as export expansion grants if the Venture Project exports its products;

d. exemption from payment of capital gains tax on gains realised by Venture Companies from a disposal of equity interest in the Venture Project; and

e. 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.

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. A digital payments and switch company had initially planned a dual listing in Nigeria and London in 2016 but this was postponed due to market conditions.

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 market place 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.

Payments: the CBN regulates mobile payments and transfers pursuant to the CBN Guidelines on Mobile Money Services in Nigeria 2015 (the "Guidelines"). The 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.

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 Service ("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. As we understand, 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.

There are no regulations for reward- and donation-based crowdfunding.

3.2 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?

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 the 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. Recently, the CBN set up a committee charged with the obligation of preparing a road map for the policies and guidelines that will guide blockchain technology regulation and a domestic cryptocurrency in Nigeria. Also, the SEC is considering a regulatory framework for equity crowdfunding in Nigeria.

3.3 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 peculiar to a foreign fintech business other than the requirement that any foreign entity who 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 or the NCC or a moneylenders' 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?

There is no specific law on the usage, transmission or collection of data in Nigeria. The following legislation and regulations have provisions on the use or collection 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") 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; 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 programs to prevent 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 observe this right.

d. Draft guidelines on data protection issued by the NITDA. The NITDA Guidelines prescribe the minimum data protection requirements for the collection, storage, processing, management, operation, and technical controls for information and is currently the only set of regulations that contains specific and detailed provisions on the protection, storage, transfer or treatment of personal data. The NITDA Guidelines apply to private sector organisations that own, use or deploy information systems within Nigeria and to organisations outside Nigeria if such organisations process personal data of Nigerian residents. The NITDA Guidelines are currently not being enforced.

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 regulations which we have referred to above apply mostly to Nigerian entities and to entities with operations in Nigeria. Some regulations also restrict the international transfer of data and we have discussed these briefly below:

a. Under the draft NITDA Guidelines, companies operating in Nigeria and organisations operating outside of Nigeria are prohibited from transferring personal data of Nigerian residents to any country without an adequate level of protection.

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.

Generally, the consequences of failure to comply with the provisions of the data regulations include fines, damages or equitable remedies in the form of injunctions.

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.

A 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 combating financing 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 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; and
- Advance Fee Fraud and Other Related Offences Act 2006.

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

None, other than the regulations stated 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?

The principal law governing the employment of persons in Nigeria is the Labour Act, chapter L1, LFN 2004 (the "Labour Act") but this law applies to junior and non-professional staff.

The terms of 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 a good, or bad, or for no reason at all. 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 provide the employee all accrued contractual entitlements to avoid actions for wrongful termination by employees.

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 employee 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 its employees. Employers contribute 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 (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 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 Employees 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 to 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 of places 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 trademarks. Owners of unregistered trademarks are not protected by the Trade Marks Act but are entitled to seek relief under the English 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 trademarks, 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. Trademarks 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 to 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)?

Trademarks, patents and industrial designs must be registered in accordance with the procedure prescribed in the relevant legislations 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 been so domesticated to date. 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 tradable just like any other property. They may, therefore, be assigned, transferred or licenced 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. Trademarks, 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 right (in relation to copyright), 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 licenced, 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 and Belo-Osagie
St. Nicholas House (10th & 13th floors)
Catholic Mission Street
Lagos
Nigeria

Tel: +234 1 462 2307-10
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 team. 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 depositary receipt programme, derivatives, mergers and acquisitions, equity issuances and the establishment of collective investment schemes.

Yinka is ranked in *Chambers Global* for 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*. She is also the current Chairperson of the Nigerian Capital Markets Solicitors Association and sits on the board of several companies.

Yinka is at the fore front 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 and Belo-Osagie
St. Nicholas House (10th & 13th floors)
Catholic Mission Street
Lagos
Nigeria

Tel: +234 1 462 2307-10
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 the trends in fintech in Nigeria.

Udo Udoma and Belo-Osagie ("UUBO") has been described in international rankings as one of Nigeria's "Magic Triangle" law firms – a description underscored by one of the highest ratios of internationally recognised partners per firm in the Nigerian legal market.

Although a full-service firm, we are especially well regarded in our niche specialisations which include: private equity; energy, electric power and natural resources; banking, finance and capital markets; corporate restructuring (including mergers and acquisitions); project finance; foreign direct investments; telecommunications; taxation; and labour and employment. Together with our litigation, alternative dispute resolution and company secretarial departments, we are able to provide proactive and cost-effective legal services throughout Nigeria and to clients outside Nigeria.

The firm was awarded the title of law firm of the year in 2014 by '*Who's Who Legal*' and has been ranked in Tier 1 by the *Chambers and Partners* for its Banking and Finance and Corporate Commercial Practice. *The Legal 500*, *Who's Who Legal* and *IFLR 1000* currently record that UUBO is "widely accepted as the corporate firm of choice in Nigeria, and the go-to firm for a large percentage of international outfits looking for local counsel in the country".

Norway

Markus Nilssen

Sondre Graasvoll

BA-HR

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 within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Notable fintech business in Norway at the time of writing includes:

- Vipps (DNB Bank ASA) and Mobilepay (Danske bank) both offers mobile application payment services. Vipps, being the largest fintech business in Norway with more than two million users alongside Mobilepay, have been offering swift and simple solutions for carrying out money transactions from one person to another in Norway since 2015. Furthermore, the two services are in tough competition of being the preferred future in-store payment solution in Norway.
- Cloud insurance is a Software-as-a-Service (SaaS) for insurance companies, agents and brokers, and is, according to the company itself, ready in use in 18 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.
- Mysharelive 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 is a mobile application which aims to make it social, easy and fun to save and invest for everyone without regard to the users' income. Spiff strives to be easy to understand and puts the customer directly in charge of his/hers savings using a smartphone.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

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' and the lack of a 'regulatory sandbox' or similar initiatives which would enable fintech startups to test their ideas on the public before becoming licensed.

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 is rapidly growing. This is most likely a result of both the current global interest in innovation, and the dramatic reduction in the price of crude oil since the summer of 2014 which has cost thousands of jobs in the oil industry. The redundancies created by the oil crisis have pushed several well-qualified members of the workforce into new ventures, while investors deterred by losses in the oil sector have 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 35 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.

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?

As of today there are no such special incentive schemes. The relevant Norwegian tax rules for fintech investors can be summarised as follows: Norway currently has a wealth tax rate of 0.85%. The wealth tax only applies for individual taxpayers who are tax resident in Norway. For shares, only 90% of the market value shall be calculated for wealth tax purposes, which would also apply for share investments in venture capital.

Payment of wealth tax for the income years 2016 and 2017 related to share investments may be postponed for up to two years. Payment of wealth tax for the income years 2016 and 2017 related to other investments than shares may be postponed for up to two years, provided such investments were operating with a loss in the year prior to the income year. The postponement of payment of wealth tax is only available for investments directly owned by individual taxpayers, and where the wealth tax on such investments exceeds NOK 30,000 for an income year.

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 24% (25% for financial enterprises), giving an effective tax rate on dividends of 0.72% (0.75%). 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 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 minimum 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 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.

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 is the recent co-investment by more than 100 local Norwegian banks in DNB Bank's mobile payment platform 'Vipps'.

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 startups intending to market its 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. At the time of writing, no precedents or clarifying statements with respect to licensing requirements for fintech businesses have been published by the Norwegian regulator. It should be noted that Norway as a member of the EEA is obligated to respect and facilitate the EU's 'four freedoms' within the scope of the EEA agreement. Whether Norway's wide-reaching licensing regime for financial services is in line with the country's obligations under the EEA agreement has not yet been tested by the courts.

3.2 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?

The Norwegian FSA has not yet expressed a formal opinion on its approach to regulating the fintech sector and its views on innovation and new technology in the financial services markets. The FSA has

historically taken a conservative approach to its regulation activity, and has not often granted exemptions from the licensing requirements. Absent new legislation or regulations from the Ministry of Finance, we would not expect the FSA to grant exemptions from licensing requirements to fintech business. However, it is encouraging to note that the fintech sector, as part of the 'digital revolution', has been put on the political agenda in Norway and received increased attention from politicians and legislators. To that end, a special committee of the Norwegian Parliament issued a report in November 2016 recommending that Norway should implement similar measures as the 'regulatory sandbox' initiative taken by the FCA in the UK. It remains to be seen whether the Parliament will follow-up on this recommendation and implement exemptions from the licensing requirements to facilitate increased fintech innovation.

3.3 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 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 Norwegian Personal Data Act and Regulation regulates the collection, use and transmission of personal data within the Norwegian jurisdiction. The Act and Regulation implements the Data Protection Directive 95/46/EC.

The Personal Data Regulation states that financial institutions must have a personal data licence in order to handle their customer's personal data. Accordingly, fintech businesses conducting licensable activities (*cf.* question 3.1 above) in Norway will need a personal data licence from the Data Protection Authority before the Fintech-company can process personal data on behalf of their customers.

The revised Data Protection Regulation (EU) 2016/679 is expected to be implemented in Norway at the same time as it becomes effective in the EU (25 May 2018).

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 Norwegian Personal Data Act applies to all undertakings and physical persons within the Norwegian jurisdiction. Norwegian personal data law will thus apply to organisations established outside the Norwegian jurisdiction when operating and offering their services to Norwegian customers and companies based within Norwegian jurisdiction.

The Norwegian Personal Data Act allows international transfer of data within the EEA-area and also to the US based on the Privacy Shield framework. Furthermore, international transfer of data may be transferred to countries approved by the European Commission. 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 Data Protection Authority may issue a fine to legal persons who violate provisions set out in the Act. Physical persons may only be fined for violations due to gross negligence or wilful misconduct. Such fines are capped at NOK 925,000 (USD 109,000) at the time of writing.

Furthermore, the Data Protection Authority may order that processing of personal data in violation of the provisions of the Act shall cease, or impose conditions which must be met in order for the processing to be compliant with the Act. The Data Protection Authority may impose a daily fine for each day of non-compliance with the order (subject to applicable grace periods).

Anyone who wilfully or by gross negligence violates the personal data licensing requirement and certain other provisions of the Act may be fined (no cap applicable) or sentenced to prison for up to one year, and in the most severe cases up to three years.

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

There are no cyber security laws or regulations currently in effect in Norway, but 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 3rd AML Directive. A proposal for implementation of the 4th AML Directive has been put forward.

Entities conducting licensable services (*cf.* question 3.1 above) are subject to the Anti-Money Laundering Act and Regulations, and 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 up to one year.

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 hiring of employees in Norway, and the hiring process is, to a large extent, subject to the employer's discretion. There are no particularly onerous requirements or restrictions that are frequently encountered by businesses regarding hiring, however, 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 "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 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 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 out holiday pay in June instead of ordinary salary, regardless of when the employee takes out holiday.

In addition, the employee will be entitled to time off on the public holidays.

Pension:

Norwegian companies have a legal obligation to establish pension plans for their employees. Thus, all employees are entitled to occupational retirement pension, i.e. a pension financed primarily by the employer (with 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 period of maximum 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 EEA and Switzerland wishing to work in a company in Norway, have to apply for a residence permit. Citizens from 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, hereby 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 itself 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 programme 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 the 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 ECJ) 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 Employer 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.

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 the 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 Bern Convention. A state which has ratified the Convention is obligated to provide copyright holders 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' right to private copying, the right to quote from a copyright protected work, and the use of a copyright protected work within education 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 license agreements on behalf of the copyright holder.

Markus Nilssen
BA-HR
Tjuvholmen Allé 16
0252 Oslo
Norway

Tel: *+47 9006 4626*
Email: *marni@bahr.no*
URL: *www.bahr.no*

Markus Nilssen is a senior associate with Advokatfirmaet BA-HR DA. He has worked in BA-HR's finance group since 2008. He holds an LL.M. in business law from UCLA School of Law.

Sondre Graasvoll
BA-HR
Tjuvholmen Allé 16
0252 Oslo
Norway

Tel: *+47 2100 0050*
Email: *sogra@bahr.no*
URL: *www.bahr.no*

Sondre is an associate with Advokatfirmaet BA-HR DA. He has been part of BA-HR's technology department since 2015 and has experience within data privacy law, IP- and IT-law. He holds a Master of Laws from the University of Bergen.

BAHR

As one of the most international law firms in Norway, BA-HR has been successfully advising leading Norwegian and global clients since 1966. Today BA-HR's practice covers all the key commercial disciplines, with a particular focus on domestic and international transactions, commercial law advice and dispute resolutions. The firm is consistently ranked as a "tier one" firm in Norway.

In order to enhance our understanding of business sectors and commercial relationships, and assist in sharing expertise and information, BA-HR's lawyers are arranged into industry groups, as well as practise 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, 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.

Poland

Marcin Smolarek

WKB Wierciński, Kwieciński, Baehr

Agnieszka Wiercińska-Krużewska

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 within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

There are a few dozen fintech businesses operating in Poland. Collectively, they cover all of the main sub-sectors of the market. The largest fintech sub-sector in Poland comprises finance platforms, followed by digital and mobile payments, crowdfunding/P2P lending and big data/analytics/machine learning. Cryptocurrency and personal finance management are also active areas.

The Polish banking sector is among the most technologically advanced in Europe, with highly advanced card, online and mobile payment technology. Mobile banking and e-banking (with almost 7 and 14 million active users respectively) are very popular in Poland.

Even though many Polish fintech businesses directly target the consumer market, there is widespread recognition of the need for cooperation with the banks and the mutual benefits resulting from such collaboration (see: the "FinTech in Poland – barriers and opportunities 2016" report prepared by the FinTech Poland foundation).

Recent examples of major Polish banks investing in the fintech sector include the establishment by mBank S.A. of a special fund (mAcelerator) which is to invest EUR 50 mln in fintech start-ups over the next three years, and the acquisition by PKO BP (the largest Polish bank) of a loyalty programmes start-up, both of which were announced in early 2017.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

Under Polish law, the following activities may only be performed by banks:

- accepting money contributions payable on demand or upon a predetermined date and maintaining accounts for such contributions;
- maintaining other bank accounts;
- granting credit facilities (i.e. facilities for financing a specified purpose);
- granting and confirming bank guarantees and issuing and confirming letters of credit;
- issuing bank securities; and
- conducting bank money clearances.

The performance of payment activities (including, among other things, execution of payment transactions, direct debits, transfer services and transactions through a payment card) are also regulated.

In addition to these general restrictions, the Polish Financial Supervision Authority ("**PFSA**"), by way of a recommendation to the Polish banks, has blocked the use of screen scraping. The recommendation has been in place since August 2014.

