mcmillan

Bulletins: Cybersecurity, Blockchain and Cryptocurrencies

Contents

July 2018

CSA Reinforces Position that Securities Laws Apply to Cryptocurrency Offerings, Confirms Regulatory Scrutiny for Industry Participants

Rajeev Dewan, Jeffrey P. Gebert, Alex Bruvels

Introduction

On June 11, 2018, the Canadian Securities Administrators (the "**CSA**") published CSA Staff Notice 46-308 – *Securities Law Implications for Offerings of Tokens* (the "**Staff Notice**") providing regulatory guidance on token and coin offerings.

The Staff Notice builds on CSA Staff Notice 46-307 – *Cryptocurrency Offerings* ("**SN 46-307**"). In SN 46-307, the CSA stated its view that cryptocurrency offerings, including initial coin offerings ("**ICO**") and initial token offerings ("**ITO**"), may involve an offering of securities and therefore may trigger prospectus or registration requirements under applicable securities laws. However, SN 46-307 did not provide much practical guidance to businesses that were contemplating completing an ICO/ITO on when such offerings would constitute the sale of securities. In particular, SN 46-307 did not directly address the concept of "utility tokens", an industry term commonly used to describe a sub-set of tokens which have one or more specific functions, such as allowing its holder to access or purchase services or assets based on blockchain technology.

The Staff Notice offers some practical guidance on two primary issues relating to crypto-offerings: (i) when an ICO/ITO may constitute an offering of securities and therefore, trigger the application of securities laws; and (ii) ICOs/ITOs structured in multiple steps.

When an ICO/ITO may involve an offering of securities

An ICO/ITO may involve the distribution of securities if: (i) it involves the offering of "investment contracts"; and/or (ii) the tokens that are offered are otherwise considered securities under the broad definition of a "security". A token may constitute an "investment contract" (and accordingly, a security) by virtue of the presence of the following elements:

- an investment of money;
- in a common enterprise;
- with an expectation of profit;
- coming significantly from the efforts of others.[1]

To determine whether an offering of tokens involves an offering of investment contracts, the CSA will focus on not only the technical characteristics of the token, but the economic realities of the offering as a whole, with focus on substance over form. The Staff Notice provides non-exhaustive examples of situations that may indicate the presence of one or more elements of an investment contract including[2]:

- tokens are not immediately delivered to purchasers: Purchasers may not be purchasing tokens because of their immediate utility but because of profit expectations. Additionally, a "common enterprise" may be present because of the purchaser's reliance on management to deliver the tokens;
- the stated purpose of the offering is to raise capital to be used to perform key actions related to supporting the value of the token, the issuer's business, or the platform's usability: These statements may indicate an expectation of profit and the presence of common enterprise;
- the issuer suggests that the tokens will be used as a currency or have utility beyond the issuer's platform but the issuer is not currently able to demonstrate the wide use or acceptance of the token: A "common enterprise" may be present because of the purchaser's reliance on management to deliver the tokens;
- the issuer's management representing expertise that will increase the token's value: These statements may indicate common enterprise via reliance on management and an expectation of profit derived from that expertise;
- a finite number of tokens: may indicate an expectation of profit as token value may rise if demand increases in relation to the fixed supply;
- tokens are sold at a value disproportionate to their purported utility: may indicate that the tokens' real value is in the expectation of profit from resale;
- marketing of the offering is targeted to persons who would not reasonably be expected to use the issuer's product, service, or app: indicating the motivation of purchase is profit and not usage of the product, service, or app;
- statements of management suggesting that the tokens will appreciate in value or comparing them to other cryptocurrencies that have increased in value: indicative of an investment thereby creating an expectation of profit. In contrast, to the extent management clearly promotes the utility of the token and not its investment value, the implication that purchasers have an expectation of profit may be reduced; and
- tokens are reasonably expected or marketed to trade on one or more cryptoasset trading platforms including decentralized or "peer-to-peer" trading platforms or to otherwise be freely tradable in the secondary market: the CSA states that to determine whether tokens are reasonably expected to be subject to secondary trading, they consider all representations made formally and informally by the issuer including through social media. Considerations are also given to representations by third parties that are endorsed by the issuer.

Offerings of tokens structured in multiple steps

The CSA also acknowledges consistent with their focus on substance over form that the occurrence of ICOs/ITOs occurring in multiple steps may trigger the applicable of securities laws. Specifically, where the offering has been structured on the following basis: (i) the purchaser agrees to contribute money in exchange for a right to receive tokens at a future date and the tokens are not delivered at the time of purchase (often completed via a "simple agreement for future tokens" or "**SAFT**"); and (ii) the token is delivered later than the time of purchase. At the time of delivery, the token issuer typically represents that the software, online platform or app is built, that services are now available or that the tokens are now functional. In relation to such offerings, the CSA states:

- the token delivered at a second or later step may be a security and will be subject to further assessment, including a consideration of the elements set out above;
- the distribution of the security is subject to prospectus or exemption requirements;
- a person or company in the business of trading securities is subject to the dealer registration requirements;
- if the distribution at the first step is made without compliance with securities law, the issuer remains in default of securities law despite the occurrence of subsequent steps; and
- the CSA has concerns where a multiple step transaction structured to attempt to avoid securities legislation.