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 three most frequently used sources of funding are grants from the European Union, venture capital funds and business angels. Generally, the availability and appropriateness of each type of funding (i.e. grants *versus* equity *versus* debt) will depend on factors such as the type of business and its stage of development and the financial position of the business. At the very early stages of a fintech company's lifecycle, seed money is usually gathered from the founders' personal resources and acquaintances. The most common subsequent sources of third party funding include venture capital, grants from the European Union and funding from private investors i.e. business angels. Crowdfunding is another, although less popular, source of funding for fintech companies in Poland. Emerging fintech businesses often have difficulties in obtaining funds for expansion and development through banking loans due to the lack of a long-term finance scheme with adequate predictability of cash flow as well as the poor quality of many business plans.

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 particular tax incentive schemes in Poland of particular relevance to the fintech sector. However, fintech entities may receive the support of governmental funds. In particular, the Polish Development Fund has launched an information and business support centre for entrepreneurs, investors, local administration and individual clients that are looking for development incentives in Poland.

The Polish Development Fund comprises a group of financial and advisory institutions for entrepreneurs, including innovative

companies at the earliest stages of development. The Polish Development Fund arranges financing of innovative projects from European funds (e.g. the "Smart Growth Operational Programme 2014–2020") and private funds from selected financial institutions.

The PFR Starter FIZ (closed-end investment fund) fund supports innovative companies at their earliest stages of development (i.e. pre-seed, seed and start-up). The total amount of funds available is PLN 782,000,000, with individual investments ranging up to PLN 3,000,000. The PFR Biznest FIZ (closed-end investment fund) also supports innovative companies at the initial stages of development. The total amount of funds available is PLN 258,000,000, with individual investments of up to PLN 4,000,000.

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

Only a joint-stock company may offer its shares in an initial public offering. In brief, the principal conditions for an IPO are as follows:

- **Information document**

The company should produce an appropriate information document which must be approved by the PFSA (subject to certain exceptions).

- **Registration by the National Depositary for Securities**

The company must have the shares which are the subject of the IPO registered with the National Depository for Securities.

- **Minimum capitalisation**

The issuer whose shares are to be traded on the Warsaw Stock Exchange (a fully regulated stock market) must meet certain minimum levels of market capitalisation, i.e. generally, at least the PLN equivalent of EUR 15,000,000.

This requirement does not apply, if the shares are to be traded on New Connect, which is the Polish equivalent of the London AIM.

- **Public spread**

Shareholders of the company, each of which is only able to exercise less than 5% of votes at a meeting of shareholders of the issuer, must hold at least:

- 15% of the shares referred to in the application for admission to trading; and
- 100,000 shares referred to in the application for admission to trading with an aggregate value equal at least to EUR 1,000,000, calculated based on the last sale or issue price.

Again, this requirement only applies if the shares are to be traded on the Warsaw Stock Exchange rather than the New Connect market.

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

On 26 January this year, PKO Bank Polski (the largest bank in Poland) acquired 100% of the shares in ZenCard Sp z o.o. ZenCard was established in November 2013. The company is a fully digital company that has developed a technologically advanced platform for sellers to create discount and loyalty programmes, which also enables virtualisation of loyalty cards. The shares in Zencard were purchased from the venture capital funds, Experior Venture Fund and SpeedUp Group, and from LMS Sp. z o.o. and ZenCard's founders.

In July 2016, the Polish media reported the potential acquisition of shares in another start-up company, Billion Polska (a provider of digital cash) by Bank Mizrahi-Tefahot (Israel). However, the transaction has not been finally completed.

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 currently one of the fastest growing technology sectors in Poland. The variety of fintech businesses means that each is subject to slightly different regulations. However, the most relevant laws with respect to fintech in Poland include:

- the Payment Services Act (implementing payment services directive 2007/64/EC of the European Parliament) covering solutions in the area of payment services such as acquiring, issuance of electronic money, money remittance, and services enabling cash to be placed on or withdrawn from a payment account, as well as all the operations required for operating a payment account;
- the Consumer Credit Act which applies when loans or credit are granted to consumers, as well as to intermediation in respect of such activity;
- the Consumer Rights Act which imposes certain obligations on business entities if services are provided at a distance;
- the Act on Combating Money Laundering and Financing of Terrorism which applies to various types of financial institutions, but may sometimes also apply to fintech businesses; and
- the Act on Protection of Personal Data which regulates the collection, use, transmission and other forms of processing of personal data.

This list is far from exhaustive, and other regulations concerning, for example, investment funds, insurance and data protection may form part of the legal environment for a fintech business in Poland.

3.2 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?

The positions taken by regulators, such as the PFSA, with respect to fintech are mainly driven by the growing scale of threats to cybersecurity.

PFSA does not include among its strategic goals support for creation and promotion of innovative solutions. Rather, it mainly focuses on ensuring the stability, security and transparency of the market and providing protection for the interests of market participants.

Having said that, thanks to growing interest in the fintech sector, in 2016 the PFSA appointed a Working Party for the Development of Financial Innovation in Poland. The Working Party includes, among others, representatives of the following institutions: the Ministry of Finance; the Ministry of Economic Development; the National Bank of Poland; the PFSA; and the Office of Competition and Consumer Protection. The objective of the Working Party is to prepare a report (by the end of 2017) on the legal and regulatory framework in order to identify regulatory and administrative barriers for the further development of businesses implementing innovative solutions in the field of financial services.

3.3 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 cross-border offer of financial products or services in Poland raises questions as to the extent to which the laws from other jurisdictions will apply. This is critical since the success of financial products or services often depends on the ability to scale the operations appropriately.

Under Polish law, parties to a contract are generally free to choose the governing law. However, this right is subject to certain limitations when the agreement is concluded with a consumer. The choice of law cannot lead to a consumer being deprived of protections afforded to them by Polish law.

Additionally, a fintech business has to overcome barriers such as the excessive length and complexity of procedures for obtaining an authorisation from the PFSA to provide payment services (usually this takes about nine months). However, in certain situations, an entity that is refused or does not yet have a licence issued by the PFSA, but obtains a licence to carry on the relevant activity in another European Union Member State, is free to provide these services in Poland on the basis of a European passport.

A further barrier is the imprecise or excessively strict implementation in Poland of European Union legislation. In particular, Polish law often goes further than the European Union law. Even where the Polish law accurately reflects the European law, the interpretation of the relevant Polish regulatory authority may be more severe than elsewhere. For example, the PFSA takes the view that pre-paid cards issued by banks in Poland should not be treated according to the legal regime for electronic money (as such, they are not issued in a closed loop system, among other things). This approach differs to that taken by other European Union Member States which have implemented the EMD2 directive (2009/110/EC).

Also, in Poland, there is also a high cost of the PFSA supervision and there are no exemptions which may reduce such costs for start-up enterprises.

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 general, the collection, use, transmission and other forms of processing of personal data are regulated by the Act on Protection of Personal Data (which implements the Data Protection Directive (95/46/EC)) ("**PDP**").

Data controllers (i.e. entities deciding about the means and purposes of processing) must meet requirements laid down by the PDP, such as processing personal data on valid legal basis or fulfilling notification obligations towards data subjects (i.e. users of fintech services). Data controllers are also obliged to register data bases with the Polish Data Protection Authority ("**DPA**") or appoint and register a Data Protection Officer ("**DPO**"), in which case, only data basis containing sensitive data must be registered with the DPA. Also, additional requirements must be met in respect of transfers of data to third countries i.e. outside the European Economic Area.

The PDP also sets out detailed requirements for ensuring the security of personal data (such as a minimum length of passwords and the required frequency of changes).

Polish data protection law will be changed once the General Data Protection Regulation becomes effective on 25 May 2018. As a result, in principle, the same data protection rules will apply in all EU countries.

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 PDP applies to entities having their registered seat in Poland or which process personal data using technical means located in Poland (with the exception of the mere transit of personal data).

Transfers of personal data to third countries (outside the European Economic Area) may take place only if the country of destination ensures an adequate level of personal data protection in its territory (unless the transfer of personal data results from an obligation imposed on the data controller by law or the provisions of a ratified international agreement which guarantees an adequate level of data protection).

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

There are two types of sanctions provided under the PDP: administrative; and criminal.

Administrative sanctions: In the event of a breach of PDP, the DPA may request that the appropriate state of affairs be implemented or restored (through, for example, removal of the violation, application of additional safeguards to protect personal data, cessation of transfers of personal data to a third country or erasure of personal data).

Criminal sanctions: A person who is responsible for processing personal data and violated the PDP (e.g. by way of disclosure of personal data or providing access to data to unauthorised persons, failing to notify data bases for registration with the DPA or failing to inform a data subject of their rights) may be subject to a fine, a restriction of freedom or a prison sentence of up to two years. However, criminal sanctions are rarely imposed in practice.

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

Polish law does not regulate matters related to cyber security in any single law. However, provisions that may relate to activity in the field of cybersecurity are contained in acts such as the following:

- The **Criminal Code**, which does not define cybercrime includes, among other things, offences such as illegal access to data or a computer system, destruction of data, damage to databases, computer sabotage, scam and disruption of network operations.
- The **Telecommunications Law** obliges providers of telecommunication services to take technical and organisational measures to ensure the security and integrity of their networks, services and transmission of messages, and to inform users about the occurrence of the risk of a security breach, and to have a current action plan (developed in consultation with the relevant state authorities) in respect of particular threats.
- The **Act on Electronically Supplied Services** obliges service providers to, for example, ensure the services are supplied in a way that prevents unauthorised persons from accessing the communication contained in the service.

- The **PDP** and other regulations apply to data protection (*please see above*).
- The **Strategy for Cybersecurity of the Republic of Poland 2016-2020** contemplates that a new approach to cybersecurity is required and should consist of, among other things, "*protection in cyberspace of the essential functions of the State i.e. ensuring energy supply, banking, transport, health, etc.*".
- The draft **Act on the National System of Cybersecurity** which is scheduled to be presented to the Sejm (i.e. the Lower House of Polish Parliament) in April 2017 and is supposed to fulfil requirements imposed by the **NIS Directive**, regarding the security of network and information systems.

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

Poland has developed a system of combating money laundering and terrorist financing consisting of supervisory entities, units co-operating with supervisory entities, obliged institutions and law enforcement authorities supporting the General Inspector in fulfilling its statutory duties. According to the Act on Combating Money Laundering and Financing of Terrorism, obligated institutions and units co-operating with supervisory entities shall inform the Polish Financial Intelligence Unit about suspicious transactions or suspicious activity. The obligated institutions include, among others, banks, entrepreneurs receiving payments for commodities in cash of a value equal to or exceeding the equivalent of EUR 15,000, and entities professionally providing currency exchange services.

The Polish Financial Intelligence Unit and other authorities supervising obligated institutions conduct checks as to whether individual obligated institutions are adequately prepared to combat money laundering.

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

The key regulatory regimes are discussed 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?

In general, Polish law does not regulate the process for employee recruitment in the private sector (although recruitment in some sectors of economy is subject to special requirements). However, the Labour Code, which generally regulates employment relationships, does limit the scope of personal data that can be collected from candidates. Additionally, the Labour Code requires the employer to respect the principle of equal treatment (i.e. a hiring decision cannot be based on discriminatory criteria such as age, gender or sexual orientation).

The termination of an employment relationship is strictly regulated by the Labour Code. In particular, an employment contract can be terminated: (i) by mutual agreement of the parties; (ii) with notice; or (iii) without notice (disciplinary termination). The termination of an employment contract by the employer, either with or without notice, should be in writing and should include information on the employee's right to file an appeal against the termination with the labour court within 21 days of the notice of termination being served. Otherwise, the employee can challenge the termination. Importantly, in the case of termination of an employment contract concluded for an indefinite period of time, the employer is obliged to state the basis for the termination.

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

Polish law requires the employer to grant certain basic benefits to employees. For example, the employer is obliged to pay remuneration for up to 33 days of sick leave. Additionally, employees should be reimbursed for travel expenses connected with business trips or protective clothes, and a lump sum to cover cleaning costs of such clothes.

In practice, in the private sector, employers also grant employees other benefits, such as health insurance, life insurance, pension packages and sports club cards. Key employees are often provided with company cars and mobile phones, but typically they may only be used for work purposes.

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 recent years, Poland has opened up its labour market to foreigners. As a rule, foreigners require a work permit to perform work in Poland. There are some exceptions to this rule (e.g. citizens of EU Member States). Also, in the case of highly qualified employees, there is a separate procedure for issuing work permits.

A work permit is issued by the Voivode which is competent for the place of residence of the employer who applies for a work permit for a foreign employee. The permit is valid for the period indicated in the permit, which will be no longer than three years, but it may be extended. Additionally, an employer intending to employ a foreigner should be informed about the results of the labour market test by the district governor which is competent for the registered office or place of residence of that employer. The labour market test must be carried out to check whether there are any unemployed individuals registered with the labour office who could meet the expectations of the employer, and who could be hired instead of the foreigner).

6 Technology

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

Rights with respect to "works" within the meaning of the Act on Copyright and Related Rights ("**Copyright Act**") (i.e. an author's economic rights and author's moral rights) belong from the moment of their creation to the individual natural persons (i.e. an authors or co-authors) who created them. Only an author's economic rights can be transferred. For an effective transfer, the agreement has to be in written form. An author's economic rights are limited in time and generally expire 70 years after the author's death. However, rights to works created by employees are, generally speaking, acquired by force of law upon acceptance of the work by the employer.

With respect to inventions, utility models and industrial designs, the entitlement to obtain a patent, protection or a right in registration initially resides with the creator. These entitlements (and any related priority) can be transferred. Again, for an effective transfer, the

agreement has to be in written form. However, where an invention, a utility model or an industrial design is created by a person in the course of his employment duties or in the performance of any other contract, the rights are vested in the employer or the ordering party unless otherwise agreed by the parties.

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

Regardless of the field of technology, inventions are protected by patents granted by the Polish Patent Office ("**UPRP**") under the provisions of the Industrial Property Law ("**IPL**"), provided that they are new, have an inventive step and are susceptible to industrial application. The term of a patent is 20 years from the date the patent application was filed with the UPRP. From an IT perspective, computer programs are not considered inventions and, as such, cannot be protected by patent.

Innovations that are considered to be utility models or industrial designs are protected under the provisions of the IPL by protective rights and rights in registration respectively. The term of protection for a utility model is 10 years, while a right in registration in respect of a design is granted for up to 25 years and is divided into five-year-long terms.

In cases where innovations or inventions are not or cannot be protected by the means available under the IPL, some degree of protection may be implemented through confidentiality obligations. In Poland, confidentiality agreements with employees and other entities cooperating with a business are quite common. Such agreements often include penalty clauses for disclosure of business secrets. Business secrets are also protected under the provisions of the Act on Combating Unfair 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)?

- **Works**: The provisions of the Copyright Act apply to works: (i) whose author or co-author is a Polish national; (ii) whose author is a national of a Member State of the EU or a Member State of the EFTA – party to the Agreement on the European Economic Area; (iii) which were first published in Poland, or simultaneously in Poland and abroad; (iv) which were first published in Polish; or (v) which are protected under international agreements within the scope set out in those agreements (e.g. the Berne Convention for the Protection of Literary and Artistic Works or TRIPS).
- **Polish registered industrial property**: Due to the territorial character of industrial property protection, the provisions of the IPL shall generally apply with respect to industrial property registered within the territory of Poland.
- **EU registered industrial property**: The protection of industrial property registered within the territory of the whole EU (EU trademarks and registered Community designs) is granted on the basis of EU regulations. There is a special court in Poland, called the Regional Court in Warsaw – Court for the Community Trademarks and Community Designs, which is dedicated exclusively to examining cases related to EU trademarks and Community designs.
- Poland is a party to, among other things, the Paris Convention for the Protection of Industrial Property, the Patent Cooperation Treaty, TRIPS, the Madrid Agreement and the Madrid Protocol.
- Poland has not yet decided to join the European single patent system.
- Poland is also obliged to comply with laws of the EU concerning intellectual property.

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 may be exploited/monetised in various ways including:

- **sale**: patents, protective rights, rights in registration, as well as author's economic rights (including rights to software), rights to domain names or *sui generis* database rights can be transferred. With respect to industrial property, it is also possible to transfer a right to obtain a patent, protective right or a right in registration, as well as the related priority;
- **licence**: intellectual property such as inventions, utility models, industrial designs and trademarks, as well as author's economic rights can be the subject of a licence (exclusive or non-exclusive) and a sub-licence;
- **contribution in-kind**: intellectual property can be the subject of a non-pecuniary contribution in-kind to a company in exchange for the issue of shares;
- **pledge**: a pledge may be granted over intellectual property rights;
- **franchising**; or
- **litigation**.

However, restrictions on exploitation/monetisation may be imposed in certain respects including:

- **permitted use**: the rightholder in respect of authors' economic rights cannot prohibit third party use of his work if such use constitutes permitted use (for example, use of a single copy of a work by a group of individuals who are related, especially by blood or marriage, or who are in a social relationship, although with respect to software provisions regarding such use do not apply);
- **authors' personal rights**: authors' personal rights, including, in particular, rights: (i) to claim authorship; (ii) to be identified on the work by name or pseudonym or to make the work available anonymously; (iii) to the integrity of the form and content and fair use of the work; (iv) to decide whether and how the work is made available to the public for the first time; and (v) to supervise how the work is used, are not transferable (although with respect to software provisions regarding authors' moral rights referred to in points (iii)–(v) do not apply);
- **limitation to acquire all works**: Polish law does not permit the acquisition of rights to all works or all works of the same kind as may be created by the same author in the future;
- **abuse of patent**: the IPL prohibits a patent or licence holder abusing its rights including, in particular, by preventing a third party from using the invention if use is required to meet the needs of the domestic market, and especially if required by public interest, and the product is publicly available in insufficient quantity or quality or only at extremely high prices;
- **rights of an entrepreneur**: where an invention, a utility model or an industrial design is made by the creator with the assistance of an entrepreneur, that entrepreneur may use the invention, utility model or industrial design for its own account; and
- **rules on the territorial character of industrial property rights protection**: the protection only applies within the territory where protection was granted.

Acknowledgment

The authors would like to acknowledge Izabela Szczygielska, Agata Szczepańczyk-Piwek, Paulina Komorowska, Monika Obiegło and Matylda Budzyn for their assistance during the preparation of this chapter.

Marcin Smolarek
WKB Wierciński, Kwieciński, Baehr
Polna 11
00-633 Warsaw
Poland

Tel: +48 22 201 00 00
Email: marcin.smolarek@wkb.pl
URL: www.wkb.pl

Marcin is the head of WKB's banking and finance practice. He specialises in project finance, lending (LBO or REF), debt restructuring, distressed debt and financial litigation. He also advises on securitisation and secondary markets (NPLs), as well as investment funding and construction investment. He has hands-on experience in debt restructuring, gained while advising on large projects that involved restructuring Polish bonds issuers, listed companies, and energy sector and real estate loans. Marcin's experience also covers NewTech (FinTech and AdTech) projects, mainly in the payment services sector, and regulatory advice for banks and other financial institutions on various matters. He also represents clients, including banks, on cybercrime cases.

Agnieszka Wiercińska-Krużewska
WKB Wierciński, Kwieciński, Baehr
Polna 11
00-633 Warsaw
Poland

Tel: +48 22 201 00 00
Email: agnieszka.wiercinska@wkb.pl
URL: www.wkb.pl

Agnieszka is the head of WKB's intellectual property & TMT practice. She specialises in, among other things, new technologies, IT contracts, cybersecurity and data protection, as well as all aspects of IP protection and enforcement. Agnieszka also has significant expertise in transactional work and often assists leading IP owners, tech companies and investors (notably in the online services, FMCG, retail, clothing and healthcare industries) on M&A and other types of investment.

WKB
WIERCIŃSKI KWIECIŃSKI BAEHR

WKB Wierciński, Kwieciński, Baehr is a leading Polish independent law firm with a strong team of solution-oriented lawyers advising on the most complex transactions and cases, including cross-border deals. In a rapidly changing world, we help domestic and international clients from the banking and finance sector face challenges posed by new regulatory frameworks and legal complexities resulting from technological developments.

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 within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

According to Statista.com, the transaction value processed in the Portuguese FinTech market is expected to amount to US$ 5,580 million in 2017 and to show an annual growth rate of 17.2% resulting in the total amount of US$ 10,538 million in 2021.

In 2017, the largest segment of the Portuguese FinTech market is expected to be payment, with both domestic and international players operating in the market and in different stages of the payment services value chain. Nonetheless, there are also relevant players in other FinTech segments in Portugal, such as peer-to-peer lending, personal finance management, mobile-first banks, financial, investment advisory and management, financial transactions safety, etc. As for crowdfunding, equity-based and lending-based crowdfunding activities are facing a deadlock: there is a specific legal framework in Portugal applicable to them, but it has not yet entered into force.

Lastly, although the Portuguese FinTech scene is still taking the first steps, with most of the start-ups (75.2%) in the seed or start-up stages and only *circa* US$ 18.5 million in venture capital investments in 2016, the Portuguese Government and the private sector have been very committed to support the emerging start-up ecosystem in Portugal.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

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.

Lastly, the specific legal framework enacted in Portugal in respect of equity-based and lending-based crowdfunding has not yet entered into force, thus the players from this segment have been reluctant to operate 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 last year has seen several initiatives launched by the Portuguese Government with the aim of offering alternatives to traditional sources of funding to start-ups in general, including FinTech businesses. Those initiatives range from (i) funding of daily-expenses of entrepreneurs, (ii) to funding of the acquisition of professional incubation services, (iii) to 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.

Lastly, equity-based and lending-based crowdfunding is not yet an alternative source for funding as the specific legal framework enacted in Portugal in this regard has not yet entered into force, which has prevented players in this sector from starting to operate in Portugal.

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 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 €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 €5 million, which are reinvested in eligible investments in the two tax years following the option to retain. The CIT credits are capped to 25% of the CIT due by the relevant company.

Companies that develop 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 in 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.

A specific tax regime to support investment 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 €10 million, and up to an amount of 10% of the investment amounts exceeding €10 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 with 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 shareholders loans into share capital.

Finally, at the level of the investors, the Portuguese State Budget Law for 2017 introduced a programme called *Semente* (Seed) in order to encourage individuals investing in start-ups. According to this new regime, and provided that certain conditions are met, an individual may be granted with a personal income tax credit ranging between €2,500 and €25,000, depending in 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 heaven, 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 €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 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 (such as 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; 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?

No. Nevertheless, there are some notable investments from major traditional players. Those are the cases, for instance, of the undisclosed multi-million euros investment of Citigroup in Feedzai (which is a FinTech start-up that uses software to detect financial anomalies and fraud in banking and e-commerce in European and US companies); of the joint-venture between Banco CTT and an undisclosed Portuguese FinTech business to provide financial services through an app; and of the FinTech accelerator launched last year by SIBS (*SIBS Pay Forward*), one of the most important traditional players in the Portuguese payment services market.

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, the 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, 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 start 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. Nonetheless, the legal framework applicable to equity-based and lending-based crowdfunding activities has not yet entered into force. Moreover, 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, any FinTech business carrying out a regulated activity will need to first obtain the necessary authorisation and/or registration with the competent regulatory authority(ies).

3.2 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?

Yes. The Portuguese Government has been very committed to supporting the emerging start-up ecosystem in Portugal in general, including FinTech, and the three-year deal with Web Summit is just part of the momentum. In fact, 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 support for internationalisation of start-ups.

3.3 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, the type of services it provides and its jurisdiction, we may have one of three scenarios:

- FinTech business established in a 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, consumers' and employees' protection, etc.
- 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 general terms of law, including, but not limited to, legislation governing marketing materials, data protection, consumers' and employees' protection, etc.
- 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, 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, article 35 of the Portuguese Constitution and Law no. 67/98 of 26 October that transposed Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data (the "Data Protection Law") into the Portuguese legal system. These rules apply to the processing of personal data wholly or partly by automatic means, and to the processing other than by automatic means of personal data which form part of manual filing systems or which are intended to form part of manual filing systems. These rules do not apply to natural persons processing personal data in the course of a purely personal or household activity. As applicable from 25 May 2018, the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), which repeals Directive no. 95/46EC, will also apply in Portugal.

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 recently amended by Law no. 46/2012 of 29 August, which transposed Directive no. 2009/136/EC, also contain relevant rules regarding the sending of unrequested communications for direct marketing purposes.

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 Protection Law also applies even when personal data is processed outside of Portugal: (i) in the context of activities of an establishment of the controller in the Portuguese territory; (ii) if, in the place where the processing is carried out, national laws apply by virtue of international public law; or (iii) when the controller is not established within the EU but makes use of equipment, automated or otherwise, situated in Portugal, unless such equipment is used only for purposes of transit through the EU.

As concerns transfers of data, the Data Protection Law states that whenever these transfers occur within the EU they are free of additional requirements. Transfers of personal data to any third countries may only take place provided that said third country ensures an adequate level of protection. Notwithstanding this general rule, the Portuguese Data Protection Authority ("**CNPD**")

may authorise a transfer or a set of transfers of personal data to a receiving state that does not provide an adequate level of protection if the data subject has given clear consent to the proposed transfer, or if the transfer is: (i) necessary for the performance of a contract between the data subject and the controller, or the implementation of pre-contractual measures taken in response to the data subject's request; (ii) necessary for the performance or conclusion of a contract between the controller and a third party that is concluded, or to be concluded, in the data subject's interests; (iii) necessary or legally required on important public interest grounds, or to establish, exercise or defend legal claims; (iv) necessary to protect the data subject's vital interests; or (v) made from a register which is intended to provide information to the public and is open to consultation, either by the public or by any other person who can demonstrate a legitimate interest, provided the conditions laid down in law for consultation are fulfilled. In addition, the CNPD may also authorise a transfer or set of transfers of personal data to a State which does not ensure an adequate level of protection, provided the data controller adduces adequate safeguards particularly by means of appropriate contractual clauses (for example, the Model Standard Contractual Clauses approved by the European Commission).

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

Non-compliance with the Data Protection Law is generally deemed an administrative offence and the penalty for each breach ranges between €1,500 and €15,000 (€3,000 and €30,000 when dealing with sensitive data). The data controller can also incur civil or criminal liability (with penalties ranging from one year of imprisonment or fines of up to 120 days (the daily rate for fines corresponds to an amount ranging between €5 and €500), plus ancillary sanctions.

Also, the violation of rules applicable to marketing communications and cookies set forth in Law 41/2004 of 18 August, as amended, constitute an administrative offence, punishable with fines ranging from €5,000 to €5,000,000 for legal entities.

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 Convention on Cybercrime and the Council Framework Decision no. 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 of companies providing publicly available electronic communication services to promptly notify the CNPD 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 data breach notification shall be extended to all companies with the implementation of the General Data Protection Regulation and shall be carried out under the conditions set out therein.

The provision of the Data Protection Law regarding the obligation of the data controllers to implement security measures 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.

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

Law no. 25/2008, of 5 July, provides for the legal framework on the prevention of money laundering and the financing of terrorism, as has been complemented for a set of regulations and instructions issued by the national supervisory authorities ("**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, although it has not yet entered into force, the Portuguese legal framework applicable to equity-based and lending-based crowdfunding platforms sets forth that these platforms must adopt written policies and procedures adequate and effective to prevent fraud, money laundering and financing of terrorism and that they must make such policies available in the platform's website.

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. 317/2009); (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 (Law no. 67/98, of 26 October, and 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 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 requires, 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 year 2017 is of €557. 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 2017 is of €568.14 and €584.85, respectively).

Furthermore, collective bargaining agreements usually set forth the minimum remuneration scale that has to be paid to the 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 his 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 Industrial Property Code (*Código da Propriedade Industrial*, the "CPI"), as approved by Decree-Law 36/2003, of 5 March, as amended. The CPI includes the main legal provisions regarding invention patents, utility models (with a lower inventive rank than patents), registered designs and trademarks.

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 patent, unless the software in question is part of a process subject to patent protection *per se* (the 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 not specifically regulated in the CPI. However, whenever there is a disclosure, acquisition or use of the business secrets of a competitor without its consent, provided that said information: (a) is secret in the sense that it is not common knowledge or easily accessible, in its totality or in the exact configuration and connection of its constitutive elements, for persons in the circles that normally deal with the type of information in question; (b) has commercial value based on the fact that it is secret; and (c) has been the object of considerable diligences on the part of the person with legal control over it, with a view to keeping it secret, this may constitute an act of unfair competition under the CPI.

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 registration date and may be indefinitely renewed for identical periods of time.

The Portuguese Code of Copyright and Related Rights (*Código do Direito de Autor e Direitos Conexos* "**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. It exists from the moment the work is created. As a general rule, the 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 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 relevant of the invention importance of the invention and may 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 (and only from uses resulting from its copy); and (c) know-how and business information (trade secrets) may be protected if the requirements set forth in the CPI on unfair competition are satisfied.

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 to 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 Industrial Property Institute (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.

Acknowledgment

The authors would like to acknowledge the assistance of their colleague Joana Mota (*Senior Associate*) in the preparation of this chapter. Joana Mota joined Uría Menéndez as a junior associate in February 2012 and became a senior associate in February 2014. 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 advises 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.

Pedro Ferreira Malaquias
Uría Menéndez – Proença de Carvalho
Rua Duque de Palmela, no. 23
1250-097 Lisbon
Portugal

Tel: +351 21 030 8661
Email: ferreira.malaquias@uria.com
URL: www.uria.com

Pedro Ferreira (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
Rua Duque de Palmela, no. 23
1250-097 Lisbon
Portugal

Tel: +351 21 030 8649
Email: helder.frias@uria.com
URL: www.uria.com

Hélder Frias joined the Lisbon office of Uría Menéndez – Proença de Carvalho in 2006. In 2009, he was seconded to the in-house legal department of a British bank in Lisbon for six months and from September 2010 to August 2011 he was based in our London office.