Compliance and enforcement

Businesses should note that the CSA is conducting active surveillance of coin and token offerings and intend to continue to take enforcement action against non-compliant businesses. To ensure regulatory compliance, the CSA encourages businesses with proposed ICOs/ITOs to consult legal counsel and to contact their local securities regulatory authority to discuss their project. Finally, the CSA promotes the "Regulatory Sandbox", its initiative supporting fintech businesses seeking to offer innovative products, services, and apps by allowing firms to register and/or obtain exemptive relief from securities laws under a faster and more flexible process than the standard application. Applications are analyzed on a case by case basis. A list of firms that have been authorized in the CSA Regulatory Sandbox is available on the CSA website.

Conclusion

The Staff Notice makes it clear that utility tokens may constitute "investment contracts" depending on the economic realities of the offering as a whole. Accordingly, businesses should complete a meaningful analysis of any proposed ICO/ITO to ensure that the business goals of such offering are achieved in compliance with applicable securities laws.

Please contact a member of McMillan's Capital Markets Group if you have any questions, are seeking assistance with an ICO/ITO, or wish to seek exemptive relief in relation to an offering via the CSA Regulatory Sandbox.

by Raj Dewan, Jeffrey Gebert, Alex Bruvels and Joseph Osborne, Student at Law

[1] See, for example: *Pacific Coast Coin Exchange v. Ontario (Securities Commission)*, [1978] 2 SCR 112.

[2] Refer to the Staff Notice for the complete list of situations outlined by the CSA that may be indicative of the existence of one or more elements of an investment contract and associated implications.

a cautionary note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.

May 2018

PIPEDA's Breach Reporting Requirements Finalized, to Come Into Force November 1, 2018

Lyndsay A. Wasser, Mitch Koczerginski

Through an Order in Council, the federal government has announced that certain sections of the *Digital Privacy Act*("**DPA**") that amend the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") will come into force on November 1, 2018. The Breach of Security Safeguards Regulations (the "**Regulations**") will also come into force on the same day.

The new notice obligation will require organizations to report a breach of security safeguards involving personal information where it is reasonable in the circumstances to believe that the breach creates a "real risk of significant harm"[1] to affected individuals. A "breach of security safeguards" is defined as a loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards or from a failure to establish those safeguards.

This update provides an overview of the breach reporting requirements.

The Objectives of the Breach Reporting Obligations

The breach reporting obligations are designed to: (1) ensure that all Canadians receive the same information about data breaches that pose a risk of significant harm to them; (2) ensure that notifications of data breaches contain enough information to permit individuals to understand the significance and potential impact of the breach; (3) ensure that the Commissioner receives consistent and comparable information about breaches; and (4) ensure that the Commissioner can provide meaningful and effective oversight and verify that organizations are complying with their notification requirements.

Reporting to the Commissioner

The form and content of required notice is set out in the Regulations. Where an organization determines that a breach meets the requisite standard for notice, it will be required to deliver a written report to the Commissioner that, at a minimum, includes:

- a description of the circumstances of the breach and, if known, the cause;
- the day on which, or period during which, the breach occurred;

- a description of the personal information that is the subject of the breach;
- an estimate of the number of individuals in respect of whom the breach creates a real risk of significant harm;
- a description of the steps that the organization has taken to reduce the risk of harm to the affected individual resulting from the breach or to mitigate that harm;
- a description of the steps that the organization has taken or intends to take to notify each affected individual of the breach in accordance with PIPEDA; and
- the name and contact information of a person who can answer on behalf of the organization, the Commissioner's questions about the breach.

Notably, the Regulations do not require organizations to include an assessment of the potential harm likely to be caused, which is required when providing notice to the Information and Privacy Commissioner of Alberta under Alberta's Personal Information Protection Act.

Notifying Affected Individuals

Under the Regulations, where an organization determines that it is reasonable in the circumstances to believe that a breach involving personal information is likely to cause a "real risk of significant harm", it is required to deliver a notice to affected individuals that, at a minimum, includes:

- a description of the circumstances of the breach;
- the day on which, or period during which, the breach occurred;
- a description of the personal information that is the subject of the breach;
- a description of the steps that the organization has taken to reduce the risk of harm to the affected individual resulting from the breach or to mitigate that harm;
- a description of the steps that the individual could take to reduce the risk of harm resulting from the breach or to mitigate that harm;
- a toll-free number or email address that the affected individual can use to obtain further information about the breach; and
- information about the organization's internal complaint process and about the affected individual's right, under the PIPEDA to file a complaint with the Commissioner.