His practice is focused on banking, finance and insurance. Notably, he advises on M&A transactions involving financial institutions, bancassurance joint ventures, the transfer of insurance portfolios and on other regulatory matters related to these markets, including insurance and reinsurance intermediation.

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

Uría Menéndez is the leading law firm in the Ibero-American market. With 555 lawyers, including 128 partners, the firm advises on Spanish, Portuguese and EU law in relation to all aspects of corporate, public, litigation, tax and labour law. We have 17 offices in 13 countries and over 2,000 clients.

In January 2015, after nearly 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.

Uría Menéndez celebrates its 70th anniversary this year. Our decades of experience have made the firm a frontrunner in client service, intellectual leadership and talent recruitment in Spain, Portugal and Latin America. It maintains the academic tradition of its two founders, with more than 50 university professors among its ranks, as well as a commitment to society that the founders – who were both "Prince of Asturias" award winners (the highest recognition awarded in Spain to extraordinary men from all backgrounds) – maintained throughout their lives.

South Africa

Prof. Angela Itzikowitz

ENSafrica

Era Gunning

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 within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

In recent months, there has been a growing number of fintech startups whose product offerings or services have had (or will have) a 'disruptive impact' on traditional banking and financial services providers. Fintech businesses include online peer-to-peer lending, mobile money transfers, crowdfunding, 'robo' advisers, and the like.

To illustrate: Jumo, facilitates financial access through mobile wallets, with no need for a bank account, physical structure or collateral, and is linked to large mobile networks, including MTN.

RainFin is an online lending marketplace that connects borrowers seeking transparent, cost effective loans with lenders wanting significant returns. RainFin's lending marketplace matches providers of funds to borrowers in an automated fashion with reduced overheads and more efficient execution.

LulaLend grants short-term business loans of R20,000 (twenty thousand rand) to R250,000 (two hundred and fifty thousand rand) to small business, with less stringent requirements than banks.

Private institutions in South Africa, such as Bankymoon, have made significant overtures to explore, test and deploy bitcoin and blockchain technology.

WiGroup is a mobile transactions solutions company, which provides a point of sale integrated, open and interoperable mobile transactions platform.

Snapscan provides a cashless and cardless payment app that consumers can use at participating merchants across South Africa.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

The very broad definition of the 'business of a bank' in the Banks Act, 1990, which has at its heart the taking of deposits from the public, is an issue for any person (natural or juristic) taking money from the public (which includes corporates) with an undertaking that the moneys will be repaid on demand or otherwise, conditionally or unconditionally, and with or without interest.

Similarly, peer-to-peer or market-place lenders are constrained 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 generated. 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 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 by the South African Reserve Bank. Bitcoin exchanges may, however, have to be licensed as money remitters and there may be Banks Act issues where these virtual currencies are exchanged for real money. Furthermore, BlockChain, where it is used to facilitate the buying and selling of securities, could be regarded as an exchange under the Financial Markets Act, 2012.

A person giving advice, or rendering intermediary services, in respect of financial products, would need to be registered as a financial services provider under the Financial Advisory and Intermediary Services Act, 2002, and this is true also of the entity or person behind the 'robo' adviser.

Crowdfunding is not currently regulated under South African law. Crowdfunders may find themselves falling foul of the Banks Act, 1990 where the funding is by way of debt, or having to register as an exchange under the Financial Markets Act, 2012 where the funding is by way of equity.

Fintech also poses novel and increased risks to anti-money laundering regimes in South Africa and around the world.

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 are on the rise. A comprehensive list of venture capital and private equity firms is available on the website of South African Venture Capital and Private Equity Association.

Also see 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 of R1,000,000 (one million rand) investment to a 51% (fifty one per cent) black-owned entity with 50% (fifty per cent) 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 R150,000,000 (one hundred and fifty 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 R1.5bn (one and a half billion rand) 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.

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 R50,000 000 (fifty million rand); not less than 25,000,000 (twenty five million) equity shares in issue and 20% (twenty per cent) of each class of equity securities must be held by the public to ensure reasonable liquidity; a satisfactory audited profit history for the preceding 3 (three) financial years, where the last report must show an audited profit of at least R15,000,000 (fifteen million rand) 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?

Notable exits include:

- Gyft, a mobile gift card app that allows customers to buy, store, send, and redeem gift cards from their mobile device, exited to Silicon Valley.
- Visa acquired South African mobile financial services company Fundamo for $110 million in cash.
- M-Pesa, a mobile phone-based money transfer service operated by mobile network operator, Vodacom, no longer operates in South Africa partly because of the stringent regulatory regime and partly because it struggled to grow its consumer base.
- Tyme, which launched mobile money for cellular network MTN and retailer Pick n Pay, was acquired by Commonwealth Bank of 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.

See question 1.2 above and section 4 below.

Money laundering in South Africa is regulated by the Financial Intelligence Centre Act, 2001 ("FICA") and the Prevention of Organised Crime Act, 1998 and the regulations promulgated thereunder. The latter sets out the money laundering offences, while the former (for the most) provides the administrative framework for regulating anti-money laundering. 'Accountable institutions', as defined in the FICA, include banks, insurers, money remitters, investment advisers and the like, are subject to onerous compliance obligations, including identifying and verifying customers and record-keeping as well as registering with the 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 the FICA. In respect of certain low-value transactions, the Minister of Finance has exempted accountable institutions in terms of 'Exemption17' to FICA, from having to obtain and verify the residential address of its client.

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. If a non-bank, commercial company were to offer any payment service or product to its customers (such as a debit or credit card), it would not be able to do so directly but would have to be 'sponsored' by a bank participating in the relevant PCH. The Payment Association of South Africa has been appointed by the South African Reserve Bank ("SARB") to oversee and regulate the participation of its members in the national payment system.

3.2 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?

Financial markets are very 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 in other jurisdictions, such as Singapore and the United Kingdom, neither the SARB nor the Financial Services Board have to date created regulatory sandboxes for these companies. The very tight regulation of M-pesa (a money transfer service which allows people to send money using their cell phones) in South Africa was certainly one of the causes of its failure. From an anti-money laundering perspective, the SARB and the Financial Intelligence Centre is resistant to non-face-to-face fintech KYC methods.

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 Financial Services Board.

3.3 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 fintech business is required to register as an external company in terms of the Companies Act, 2008, within 20 (twenty) 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, as a general rule, persons wishing to remit money cross-border would have to apply for permission.

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?

South Africa's data protection law, 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 making of Regulations under POPI, however, came into force on 11 April 2014.

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 if it were reasonably practicable, the data subject would have given his or her consent.

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 (ten) years, or to both such a 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 R10,000,000 (ten million rand).

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 and Cybersecurity Bill was published on 28 August 2015 as part of a set of laws and policy initiatives in South Africa that aim to regulate the ever-expanding online economy, and the surge in cyber-related crimes from a South African (and global) perspective.

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 and FICA. 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, in the main, 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 (which, as a general rule, would include any banking services, or related or similar financial services); (b) all transactions for the 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 which provide products or services to natural persons or juristic persons with an annual turnover or asset value not exceeding R2,000,000 (two million rand) at the time of the transaction.

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 3 (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 (twenty one) days in an annual leave cycle);
- paid sick leave (6 (six) weeks during a 36 (thirty six) month cycle);
- maternity leave (4 (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 (forty five) hours in any week. 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 in so far 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 trade marks 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 ENSafrica's Rachel Sikwane, director, and Jan Norval, associate, for their assistance during the preparation of this chapter.

Prof. Angela Itzikowitz
ENSafrica
150 West Street
Sandton
South Africa

Tel: +27 112 697 702
Email: aitzikowitz@ensafrica.com
URL: www.ensafrica.com

Professor Angela Itzikowitz is an executive in ENSafrica's banking and finance department. She specialises in banking and financial market regulation.

Angela has done a significant amount of work in SADC countries, has participated in a number of financial market initiatives in Asia and acts for a number of European clients.

Angela is a professor in Banking and Financial Markets Law at the University of the Witwatersrand and teaches at Queen Mary College, the University of London on Legal Aspects of International Finance.

She is a member of the Board of International Scholars, London Institute of Banking and Finance and is a Professorial Fellow at the Asian Institute of International Financial Law, University of Hong Kong.

Recent recognition given to Angela includes:

- Best Lawyers® 2016, 2013 – Banking and Finance (South Africa).
- Chambers and Partners Global Guide to the World's Leading Lawyers 2015, 2014, 2013 – Banking and Finance (South Africa).

Era Gunning
ENSafrica
150 West Street
Sandton
South Africa

Tel: +27 113 023 157
Email: egunning@ensafrica.com
URL: www.ensafrica.com

Era Gunning is a senior associate in ENSafrica's banking and finance department.

She is an admitted solicitor of the Supreme Court of New South Wales, Australia and has advised various clients, including leading banks, on the practical application of international anti-money laundering initiatives and statutory compliance issues.

Era's experience also includes the drafting and perusal of all legal documents such as commercial leases, as well as advising on consumer and data protection. She has been quoted in various media publications as a data and consumer protection expert.

Era has conducted numerous workshops and seminars in respect of data and consumer protection for clients, including banks, insurers, credit providers, pharmaceutical companies, medical schemes, government agencies, parastatals and direct marketers.

Era is an *ad hoc* lecturer at the University of the Witwatersrand for postgraduate students, and has also authored the data protection chapter in Juta's Company Secretarial Practice.

ENSafrica's banking and finance department of over 40 practitioners differentiates itself by high levels of specialisation across the full spectrum of finance and debt capital markets work, including financial services regulation, leveraged finance, asset finance, debt finance and trade finance.

The key to the Banking and Finance Department's success is its large number of senior practitioners who are each dedicated to, and have deep expertise in, specific areas of banking and finance. In addition, the team has competence in English law, with qualified English law practitioners at executive level, as well as practitioners who are qualified to practise French law. ENSafrica's Banking and Finance Department works closely with the firm's other market-leading departments and business areas, including tax, corporate commercial, insolvency and debt recovery, and employment.

Spain

Leticia López-Lapuente

Uría Menéndez

Livia Solans

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 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. In 2013, it was estimated that there were 50 Fintech companies; this number has increased to 238 as of February 2017 (source: Spanishfintech.net).

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 (AI) tools represent the most recent trends in innovation (to date, mainly crowdfunding and crowdlending 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. The 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 is also expected to bring considerable growth of the insurtech business. Apart from the above, the main disruption in the global financial sector is expected to result from ledger technologies such as blockchain. Although the use of this type of technologies is not yet widespread, it is currently emerging in Spain in areas such as 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. 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?

The feasibility of setting up and operating out 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 today, there is no specific regulation governing fintech or insurtech companies in Spain.

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 founded 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).

Crowdfunding has also grown 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 to demonstrate 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?

The (i) Spanish "patent box" regime and the research, development and innovation tax credit potentially applicable to Spanish resident

companies engaged in tech/fintech activities, and (ii) the corporate income tax benefits for start-ups (e.g. a 15% rate for the start-up's first two fiscal year, 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 Exchange Commission or 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 €6m, only €2m 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, it has been estimated that the Spanish fintech sector has received approximately €300m in financing rounds (source: http://spanishfintech.net/entrevista-jesus-perez/). Among the most notable investments are Peer Transfer (international educational payment tool), which has received €18m from Bain Capital and SpotCap (alternative financing platform), which received €31.5m from the private equity house Finstar Financial Group. Other noteworthy financing rounds include NoviCap (invoice trading marketplace) and Housers (real-estate financing platform), which received $1.7m and €0.85m, respectively, in the latest financing rounds.

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.

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 of crowdfunding and crowdlending 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 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?

Although no active legislative or governmental action has yet been taken other than the regulation of crowdfunding and crowdlending platforms, Spanish regulators show that they are receptive to the fintech activities. By way of example, the Spanish securities regulator (the *Comisión Nacional del Mercado de Valores*, "**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*, "**DGSFP**") 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*, "**AEFI**") 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 are required 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.

3.3 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 of 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?

Spanish Basic Law 15/1999 on the Protection of Personal Data ("**Spanish Data Protection Law**") transposes the EU Data Protection Directive (Directive 95/46/EC) into Spanish law. The Spanish Data Protection Law thus sets out the main rules and principles in Spain that apply to the collection and further processing of individuals' personal data. In Spain, fintech businesses must comply with the data-quality principle, as well as with information and consent duties, security standards and other registration and notification duties *vis-à-vis* the Spanish data protection authority (the "**Spanish DPA**").

As a general rule, the Spanish Data Protection Law and its ancillary regulations (mainly Spanish Royal Decree 1720/2007) are consistent with the rules set out in the EU Directive; however, certain local peculiarities nevertheless exist. As regards the legal basis entitling companies, including fintech businesses, to collect and process personal data, the Spanish Data Protection Law recognises, among other grounds, informed consent and the existence of a law authorizing or imposing that processing as legitimate grounds to process the data. However, the "legitimate interest" of companies, which is a legal ground to process persona data recognised by the EU Directive, was not correctly implemented in, and recognised by, the Spanish Data Protection Law. For this reason, for many years it was not possible (or extremely complex) to ground the processing of personal data on the existence of a legitimate business interest and this made many processing activities that were generally accepted in other EU jurisdictions difficult to legally ground in Spain.

In Judgment C/468/10, of 24 November 2011, the Court of Justice of the European Union ruled that Article 7.f of the EU Directive (recognising legitimate interest as a legal basis for data processing) has direct effect in Spain. However, since that time, the Spanish DPA has nevertheless followed a very restrictive interpretation of this legal ground and has on several occasions emphasised that, for the correct application of the "legitimate interest" criterion, a balancing test must be performed − i.e., the legitimate interests must be balanced against the rights and freedoms of data subjects − and the data controller must adopt effective measures mitigating the impact on data subjects' privacy. It is expected that a wider interpretation of this legitimate interest will be able to be argued more effectively following the implementation of the new General Data Protection Regulation (EU Regulation 2016/679), which clearly recognises legitimate interest as a legal ground for the processing of personal data.

Furthermore, several fintech businesses may act as data processors on behalf of other companies. The Spanish Data Protection Law imposes specific duties on such processors including, in particular, the necessity of implementing a list of mandatory security measures (as listed in Spanish Royal Decree 1720/2007) when processing personal data on behalf of Spanish companies. It is likely that those measures will cease to be mandatory upon the new General Data Protection Regulation's enactment, but will remain as a market standard in Spain.

Finally, as indicated, the General Data Protection Regulation will enter into force in May 2018 and will provide a more unified legal framework on the processing of personal data within the EU. This will undoubtedly benefit fintech businesses given that the same general rules will apply throughout all EU jurisdictions. Nevertheless, specific local data protection rules will remain applicable in Spain and, in particular, it is expected that a new Spanish Basic Data Protection Law – adapted to the general framework under the General Data Protection Regulation – will be made public and approved in the following months.

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 Spanish Data Protection Law and its ancillary regulations apply to data controllers incorporated and located in Spain, such as Spanish companies and Spanish branches of foreign companies. However, under certain circumstances and regardless the applicability of their local data protection laws, foreign fintech businesses may also fall within the scope of the Spanish Data Protection Law. This is the case, for instance, of EU and non-EU fintech businesses that operate in the Spanish market through an establishment in Spain. It should be noted that the Spanish DPA has interpreted the concept of "establishment" broadly and, in their opinion may include, for instance, affiliates providing ancillary consultancy services or sales support. This approach has been contested by the market.

The applicability of the Spanish Data Protection Law to non-EU fintech businesses may also result from the use by that fintech business of processing means located in Spain other than for transit purposes. For example, the Spanish DPA has on certain occasions (and contentiously) considered that the mere use of cookies implemented on Spanish devices qualifies as the use of "means located in Spain".

Finally, the Spanish Data Protection Law sets out various additional requirements to transfer personal data outside the Economic European Area ("**EEA**") or to other white-listed countries or companies apart from the requirements applicable in other EU jurisdictions. In general, an international transfer may be grounded on the individual consent of each affected data subject or, alternatively, on prior authorisation by the Spanish DPA. Other limited legal grounds exist, such as in the event of transfers required for the execution of money transfers. Conversely, the mere execution by the data exporter and the data importer of the "EU Model Clauses" is not in itself sufficient for carrying out international data transfers. EU Model Clauses properly executed by the parties must be filed with the Spanish DPA for analysis and a decision on whether or not to grant the authorisation previously indicated.

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

Administrative sanctions arising from data protection breaches in Spain are among the highest potential sanctions in the EU. It is also worth noting that the Spanish DPA is very active and opens hundreds of sanctioning proceedings per year. For these reasons, compliance with data protection duties is of the utmost importance for fintech business operating in Spain.

The amount of the fines depends on the severity of the breach. The Spanish Data Protection Law sets out three different ranges of sanctions: (i) minor infringements, which are subject to fines ranging from €900 to €40,000; (ii) severe infringements, ranging from €40,001 to €300,000; and (iii) very severe infringements, ranging from €300,001 to €600,000. The Spanish DPA is also vested with other sanctioning powers, including the power to immobilise data files if data subjects' rights and freedoms are put at stake. Some of the data processing that is likely to happen within the fintech activities, such as international transfers of data flows outside the EEA are considered very severe infringements and, thus, may be sanctioned with fines of up to €600,000.

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

The approval in July 2016 of the EU Directive on Security of Network and Information Systems (the so-called "**NIS Directive**") has been the most important recent milestone on cybersecurity. It represents the first EU-wide rules on cybersecurity; it has not yet been transposed into Spanish law. Until transposition occurs, the regulation of cybersecurity matters in Spain remains disseminated and insufficient. In general, the most important Spanish rules currently in force regarding cybersecurity that could potentially affect fintech businesses are those set out in (i) the Spanish Criminal Code (according to which specific acts, mainly related to hacking or the illicit collection or discovery of information and communications, may qualify as a criminal offence), (ii) data protection laws (establishing a list of mandatory security measures applicable to all entities that process personal data in Spain), and (iii) Spanish e-commerce law, which was amended in 2014 to establish specific obligations in connection with cybersecurity incidents applicable to information society services providers, domain names registries and registrars. These obligations, resulting from e-commerce law, are twofold: to collaborate with the corresponding computer emergency response teams in the wake of cybersecurity incidents affecting the internet network and to follow specific recommendations on the management of cybersecurity incidents, to be developed through codes of conduct (which have not yet been developed).

Also, operators of critical infrastructure (i.e. entities responsible for investments in, or day-to-day operation of, a particular installation, network, system, physical or IT equipment designated as such by the National Centre for Critical Infrastructure Protection (CNPIC) under Law 8/2011) are subject to specific obligations such as providing technological assistance to the Ministry of Home Affairs, facilitating the inspections performed by the appropriate authorities and creating the specific protection plan and the operator's security plan, etc. Fintech businesses providing services to any of the operators appointed as operators of critical infrastructure may then be subject to the specific requirements set out in these rules.

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 primarily relating 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 and the potential reporting of various events to the corresponding authorities.

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, other obligations applicable to the 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 fintechs' regulatory compliance).

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 Statute of Workers ("**SW**") acts as the basic law for all matters related to employment. The SW was approved by a consolidated text passed by Royal Legislative Decree 2/2015 of 23 October.

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 the Social Security, notifying the Social Security of the employment, health and safety and work obligations, registering employment contracts).

On the dismissal side, Spanish law recognised 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 claims 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.

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

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 2017, the interprofessional minimum monthly salary was set at €707.70.

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. Employees in Spain enjoy 14 days per year as official paid holiday.

Generally speaking, in the event of the birth, adoption, or fostering of a child, employees are entitled 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 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 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.

(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 effects 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 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 Isabel Aguilar Alonso in the preparation of this chapter. Isabel Aguilar Alonso is a senior associate in Uría Menéndez's Madrid office. She joined the firm in 2008 as an associate in the Corporate and Commercial area and her professional practice primarily focuses on financial and banking regulatory law. She frequently acts as advisor to credit entities, investment firms and management companies on matters such as authorisation, significant holdings, cross-border provision of services, marketing of products, MiFID rules and disciplinary proceedings. From January to June 2014 she was seconded to the Luxembourg law firm Elvinger, Hoss & Prussen.

Leticia López-Lapuente
Uría Menéndez
Príncipe de Vergara 187
28002, Madrid
Spain

Tel: +34 91586 0400
Email: leticia.lopez-lapuente@uria.com
URL: www.uria.com

Leticia López-Lapuente is a lawyer in the Madrid office of Uría Menéndez. 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.

Livia Solans
Uría Menéndez
Príncipe de Vergara 187
28002, Madrid
Spain

Tel: +34 91586 0081
Email: livia.solans@uria.com
URL: www.uria.com

Livia Solans Chamorro is an associate based in Uría Menéndez's Madrid Office. She joined the firm in 2009 and from 2013 to 2014 she was seconded to the Peruvian law firm Payet, Rey, Cauvi.

Her professional practice primarily focuses on commercial and corporate law, especially in the telecommunications and technology sectors. Livia provides day-to-day advice to clients operating in these sectors on regulatory, corporate and commercial matters, including the drafting and negotiation of contracts, regulatory advice, outsourcing, etc. She is also involved in major transactions advising businesses and investors in mergers and acquisitions, joint ventures and outsourcing projects. Her international experience includes cross-border deals, especially in Latin America.

URÍA
MENÉNDEZ

Uría Menéndez is the leading law firm in the Ibero-American market. With 555 lawyers, including 128 partners, the firm advises on Spanish, Portuguese and EU law in relation to all aspects of corporate, public, litigation, tax and labour law. We have 17 offices in 13 countries and over 2,000 clients.

In January 2015, after nearly 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.

Uría Menéndez celebrates its 70th anniversary this year. Our decades of experience have made the firm a frontrunner in client service, intellectual leadership and talent recruitment in Spain, Portugal and Latin America. It maintains the academic tradition of its two founders, with more than 50 university professors among its ranks, as well as a commitment to society that the founders – who were both "Prince of Asturias" award winners (the highest recognition awarded in Spain to extraordinary men from all backgrounds) – maintained throughout their lives.

Sweden

Martin Pekkari

Anders Bergsten

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 within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Investments in fintech are increasing rapidly in Sweden. In terms of investment volume, Stockholm is often regarded as being one of Europe's main centres for fintech investments. The payments segment is currently the largest of the Swedish fintech industry segments whereas asset management has thus far not been as large, but it is a growing segment. Peer-to-peer lending, insurance and blockchain 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 and automated advice on investments. In general, a 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.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

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 for individuals who invest in small companies. The incentive is granted in the form of a deduction from capital income equal to 50 percent 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.

It may also be noted that the Swedish Government recently proposed new tax rules 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 proposed rules will be 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 will be payable. The proposal has been criticised for being too narrow in scope in various respects (for instance, activities comprising of banking and financing are excluded) so it remains to be seen what effect, if any, the proposed rules will have on the fintech business if the rules are enacted. The rules are proposed to enter into force on 1 January 2018.

Lastly, a special tax relief may, under certain circumstances, be granted to foreign key personnel for a limited time period whereby 25 percent of income is exempt from income tax for personnel qualifying under these specific rules (Sw. *expertskatteregler*).

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 Aktietorget.

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 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 seeking a secondary listing from certain foreign 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 a number of smaller and medium sized exits in the broader fintech area, and there are a number of notable exits underway in the next few years (including Izettle and Klarna).

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 are 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 Payment Services Directive (PSD1). It may be noted that the new Directive on Payment Services in the Internal Market (PSD2) is predicted to have a major impact on the fintech industry, likely creating opportunities for smaller service providers to compete in a space that has historically been reserved for the major banks.
- The Electronic Money Act (2011:755), implementing the EU Electronic Money Directive.
- The Reporting of 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).
- 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 (2009:62), implementing the EU Directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (AMLD III).
- The Identification of Reportable Financial Accounts due to the FATCA Agreement Act (2015:62) and (ii) 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 (ii) 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.

3.2 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?

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. The Government has instructed the SFSA to evaluate the existing regulatory framework and the need for new rules in light of the developments and the SFSA has arranged round-table discussions with market participants. The

SFSA also issued a report on crowd funding in December 2015 and, in July 2016, the Swedish Government appointed a committee to review the current regulatory framework and the need for new rules within this area. The committee has been instructed to present its report in December 2017. The SFSA also recently issued a memorandum with a summary of its view on several aspects related to automated investment advice.

3.3 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 Swedish Personal Data Act ("**DPA**"), which implements the EU Data Protection Directive (Directive 95/46/EC). This applies to all fintech businesses, although it should be noted that the DPA is subsidiary to all other legislation. However, as is the case with all EU members, in May 2018 the Swedish legislation will be replaced by the EU's General Data Protection Regulation ("**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?

If not established in another EU Member State, the DPA applies to organisations which use equipment located in Sweden. Yes, the DPA 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.

Administrative fines (for organisations), damages, criminal sanctions (for individuals) which may include fines or a prison sentence for up to two years.

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

The DPA contains rudimentary rules on cyber security. There are also regulations imposed by the SFSA which may have cyber security implications.

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 (2009:62) ("**AMLA**"), the Penalties for Money Laundering Offences Act (2014:307) ("**APML**") and the Penalties for Financing of Particularly Serious Crimes Act (2002:444) ("**PSCA**").

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 AMLA are obliged to monitor and report matters involving suspicious transactions of money laundering or terrorist financing. The requirements of examination include customer due diligence and review of transactions. Currently, the mere provision of technical infrastructure is not subject to AMLA.

The PMLA contains criminal law provisions on money laundering. Provided that the measure is intended to conceal the fact that money or other property derives from an offence or criminal activities, 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 financing of particularly serious crimes, 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 needs 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**"), employment relationships 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 wages. If the employer is bound by a collective bargaining agreement, it normally provides for minimum wages. 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, regardless of whether such vacation has been earned or not (with certain exceptions which may apply during the first year of employment).

Parental leave

An employee who becomes a parent is entitled to full or part-time leave until the child is 18 months (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 (60 days are, however, earmarked for each parent). The parent is further entitled to part-time reduction (by 25%) of normal working hours until the child is eight years old (or 12 years old if the child was born in 2014 or later). 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.

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 works, there is no time limit for staying in Sweden and they do not need to register with Swedish Migration Agency. If the employment will last for more than a year, the EU citizen should 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 a 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 route 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 (1990:409), which imposes civil and criminal liability for unauthorised use or disclosure.

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 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.

Acknowledgment

The authors would like to acknowledge the assistance of their colleague Johan Lindström in the preparation of this chapter. Johan is a member of Mannheimer Swartling's Corporate Commercial practice (described below) and regularly advises clients in relation to IT, technology and outsourcing contracts.

Martin Pekkari
Mannheimer Swartling
Norrlandsgatan 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 comprises a number of legal areas. Consequently, he has extensive experience from managing and coordinating projects including projects of a cross-border nature and where lawyers in multiple jurisdictions are involved.

Martin has experience in 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).

Anders Bergsten
Mannheimer Swartling
Norrlandsgatan 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, license, maintenance and support contracts, cloud service contracts, software development contracts, as well as information sharing and co-operation contracts.

Anders also regularly advises clients in relation to data protection law matters. He is well versed in the upcoming changes to EU data protection and cybersecurity 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, as well as several group-wide IT outsourcings. 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.

MANNHEIMER SWARTLING

Mannheimer Swartling is the leading business law firm in the Nordic region. The firm is a full service firm with four 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, 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 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.

Chapter 30

Switzerland


Eric Stupp


Peter Ch. Hsu

Bär & Karrer 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 within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

In Switzerland, fintech has evolved significantly and gained increasing interest. Approximately 100–200 active companies in various sub-sectors form the core of the diverse Swiss fintech ecosystem. The industry has formed a number of associations and shared interest groups (*e.g.* the *Swiss Finance + Technology Association*, *Swiss Financial Technology* and *Swiss Finance Startups*) to promote, together with investors, experts and media, the development of a strong Swiss fintech sector.

Swiss-based fintech businesses include robo advisory and social trading services, crowdfunding and crowdlending platforms as well as payment systems. A key focus are blockchain-based businesses, in particular in the areas of cryptocurrencies and decentralised transaction platforms (*e.g. Ethereum, Lykke, Monetas*), many of which are based in the so-called "cryptovalley" in the Canton of Zug (the city of Zug is also the first municipality worldwide to accept payments in *bitcoin*).

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

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, certain amendments to existing regulation are currently being discussed that will further ease the Swiss regulatory framework for fintech (*see* question 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)?

Switzerland has an active start-up scene, with funding opportunities for companies at every stage. 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. However, the current perception is that the considerable funding potential is not yet fully exploited and that access to funding for fintech start-ups could be improved.

Crowdfunding as an alternative source of funding shows rapid growth rates in Switzerland. The first platform was founded in 2008 and currently there are more than 40 active platforms (compared to only four in 2014).

Furthermore, since November 2016, the association *F10*, a fintech incubator and accelerator, has been supporting and guiding start-ups in transforming their ideas into successful companies. Its members include the Swiss financial infrastructure provider SIX Swiss Exchange Ltd, banks and insurance companies, enabling *F10* to foster collaboration between start-ups and established financial institutions.

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 to 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 benefitting investors. In addition, again depending on the tax domicile of the company, the ordinary profit tax rate in Switzerland can be as low as 12%.

In particular, start-ups may benefit from a tax holiday on the cantonal and federal level if their place of effective management 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). Currently, there are furthermore discussions in Switzerland regarding the introduction of special R&D deduction regimes.

Finally, it is common in Switzerland to discuss the tax consequences of an envisioned structure with the competent tax administration.

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. Essential criteria include *e.g.* that the issuer has existed as a company for at least three years, has a reported equity capital of at least CHF 2.5 million, a spread of shares ("free float") of at least 20% and a minimum capitalisation of the securities in public ownership of CHF 25 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 or major publicly announced business sales in the area of fintech. However, the shares of Leonteq Ltd. (formerly known as EFG Financial Products Holding AG), a technology and service provider for investment solutions, have been listed on the SIX Swiss Exchange since 2012.

Furthermore, the shares of Crealogix Holding AG have been trading on the SIX Swiss Exchange since 2000. Crealogix is a software house and service provider for digital banking.

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. Rather, the legal framework governing the activities of fintech operators consists of a number of federal acts and implementing ordinances as well as circulars and other guidance issued by the Swiss Financial Market Supervisory Authority FINMA ("**FINMA**"). Fintech business models have to be assessed in light of this regulatory framework on a case-by-case basis.

Based on their (intended) activities, fintech operators may in particular fall within the scope of the Banking Act (if engaging in activities involving the acceptance of deposits from the public; *see* question 3.2), the Anti-Money Laundering Act (if active as a so-called financial intermediary, *e.g.* in connection with payments; *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 a proprietary trader), or the Insurance Supervision Act (if acting as an insurer or insurance broker). Moreover, *inter alia,* the Consumer Credit Act, the Data Protection Act 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 a regulatory audit firm appointed by the supervised firm conducts most of the on-site reviews. 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 unified supervisory authority for the Swiss financial market, *inter alia*, ensuring a consistent approach to the qualification and regulatory treatment of fintech operators. 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).

3.2 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?

Representatives of FINMA have expressed on various occasions that the Swiss regulator encourages innovation in the Swiss financial marketplace. Furthermore, FINMA's CEO in particular pushed for legislative change to lower market entry barriers for innovative financial services providers and to establish Switzerland as a fintech hub. In the wake of this call for action, the Swiss Federal Counsel proposed in late 2016 to amend banking regulation to ease the Swiss regulatory framework for fintech operators. A public consultation process on the draft legislation was opened in February 2017. The proposed new rules rest on three main pillars:

- **Banking licence "light"**: Generally speaking, Swiss banking regulation applies to persons that accept, on a commercial basis, or hold themselves out as accepting, deposits from the public. This condition is currently deemed satisfied as soon as a person accepts on an ongoing basis more than 20 deposits, regardless of the individual or total amounts, or publicly solicits deposits, regardless of how many deposits result from such activity. If the activity of a fintech company is such that it meets or exceeds this threshold, a full banking licence is required. The stringent regulatory requirements for obtaining and maintaining a banking licence create a significant market entry barrier for fintech firms. The legislative proposal seeks to solve this problem by introducing a new type of licence for fintech firms and other entities that accept public deposits but do not engage in commercial banking. Holders of this banking licence 'light' will be able to accept public deposits up to a total value of CHF 100 million but will not be allowed to invest the deposits or pay interest on them. A higher threshold than CHF 100 million can be allowed by FINMA, on a case-by-case basis, if customers are protected through additional safeguards. The regulatory requirements for obtaining and maintaining such licence will be significantly reduced versus a fully-fledged banking licence. *Inter alia*, less demanding standards will apply regarding financial reporting and audits as well as, subject to implementing provisions that are yet to be developed, organisational, equity, capital adequacy and liquidity requirements. Deposits accepted under a banking licence "light" will not be covered by the Swiss deposit protection system, a fact that licence holders have to inform their customers about.
- **Innovation sandbox**: Many fintech business models rely on scalability and require fintech operators to hold, for a certain period of time, third party monies deposited by a large number of individuals (*e.g.* crowdfunding). In this context, the abovementioned threshold of a commercial banking

activity will typically be met or exceeded while the individual deposits may be rather small. Therefore, it is proposed to introduce a "sandbox", *i.e.* an innovation space which is fully exempted from a regulatory licence requirement under banking regulation. Pursuant to the proposed draft legislation, firms will not require a banking licence as long as they do not accept deposits from the public in excess of CHF 1 million (even if they publicly hold themselves out as accepting deposits). This threshold will be measured on the basis of the aggregate deposits held at any given point in time. The sandbox would allow fintech innovators to develop and test their business idea without incurring the burden of requiring a banking licence or complying with prudential supervision requirements. However, firms that are mainly active in the financial sector will only be allowed to benefit from this exemption if no interest is paid on the deposits and the funds are not invested. Furthermore, a firm making use of the sandbox exemption will be required to inform its customers that it is not supervised by FINMA and that deposits are not covered under the Swiss depositor protection system.

- **Extension of the maximum holding period of third party monies on settlement accounts**: Under current Swiss banking regulations, 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). At present, FINMA considers that this exemption applies only if the monies may be held on a settlement account for seven days at most. It is proposed to extend this maximum holding period to 60 days. This extension will *e.g.* allow crowdfunding companies to hold funds for a longer period without triggering a licence requirement. Payment services providers are another category of fintech operators that may be able to benefit from this exemption if their business model does not require them to hold funds for more than 60 days.

It should be noted that the proposed new exemptions and reliefs do not extend to anti-money laundering regulations, which will continue to apply to fintech firms if they act as financial intermediaries (*see* question 4.5). The public consultation process will last until 8 May 2017. Assuming the proposals are received positively by all stakeholders, the amendments are likely to enter into force at the earliest in 2018.

In addition to the above, FINMA has already implemented a number of changes to its circulars (which specify the practice of the regulator under the current legislation) to make them more technology-neutral (*e.g.* by not requiring certain documentation to be held in physical written form) and therefore supportive of innovative business models. *Inter alia*, it published a new circular facilitating video and online customer identification for anti-money laundering purposes. FINMA also holds regular fintech roundtables and has established a dedicated fintech desk to interact with fintech startups.

3.3 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. 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 (incl. by frequent travel) on the ground in Switzerland. Notably, the Banking Act and the Anti-Money Laundering Act apply only to foreign operators that have established a relevant physical presence in Switzerland, *e.g.* a branch or representative office. Cross-border operators should refrain from creating an appearance of "Swissness" even though not located and regulated in Switzerland, *e.g.* by using a ".ch" website or referring to Swiss contact numbers or addresses. As Switzerland is not a member of the EU nor of the EEA, no passporting regime is available.

It should, however, 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.

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 Data Protection Act ("**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›). The registration is free of charge.

Swiss data protection law is currently under revision. The revised DPA is, however, not expected to enter into force before January 2019.

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 outlined in question 4.1 above, the processing of personal data on equipment located in Switzerland is, in principle, in the scope of the DPA. 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 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 an adequate level of data protection. In particular, all EU Member States are deemed countries with adequate data protection rules. The main 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 damage 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, the competent criminal judge may, upon a complaint, sanction private persons with a fine of up to CHF 10,000 if they have wilfully breached certain information obligations stipulated in the DPA.

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.
- The Swiss Criminal Code ("**CC**") 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.) as regards to risks relating to the use of modern information and communication technologies.

In 2011, Switzerland ratified the Council of Europe Convention on Cybercrime of 2001 (which entailed certain amendments of the CC 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 Anti-Money Laundering Act ("**AMLA**"), the Anti-Money Laundering Ordinance ("**AMLO**"), ordinances and circulars of FINMA as well as the rulebooks of self-regulatory organisations. Generally speaking, AML regulation applies to so-called financial intermediaries (and partially to merchants accepting large sums, *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. If this is the case and no exemptions are available, the fintech firm is required to either join a recognised Swiss AML self-regulatory organisation or, alternatively, submit to direct AML supervision by FINMA. 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 recently 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.

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. Depending on the specific business model, the Telecommunications Act may furthermore 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 relatively liberal. Private employment contracts can usually be terminated quite easily and such terminations, as a general

principle, do not lead to any obligations to render severance payments. 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. The party having received the unlawful notification may raise a claim for compensation up to a certain threshold. Furthermore, there are some 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 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. In Switzerland, no statutory minimum salary exists, but for certain professions, collective and standard employment agreements stipulate 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, 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 need, in principle, to be compensated (by remuneration or leisure time). However, public law provisions limit the maximum working time (to 45 hours or 50 hours per week, respectively).

Employers in Switzerland must allow their employees to have at least four weeks holiday per year, and in case of employees under the age of 20 at least five weeks holiday (excluding public holidays). Part-time employees have a *pro rata* entitlement. During the holidays, the employer must pay the full 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 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. In contrast, paternity leave is not granted under Swiss law, but may be agreed upon by the parties.

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?

Switzerland has a dualistic system for the admission of foreign workers.

Nationals from EU/EFTA countries can benefit from the Agreement on the Free Movement of Persons (*Personenfreizügigkeitsabkommen*). They do not need a work permit if they work for less than 90 days per calendar year for a company in Switzerland. The same applies to self-employed service providers and companies based in these countries sending 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 either (i) a short-term permit for up to four months uninterrupted stay or 120 days per year, (ii) a short-term permit for up to one year, its validity depending on the validity period of the limited employment contract (the "L-Permit"), (iii) a long-term permit for five years based on an unlimited employment contract (the "B-Permit"), or (iv) a so-called border-crosser permit if they continue to live outside of Switzerland but commute to their Swiss workplace (the "G-Permit").

In contrast, non-EU/non-EFTA citizens have to apply for either (i) a short-term permit up to four months/120 days per calendar year, (ii) a short-term permit up to 12 months based on a limited employment contract (the "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 (the "B-Permit"). The work permits for citizens of non-EU/non-EFTA countries are subject to a nation-wide quota. Furthermore, such permits are only granted to highly qualified employees. 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.

Special rules apply for persons holding a work permit of 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.

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.

However, there are no additional hurdles regarding immigration rules for the financial sector.

6 Technology

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

Assuming that fintech products are typically based on computer programs, they are protected by copyrights if they possess an individual character (*i.e.* if they are original). In practice, this threshold is met by 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 deceased. Software that is integral to an invention may further be patented. However, computer programs "as such" are excluded from patentability.

In addition, marketable products are protected by the Unfair Competition Act against their reproduction by technical means without own reasonable efforts. The design of fintech products (portables, wearables, etc.) may further be protected for a maximum period of 25 years by designs rights.

Unlike the laws of EU Member States, Swiss law does not provide for database rights.

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

According to statutory Swiss law, where a computer program has been created under an employment contract 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 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 Switzerland has been chosen as 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 basically 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. 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.

Acknowledgment

The authors would like to acknowledge the assistance of their colleagues Daniel Flühmann and Joel Fischer in the preparation of this chapter.

Eric Stupp
Bär & Karrer Ltd.
Brandschenkestrasse 90
8027 Zurich
Switzerland

Tel: *+41 58 261 50 00*
Email: *eric.stupp@baerkarrer.ch*
URL: *www.baerkarrer.ch*

Eric Stupp heads the Bär & Karrer's financial services department and co-heads the internal investigation and cross-border proceedings team. His practice focuses on advising banks, insurance companies, asset managers and other financial intermediaries on regulatory matters, enforcement proceedings and on M&A transactions.

In recent years, he has regularly advised financial institutions and regulatory bodies in connection with internal investigations on cross-border issues. In particular, he has assisted clients in numerous proceedings initiated by the US Department of Justice, the New York Department of Financial Services and other US or European authorities.

Eric Stupp is a regular speaker at expert conferences addressing these matters. He was a member of Bär & Karrer's management committee for eight years. He is the vice-chairman of the board of directors of Goldman Sachs Bank AG, Zurich and a member of the boards of other financial and nonprofit institutions.

IFLR 1000 2016 and *Who's Who Legal 2015* list Eric Stupp as one of the leading banking lawyers in Switzerland.

Peter Ch. Hsu
Bär & Karrer Ltd.
Brandschenkestrasse 90
8027 Zurich
Switzerland

Tel: *+41 58 261 50 00*
Email: *peter.hsu@baerkarrer.ch*
URL: *www.baerkarrer.ch*

Peter Hsu is Bär & Karrer's key contact for the practice area of banking and insurance. His practice focuses on banking, insurance, financing and capital markets. He regularly advises Swiss and foreign banks, securities dealers, insurers and other financial intermediaries as well as fintech businesses with regard to a wide range of regulatory, contract law and corporate law matters. Moreover, he often advises clients on M&A transactions.

Peter Hsu has published several books and articles on topics in banking, insurance and capital markets and is regularly invited to speak on these topics.

Peter Hsu is ranked as a leading individual in the practice areas of Banking & Finance as well as Insurance & Reinsurance and listed as "most highly regarded" practitioner in Insurance & Reinsurance (*Who's Who Legal*). He is described as "extremely knowledgeable" in insurance and regulatory matters and lauded for his "business oriented approach" and wins praise for his "unparalleled abilities" (2016). In *IFLR 1000*, a client characterises him as "very knowledgeable, detail-oriented and very open to novel solutions and approaches" (2016).

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.

2016, 2015 and 2014 Mergermarket European M&A Awards.

2016, 2013 and 2012 Chambers Awards.

2016, 2015 and 2014 Legal 500 ("most recommended law firm in Switzerland").

2016 Trophées du Droit.

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

Lee and Li, Attorneys-at-Law

Benjamin K. J. Li

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 within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Fintech is a new and developing area 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 Statute for Fintech Innovation Experiment ("Fintech Innovation Act") on January 12, 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 mechanism 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 mechanism; regulatory updates; and risk management.

In addition, conducting finance-related activities in Taiwan generally requires a licence from the FSC. However, similar to the "regulatory sandbox" concept raised by Financial Conduct Authority in UK, the FSC will set up a fintech experiment mechanism under the draft of the Fintech Innovation Act to provide a safe environment for the development and testing of fintech, exempt fintech innovation from the current licence requirements for the 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 with the FSC for prior 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. For example, according to FSC's policy, it would be possible to test peer-to-peer lending (P2P Lending) in Taiwan under the Fintech Innovation Act.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

Please refer to our advice in question 1.1 above. Currently, the FSC does not prohibit any type of fintech business from financial innovation experiments under the Fintech Innovation 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)?

Crowdfunding activity in Taiwan took a lead from the US JOBS Act crowdfunding rules and global fintech trends in crowdfunding to micro innovative enterprises for their funding needs. The two non-listed crowdfunding options in Taiwan (they are not IPO, see further requirement for an IPO advised in question 2.3 below) are as follows:

1. Non-equity-based crowdfunding – Gofunding Zone

   Taipei Exchange set up the Gofunding Zone on August 19, 2013. The Gofunding Zone provides only information disclosure functions. The plan is to increase the exposure opportunities of domestic funding projects and enhance the credibility of funding platform providers to increase the willingness to engage in crowdfunding. Gofunding Zone is only subject to information disclosure requirement and the investing funds shall be handled by the sponsors, sponsees and funding platform providers.

2. Equity-based crowdfunding – Go Incubation Board

   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 self-concluded financial statements (if the capital is less than NT$30,000,000) 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?

Taiwan's Executive Yuan proposed draft amendments to the Statute for Industrial Innovation on February 13, 2017. According to Articles 23-1 and 23-2 of the draft amendment, 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$300,000,000 in the fifth year since incorporation) and the total amount invested in the innovative enterprise reaches 35% of the paid-in capital or NT$300,000,000 (whichever is lower), or if an individual whose investment in an innovative enterprise reaches NT$1,000,000 and such individual has held the shares in the innovative enterprise for more than three 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 two non-listed crowdfunding options, Gofunding Zone and 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 shareholders' equity 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.
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; and (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.

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 approvals to five E-payment service providers (other than banks) to conduct the E-payment business in Taiwan. In addition, the draft of the Fintech Innovation Act announced on January 12, 2017 is another fintech legislation to offer a safe harbour for fintech service providers to experiment with financial technology innovations in Taiwan.

3.2 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?

According to the legislative purpose of the draft of the Fintech Innovation Act, 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 with the FSC for prior approval to conduct financial innovation experiments in accordance with the Fintech Innovation Act. We believe this is a good indication of Taiwan government's open-minded policy principles for fintech services.

3.3 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 draft of the Fintech Innovation Act does not stipulate that foreign fintech institutions may 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, will be 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.

The draft of the Fintech Innovation Act does not clearly provide that fintech business would be 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 be 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, 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) the place where the properties or property interests of the sanctioned person are located.

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.

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 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 LAS occurs.

In addition, Taiwan's Legislative Yuan passed the amendments to the LSA on December 6, 2016 which has taken effect on January 1, 2017. The key points of the amendments to the LSA include implementation of a five-day work week; a sharp increase in overtime pay for working on a rest day; reduction of public holidays; increase in the number of annual leave days; method of arranging annual leave and payment for unused annual leave; rest time between shifts; employers' obligation to provide information on wage calculation; protection of whistle-blowers'/workers' rights to file complaints; and raising fines for violations of the LSA. The amendments have a 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 IC 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 on 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 patent, copyright or trade secret in Taiwan in accordance with the Patent Act, Copyright Act and Trade Secret Act. As to patent, 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 Intellectual Property Office under the Trademark Act. For copyrights and trade secrets, there is no registration or filing requirement for a copyright or a trade secret for the 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 patent, 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 for 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 patent, 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 secret and copyright, as advised in question 6.1 above, there is no registration or filing requirement 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) information that may be used in the course of production, sales or operations; (ii) having the nature of secrecy, with economic value; and (iii) adoption of 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 "First Publication" or "Reciprocity" requirement. Since Taiwan's accession to the WTO as of January 1, 2002, the works of natural or juristic persons of WTO members enjoy the same copyright protection under 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, 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
7F, 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 Taiwan market.

Benjamin K. J. Li
Lee and Li, Attorneys-at-Law
7F, 201 Tun Hua N. Road
Taipei, 10508
Taiwan

Tel: +886 2 2715 3300 ext. 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 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).

理律法律事務所
LEE AND LI
ATTORNEYS-AT-LAW

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 the financial related industry, 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.

Turkey

SRP-Legal

Dr. Çiğdem Ayözger

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 within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Istanbul is becoming a "hot spot" for Fintech businesses in the Eastern Europe and Middle East Region. There are more than 200 Fintech businesses in Turkey most of which are located in Istanbul.

Fintech Business in Turkey operates in the following businesses:

- Payment Service Provider;
- Instore Payment/POS;
- Bill Payment;
- Prepaid And Discount Cards;
- Pre-Order And Pay;
- Mobile Operator Payment;
- Money Transfer, Order Screening;
- Collection;
- Digital Wallet;
- Digital Banking;
- Reward-Based Crowdfunding;
- Donation-Based Crowdfunding;
- Public Market And Real Estate Investment;
- Insurtech;
- Credit Compare Or Consolidation Financing;
- Credit Scoring;
- Supply-Chain Financing;
- Personal Finance Management; and
- Corporate Finance; Bookkeeping, Payroll, Accounting and E-Invoice.

Fintech businesses mainly operate in payment services.

Regtech is also one of the emerging subcategory of Fintech that we expect to continue growing in the near future. With the enactment of the Law on Payment and Security Settlement Systems, Payment Services, and Electronic Money Institutions in 2013, the payment environment has been continuously growing in favour of Fintech business. Also, digital banking is being used more and more by consumers.

2016 saw Fintech investment in Turkey has tripled compared to the previous year, raising from six deals to 16 deals and the value of the investment has tripled itself, again compared to the previous year, raising from approximately 10 million USD to 30 Million USD.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

There are no prohibited or restricted businesses that are specific to Fintech business in Turkey. In practice, the main restrictions that Fintech companies or investors come across arise from Turkish Data Privacy and Protection Regulations. For example, in payment systems and electronic money sectors, there are restrictions regarding data management. Payment institutions and electronic money institutions shall retain their main and secondary data managements systems in Turkey.

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 business can be financed through two traditional models: equity; and/or debt financing.

Many Fintech start-ups have been raised from equity financing such as venture capitalists and/or business angels. Another equity financing model is shareholder's contribution into business in the form of cash, receivables, security and participation shares, intangible rights, movable or immovable properties and other transferable rights. Crowdfunding is another way of financing which needs to be regulated in order to support the expectations and needs of businesses. There is an amendment proposal on Capital Markets Law to set the principals and terms of crowdfunding.

In the terms of debt financing, Fintech companies have to apply to a bank to raise a traditional bank loan. There are different types of bank loans but none of them are specific to tech or fintech sectors and they are generally available to qualifying companies or investors in all sectors. Also, there are some NGOs that support start-ups again not specific to tech or fintech sectors. The Small and Medium Enterprises Development Organization of Turkey is one of the supporters of start-ups via 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?

There are some general incentives for investments that may apply to

tech/fintech businesses including:

- According to Law No. 4691 on Technology Development Zones, the companies located in techno parks can benefit from numerous tax incentives including exemption of corporate tax, income tax and VAT. Also, if the company is essentially a research and development company, that company has the right to deduct 50% of the social security premium exemption for its employees for a period of five years.
- By-Law regarding Individual Investments/Angel Investment Funding offers 75% value of the participation shares of the qualifying Turkish resident joint stock companies or held by business angels/individual investors can be deducted from the individual investors/business angel's income tax for the next tax year.
- Also, there is the general Investment Incentive System which was introduced with Decree no. 2012/3305 of the Turkish Counsel of Ministers. The procedures about the Decree were detailed in the Communique no. 2012/1 of the Turkish Ministry of Economy.

This investment incentives programme comprises five different schemes:

1. General Investment Incentive Scheme.
2. Regional Investment Incentive Scheme.
3. Priority Investment Incentive Scheme.
4. Large Scale Investment Incentive Scheme.
5. Strategic Investment Incentive Scheme.

There are various support measures provided according to those schemes such as VAT exemption, custom duty exemption, tax deduction, etc.

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

According to Capital Markets Regulations, the following key requirements must be satisfied in order to apply Borsa İstanbul for an IPO:

- Company must be established as a joint stock company.
- Company must amend its Articles of Associations to comply with the requirements stipulated under Capital Market Law and Regulations.
- Company has to enter into an agreement with a brokerage investment house.
- Company shall draft a financial statement in accordance with Capital Markets Regulations and these statements are subject to an audit by an independent audit firm.
- Company shall draft a prospectus regarding the current status of the company.

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

In 2013, Mastercard acquired Provus Bilişim Sistemleri A.Ş., a payment solution service and processing provider with an undisclosed transaction fee.

In 2014, Monitise plc, a mobile payment solutions company located in UK, acquired Pozitron, Turkish mobile commerce technology provider for 100 million USD.

Also in 2014, Wirecard AG, an electronic payment and risk management service provider located in Germany, has acquired Mikro Ödeme Sistemleri A.Ş. which provides services including mobile payment to direct carrier billing services for 26 million Euros.

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 2013, the Law on Payment and Security Settlement Systems, Payment Services, and Electronic Money Institutions has been enacted to supervise the payment systems, electronic money institutions and payment institutions in Turkey. In order to run operations under this Law, Companies must apply to the Turkish Banking Regulation and Supervision Agency for payment institution and electronic money institution licences, or to the Central Bank of Turkey for payment and/or settlement system licences.

Also, for Digital Banking, service providers must ensure they comply with the relevant provisions of Turkish Banking Law No: 5411.

For insurtech business, insurtech companies needs to obtain at least brokerage licence.

3.2 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?

- Financial regulators and policy-makers generally are very receptive and supportive about the fintech environment. For example, the Banking Regulation and Supervision Agency, regulating the payment service institutions and electronic money institutions, stressed "such institutions are becoming a key element to solid growth in the financial sector" in its 2015 annual report.
- The Central Bank of The Republic of Turkey which regulates the payment and settlement systems operators stresses that "Such system has become a key stone to achieve increasing effectiveness of the Central Bank's money policy, financial stability and stable long-term growth".

3.3 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?

All Fintech businesses which wish to operate in payment services, e-money, insurance, digital banking and payment system operations businesses in the territory of Turkey must be licensed either by The Banking Regulation and Supervision Agency, Central Bank of The Republic of Turkey or relevant authorities supervising the sectors. These kind of companies must not only obtain a licence from the authorities, they are also subject to relevant laws and regulations. In practice, we usually come across if a particular fintech activity constitutes a regulated activity, therefore, we advise obtaining specific legal consultancy in terms of compliance with Turkish laws and regulations.

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 Protection of Personal Data Law is the main framework of data protection and privacy in Turkey. The Law entered into force on 7th April, 2016.

Fintech organisations are deemed as data controllers (defined as a legal person who demonstrated the purposes and means of processing personal data and is responsible for the establishment and administration of data filing system under the Personal Data Protection Law) should comply with the Law and will be monitored by the Personal Data Protection Authority.

Fintech organisations are obliged primarily to comply with Law in terms of notification and obtaining consent. The Law has not only monetary sanctions but also imprisonment sanctions to the data controller and/or data processor. This is a new practice area in Turkey of which significant legal consultancy of the experts is advised.

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 Protection of Personal Data Law applies to the organisations established in the territory of Turkey. There is no general restriction in the Law regarding international transfer of personal data. Nevertheless, if the data controller or processor wishes to transfer personal data outside of Turkey, explicit consent of the data subject is a requirement or for some of the exemption defined in the Law, an adequate level of protection of the relevant foreign country where the data will be sent must be provided, if explicit consent is not needed.

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

There are different types of sanctions available, including:

- Regulatory Sanctions – Personal Data Protection Authority can issue administrative fines up to 1,000,000 Turkish Liras.
- Criminal Sanctions – Turkish Criminal Code No: 5237 shall apply to offences related to personal data. The imprisonment term is defined in Turkish Criminal Code between two to six years.
- Damage Claims – The data subject has the right to apply to the data controller for damages caused by unauthorised processing.

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

There are many regulations and legislations regarding cyber security which may apply to fintech business. For example:

- The Law on Protection on Personal Data has security requirements for when personal data is processed.
- Communique on Principles to Be Considered in Information System Management in Payment Institutions and Electronic Money Institutions, also contains information security provisions, applies to the fintech businesses operating under the Law on Payment and Security Settlement Systems, Payment Services, and Electronic Money Institutions.
- According to Bank Cards and Credit Cards Law, digital banking services and fintech businesses operating under Law on Payment and Security Settlement Systems, Payment Services, and Electronic Money Institutions should comply with the security measurements set forth in this Law.

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

The main framework of anti-money laundering legislation is Law No: 5549 on Prevention of Laundering Proceeds of Crime and Turkish Criminal Code No: 5237.

Laundering of assets acquired from offence can be committed in the following ways: (i) transferring abroad the proceeds obtained from an offence requiring a minimum penalty of six months or more imprisonment, or processing such proceeds in various ways in order to conceal the illicit source of such proceeds or to giving the impression that they have been legitimately acquired; and (ii) without participating in the commitment of the offence purchasing, acquiring, possessing or using the proceeds which is the subject of that offence knowing the nature of the proceeds.

Also, in Law No: 5549, there are criminal sanctions for not-complying with the requirements set forth in such Law, for example, failure to notify a suspicious transaction.

Also, fintech businesses may be subject to fraud, bribery and corruption crimes stipulated under Turkish Criminal Law and the crimes that set forth in the Law No: 6415 on the Prevention of the Financing of Terrorism.

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

There are no specific regulations to be applied to the general fintech sector. Any relevant regulation would likely be applied to the sector in which fintech businesses operate.

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?

Turkish Labour Law No: 4857 is the main legal framework regulating the relationship between the employer and employee.

Discrimination between employees is strictly prohibited under Turkish Labour Law. No discrimination based on language, race, sex, political opinion, philosophical belief, religion or similar reasons is permitted before or during the employment relationship. Also, Turkish Labour Law prohibits outsourcing, unless, it is necessary for operational and work-related requirements or it requires expertise for technological reasons. Where the principal employer outsources some of its work to a subcontractor, then, they will be accepted as jointly liable for the obligations set forth under this Law.

Employment agreements which exceeds at least one year should be in written form.

Under two categories, dismissal of the employee is fair. The first one is the expiry of fixed-term contracts. Secondly, where the employee ends the relationship with reasonable cause. Other than two options, any actions regarding termination of the employment relationship, for example not complying with the termination procedures, will be subject to remedies. Such remedies can be severance payments, notice payments and in some circumstances, re-hire of the employee and obligation to pay up to four months of the total of his wages and idle time.

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

Employers must pay minimum wage to all employees and contribute to the state pension and health system on behalf of the employee. Also, all employees who have worked for at least one year are subject to annual leave which is determined by the employee's length of service.

Employees may not work more than 45 hours per week. This limit cannot be exceed, even if the parties agreed otherwise. Exceeding the 45-hour is deemed as an "overtime" and the maximum limit for overtime work is 270 hours in a year.

Also, employees must have rest break, up to one hour during the work day.

Pregnant employees can benefit from fully paid leave for eight weeks before the birth and eight weeks after the birth.

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 general framework of the foreign recruitment is set forth under the Law No: 6735 on International Workforce. Foreign employees must apply to the Ministry of Labour and Social Security or if they are abroad, they must apply to the embassies or consulate generals of Turkey for a work permit. A work permit will be granted by the Ministry of Labour and Social Security. There are some permit exemptions stated in the International Workforce Law, for example being a qualified engineer, and those who are subject to these exemptions face no work permit application obligation. Labour and Social Security shall grant such exemption.

6 Technology

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

Intellectual and industrial property rights are respectively protected by Law No: 5846 on Intellectual and Artistic Work and Law No: 6769 on Industrial Property Law. Most innovations and inventions are protected respectively by these Laws. There is also the Turkish Patent and Trademark Office for the registration of patents and trademarks, if the innovation or invention has a patent right or trademark.

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

Under the Law No: 5846 on Intellectual and Artistic Work, ownership of such IP will belong to first creator and will be deemed as an "author". Also, if an employee creates an IP during the employment contract, the employer is deemed as an "author" and holds the IP right of such work. The duration of the IP right is the life of the author and another 70 years' time following the death of the author.

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 above mentioned Turkish IP Law and Regulations, WIPO Treaty, Berne Convention for the Protection of Literaty and Artistic Works and The Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS") can be enforceable.

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

The author has the exclusive right to rent, lend, put up for sale or distribute any other way. According to Law No: 5846, contracts and disposals concerning economic rights shall be in writing and the subject matter shall be specified individually.

Dr. Çiğdem Ayözger
SRP-Legal
42 Maslak, A 11/11
Maslak Mah., Sarıyer
Istanbul
Turkey

Tel: *+90 212 401 4 401*
Email: *cigdem@srp-legal.com*
URL: *www.srp-legal.com*

Dr. Ayözger is the Founding Partner of SRP-Legal and has expertise in technology, media and communication (TMC), fintech, e-commerce law and, irrespective of sector, data privacy and protection and competition laws. She advises on all aspect of technology, media and communication (TMC), fintech, e-commerce laws and irrespective of sector data privacy and protection law, and as well as general corporate law and competition law. Before she established SRP-Legal, she was the Chief Legal & Strategy Officer in the leading telecommunication company in Turkey. She also provides regulatory strategy and policy services to her clients.

SRP-Legal is a boutique law firm with a focus on technology, media and communication (TMC), fintech, e-commerce laws and also, irrespective of sector, data privacy and protection and competition law. We are personally committed to our clients and are always interested in listening to their expectations and needs, seeking their views and feedback. At SRP-Legal, our target is to provide bespoke legal, regulatory, policy and strategic advice that is fit for the specific purpose of the client's requirements.

Chapter 33

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 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 is now reaching a degree of maturity. Likewise, the sharing economy and crowdfunding are well-established in the UK, but we would expect both of these areas to continue to grow.

Big Data continues to be an important area of innovation and research both for start-ups and established financial services firms. Big Data can, through the use of more powerful computers and smarter algorithms, increasingly be turned into 'meaningful data' with commercial application. We expect that this 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. One other emergent sub-category of fintech in the UK is regtech – tools and services to automate compliance tasks – and we expect that this area will continue to grow in the near future.

2016 saw significant growth in the application of fintech to asset management, in particular, the use of robo-advice, which is increasing in both sophistication and prevalence. As algorithms improve and artificial intelligence technology develops, we would expect this trend to continue.

2016 also saw much discussion of blockchain technology. Despite the excitement, however, blockchain technology is yet to make a meaningful practical impact on the UK fintech landscape. However, the broad range of possible use cases and the high level of disruption expected from the application of the technology means that blockchain innovation is one of the most important trends in UK fintech.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction?

There are no prohibitions or restrictions that are specific to fintech businesses in the UK.

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 'family, fools and friends' have been exhausted.

Equity

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, for example, raised £1 million in 96 seconds on 3 March 2016. 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 challenger banks (e.g., Silicon Valley 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 50% income tax relief for UK taxpayers investing up to £100,000 in qualifying start-ups. This complements the existing 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.
- R&D tax credits of up to 225% 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?

Worldpay, the payments processor, floated on the London Stock Exchange in 2015, valued at £4.8 billion – the UK's largest ever fintech IPO.

Other smaller, but nonetheless notable, IPOs include: (i) FreeAgent, an accounting software provider which was listed on the London Stock Exchange in November 2016. This was the first ever UK IPO for an equity crowdfunded company; and (ii) the IPO of Coinsilium on the ICAP Securities and Derivatives Exchange in London, which was the world's first IPO of a blockchain technology 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.

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.

3.2 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?

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 our replies to 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 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.

3.3 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, which would enable the firm to use an authorisation in another EU country to perform regulated activities in the UK. Although the UK voted to withdraw from the EU, the passporting regime is likely to continue to operate until the UK's eventual departure.

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?

The Data Protection Act 1998 ("DPA") is a principles based regime which regulates the processing of personal data in the UK. It implements the European Data Protection Directive (95/46/EC).

Fintech organisations established in the UK which are "data controllers" (defined as organisations which determine the purpose and manner in which of any personal data are processed) will be regulated by the DPA. Their obligations primarily relate to:

- Notification: Personal data must not normally be processed unless the data controller has an entry in the register maintained by the data protection regulator – the Information Commissioner's Office (or ICO). Notification includes a fee of £35 or £500, depending on the size/type of organisation.
- Compliance with the Principles: A data controller is under a duty to comply with eight data protection principles (for example, to process data fairly and lawfully, securely, and in accordance with the rights of the individuals who are the subject of the data).

The UK data protection regime is currently viewed as one of the more business-friendly European data protection regimes. However, the European (including UK) data protection regulatory regime is changing. From 25 May 2018, the General Data Protection Regulation will replace the DPA. It has direct effect in all EU Member States and is a more prescriptive and restrictive regime. For example, it includes mandatory breach notification provisions and high monetary sanctions, and imposes obligations not only on controllers but also on data processors (those who process on behalf of a data controller).

Note: Unsolicited direct marketing by electronic means is also covered by the Privacy and Electronic Communications Regulations 2003 (PECR), which again are based on an EU Directive. 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 DPA applies to data controllers which are not established in the UK, or EEA, but which use equipment in the UK for processing that data (other than for transit). The GDPR has a wider 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.
- The DPA and GDPR both restrict the transfer of personal data outside the EEA unless adequate protection is in place. There are various ways to obtain adequate protection, including using standard model data export clauses 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:

- Regulatory action – the ICO can issue fines of up to £500,000. It can also issue enforcement or information notices and apply to the court for a warrant to enter and search premises. Fines under the GDPR will be much higher – up to 4% of annual worldwide turnover or €20 million (whichever is greater).
- Criminal liability – the DPA includes a number of criminal offences, for example failing to notify and breaching an enforcement notice. Directors, managers and officers can (in certain circumstances) be held personally liable for offences by corporations.
- Damages claims – individuals may be entitled to compensation for damage and distress caused by unauthorised processing or other breaches of the DPA. Case law has also confirmed that misuse of private information is actionable as a common law tort.

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;
- 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; and
- the EU's NIS Directive, which must be implemented into UK law by May 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 banks and other 'operators of essential services' together with certain digital service providers.

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" must also comply with the Money Laundering Regulations 2007 (MLRs). The definition of "regulated sector" broadly will capture most institutions engaged in the provision of financial services (particularly customer-facing services). The MLRs set out detailed requirements in respect of customer due diligence and anti-money laundering policies and procedures.

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.

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 based on a statutory formula, or in limited circumstances reinstatement or re-engagement. Dismissals for certain reasons (such as childbirth or whistleblowing) are automatically unfair and, in most cases, do not require a qualifying period of employment.

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 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.

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 fairly 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. Following their return to work, most such employees have a right to return to the same job on the same terms, or in some cases a suitable alternative job.

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. If the UK exits the EU, the free movement rights of EEA and Swiss nationals may be restricted, but it is too early to predict if or how this will be achieved.

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 potential difficulties on patentability, 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 EU-wide and international registrations for certain IP rights and in some cases can obtain cross-border relief.

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. It is likely that a new unitary patent right, the Unitary Patent (UP), which will offer protection in up to 26 EU Member States, will come into force in late 2017 together with a centralised enforcement system, the Unified Patent Court, 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 Community Registered and Unregistered Designs) and under international registration systems. The EU rights are enforced in national courts which are designated Community courts and can issue pan-European relief.

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 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 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 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 *Chambers UK* as a leading individual in the area of financial services.

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, and to have been able to apply our expertise in this innovative area by supporting clients such as Euroclear, Equinix, Stripe, Aviva, Arm Holdings, Google and Vodafone on projects and transactions in the tech and fintech sectors.

USA

Reena Agrawal Sahni

Shearman & Sterling LLP

Sylvia Favretto

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 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 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 institutional and retail customers an increasing variety of services. While the U.S. fintech landscape and the regulation thereof continue to develop, 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, including 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, and insurance, utilise new technology such as distributed ledger technology (**DLT**) for bitcoin, and are provided across a variety of platforms, including mobile, 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 year, as regulators recognise the immense potential for DLT to transform the world of finance and the implications that DLT may have for market participants. 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-advisors will only continue to increase in the coming years.

Another notable trend in the fintech space over the past couple years is the increase in fintech companies partnering with traditional brick and mortar banks to provide financial services to consumers, providing mutual efficiencies that can serve to further increase consumer inclusion and access to financial technology. Banks' partnerships with, and investments in, fintech firms have allowed banks to participate in new platforms for traditional bank products.

Finally, regulators in the United States are also monitoring growths 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?

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.

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. A company can raise money for a variety of purposes – for working capital, to finance an expansion, for marketing purposes, and even as a source of capital to lend (as in the case of a lending marketplace). Funding is available from institutions and corporates, venture capital and hedge funds, private equity, mutual funds, family offices as well as high net worth individuals. The JOBS Act and the regulations promulgated thereunder have provided additional means of raising capital for businesses, including from non-accredited individuals in publicly-sourced crowdfunding transactions. Importantly, the JOBS Act allows new and growing businesses to conduct general solicitations and to access the public markets without the panoply of regulatory burdens typically associated with doing so.

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. 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 number of post-IPO shareholders, size of 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.

The JOBS Act made it possible for certain companies to conduct "mini IPOs" (capped at $20 million or $50 million per annum, based on whether a company satisfies certain criteria), and allows companies that qualify as "emerging growth companies" to conduct an IPO a bit more easily (including by avoiding certain attestation requirements under Sarbanes Oxley) than would otherwise be possible.

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, Square and BATS have all achieved IPOs. In addition, China-based fintech company Yirendai also achieved an IPO in the U.S. and China-based China Rapid Finance is expected to list on the New York Stock Exchange in late April 2017. 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 the 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.

Many fintech companies find that offering their services in 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 then have to contend with on-going compliance with state-level rules and regulations.

On 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 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-advisors, 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 December 2016 that it will provide a special purpose national bank charter to 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.

Regulators with jurisdiction over fintech businesses have not shied away from issuing enforcement actions where fintech businesses are conducting activities in violation of 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 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?

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 program, 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 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 will also hold office hours to provide increased OCC staff access to fintech market players.

- In September 2016, U.S. House Representative Patrick McHenry (R-NC) introduced a bill, titled the Financial Services Innovation Act, that endeavours to create a broad regulatory "sandbox" regime across various federal financial regulatory agencies and would establish a process whereby fintech companies could petition for regulatory relief from certain specified regulatory requirements in connection with such companies' financial innovation products. The bill would also require certain federal financial regulatory agencies to establish offices tasked with promoting financial innovation, which offices would coordinate with each other on developing fintech regulation while also working to navigate the regulatory framework with those fintech companies whose petitions for relief have been granted.

3.3 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, non-U.S. fintech companies must comply with the general licensing and regulatory framework described herein.

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 and 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.

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 any restrictions to 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 over the past year. In the Microsoft case, the Second Circuit Court of Appeals ruled in July 2016 that Microsoft does not have to provide copies of the data that is stored in Ireland to the Justice Department, whereas in the Google case a U.S. Magistrate Judge in February 2017 ordered Google to hand over the emails stored outside the country in order to comply with an FBI search warrant. Fintech companies should pay close attention to this area of law and monitor developments in regulation and enforcement as there is continuing debate whether certain laws need to be revised to reflect the changes in technology and how companies collect, use and store data.

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

Various federal agencies and state attorneys generals 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. The California State Attorney General created a "Privacy Task Force" in 2012 and has brought 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. 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 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. Further, the federal banking agencies published for comment in October 2016 an advanced notice of proposed rulemaking on enhanced cyber risk 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.

Also 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 regimes 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 anti-money laundering 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.

Further, "financial institutions" are also required to have in place under the USA PATRIOT Act customer identification programs (**CIP**) that allow such institutions to know and verify the identity of their customers. CIP requirements applicable to certain financial institutions were also recently bolstered by a FinCEN rule requiring further diligence as to beneficial owners in respect of legal entity customers.

Certain states also have in place their own anti-money laundering requirements which may apply to licensed fintech businesses within such states. Additionally, the 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 anti-money laundering programmes in compliance with such regulations to avoid enforcement by U.S. regulators who have been placing increased emphasis on anti-money laundering 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 kind 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 newborn 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 workweek. "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 this 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 practiced 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 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 programs, 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 (**USPTO**) 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.

Acknowledgment

The authors 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, David O'Steen, an associate in Shearman & Sterling's Intellectual Property Transactions Group, Alan Seem, a partner in Shearman & Sterling's Capital Markets Group, Jeewon Kim Serrato, a counsel in Shearman & Sterling's Privacy & Data Protection Group, and Chuck Thompson of Blockchain Consulting LLC, for their assistance in preparing this chapter.

Reena Agrawal Sahni
Shearman & Sterling LLP
599 Lexington Avenue, New York,
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 was shortlisted for the 2016 Euromoney Americas Women in Business Law Awards – Best in Financial Regulation. She was recognised as a "Rising Star" by *IFLR 1000* in 2016. Ms. Sahni also advises on corporate governance, OFAC and AML compliance, internal investigations and regulatory enforcement actions.

Sylvia Favretto
Shearman & Sterling LLP
401 9th Street NW
Washington D.C. 20004
USA

Tel: *+1 202 508 8176*
Email: *sylvia.favretto@gmail.com*
URL: *www.shearman.com*

Sylvia Favretto is Counsel in the Financial Institutions Advisory & Financial Regulatory Group of Shearman & Sterling. Her practice consists of providing guidance to domestic and foreign banks on U.S. financial regulatory reform and the U.S. federal banking laws, including providing advice to financial institutions with respect to Dodd-Frank implementation and compliance. Ms. Favretto has worked with various international bank and non-bank financial institutions in connection with their operations in the United States, Bank Holding Company Act compliance, and investment opportunities. Ms. Favretto was recently named a "Rising Star" in the Banking and Financial Services sector by *IFLR 1000* in 2016.

SHEARMAN & STERLING LLP

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 practise groups and offices and provide consistently superior results. Our lawyers come from some 80 countries, speak more than 60 languages and practise US, English, EU, French, German, Italian, Hong Kong, OHADA and Saudi law. We also practice 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.

Other titles in the ICLG series include:

- Alternative Investment Funds
- 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
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Franchise
- Gambling
- Insurance & Reinsurance
- International 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 Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com