The Regulations require that notice be made directly to each individual via email, letter, telephone, or in person, unless: (1) the cost of doing so is prohibitive; (2) direct notification may cause further harm to the individual; or (3) the organization does not have contact information for the affected individual or the information it has is out of date. In such circumstances, the Regulations permit indirect notification through public announcements or advertising.

Notifying Other Organizations

Under the DPA, organizations may also be required to notify other organizations, a government institution or a part of a government institution of the breach, if the notifying organization believes that doing so may reduce the risk of harm that could result or mitigate that harm. The Regulations do not contain any requirements as to the content of notice to other organizations.

Record-Keeping

The Regulations impose record-keeping requirements on organizations with respect to any breach of security safeguards impacting personal information – whether or not a breach is likely to cause a real risk of significant harm to affected individuals.

Organizations must keep records of every breach of security safeguards for 24 months from the date the organization determines that the breach has occurred. The record of the breach must contain sufficient information to permit the Commissioner to verify whether the organization is complying with PIPEDA.

Impact

The amendments and detailed breach reporting obligations that are set out in the Regulations largely reflect previously articulated "best practices" established by the Office of the Privacy Commissioner for Ontario and existing statutory requirements in Alberta. Once in force, these requirements will bring Canada more closely in line with the General Data Protection Regulation – i.e., the European privacy requirements set to come into force on May 25, 2018. Equivalency in privacy protection allows for the free flow of personal information from EU to Canadian organizations.

In light of these new legal requirements, organizations should ensure that:

1. all staff are trained to recognize and report any actual or potential data breach;
2. they have developed and tested their breach response plan; and
3. they maintains records of each data breach involving personal information under their control.

One of the objectives of the notice requirements is to allow the Commissioner to provide better oversight. Accordingly, data breach records will be compellable by the Commissioner to verify compliance.

Knowingly failing to report to the Commissioner, notify affected individuals, or maintain records could attract a fine of up to $100,000.

The determination of whether it is reasonable in the circumstances to believe that a breach involving personal information is likely to cause a "real risk of significant harm" is not always straightforward. Organizations that experience a breach of their security safeguards are encouraged to contact privacy professionals immediately to determine whether a particular breach requires notification and to avoid incurring significant penalties for non-compliance.

by Lyndsay Wasser and Mitch Koczerginski

[1] Defined to include "bodily harm, humiliation, damage to reputation or relationships, loss of employment or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property."

a cautionary note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.

November 2017

OSC Grants Exemptive Relief to Token Funder Inc.

Rajeev Dewan, Kosta Kostic, Valenteena Samra

Not long after Quebec-based Impak Finance Inc. completed Canada's first legally sanctioned initial coin offering ("**ICO**"), the Ontario Securities Commission (the "**OSC**") has granted exemptive relief to Toronto-based Token Funder Inc. ("Funder") to conduct Ontario's first regulated ICO or initial token offering (an "**ITO**"). In particular, the OSC has granted regulatory relief to Funder which will exempt Funder from the dealer registration requirements, and allow Funder to carry out an ICO/ITO under existing prospectus exemptions. The impact of this decision is that it provides early stage companies and other high growth companies with the ability to raise capital through an ICO/ITO, which has emerged as a novel fundraising mechanism in the last year, on the basis that such an offering of coins or tokens are treated as securities. The decision also confirms the sentiments of the CSA Staff Notice 46-307 – Cryptocurrency Offerings where the CSA stated that "many" of the digital coins or tokens investigated by regulators in Canada fall under the definition of a security; thereby triggering a range of requirements under applicable securities laws.

Background

The Canadian Securities Administrators recently launched a regulatory sandbox (the "**CSA Sandbox**") to support financial technology businesses seeking to offer innovative products, services and applications in Canada. The CSA Sandbox allows businesses to register and/or obtain exemptive relief from securities requirements, under a faster and more streamlined process than through a standard application.

In the context of the CSA Sandbox, Funder applied for and obtained exemptive relief from the OSC pursuant to National Policy 11-203 – *Process for Exemptive Relief Applications in Multiple Jurisdictions* from the dealer registration requirement (the "Registration Relief"). In reliance on Multilateral Instrument 11-102 – Passport System, the OSC's decision is intended to be relied upon in all of the provinces and territories of Canada.

Token Funder Inc.

Funder is a blockchain business that was established for the purpose of creating a platform (the "**Platform**") to, amongst other things, (i) provide token and coin management and governance services for issuers, (ii) provide for certain transferability of tokens and coins (subject to regulatory approvals) and (iii) to operate as a capital raising platform for third-party issuers through the offering of blockchain-based securities in accordance with National Instrument 45-106 – *Prospectus Exemptions* ("**NI 45-106**") or as a crowdfunding portal pursuant to Multilateral Instrument 45-108 – *Crowdfunding*.

The Offering

To fund the creation of the Platform and its ongoing working capital needs, Funder proposed to complete a private placement by way of an ITO (the "**Private Placement**") pursuant to the offering memorandum prospectus exemption set out in section 2.9 of NI 45-106. Funder will create 1,000,000,000 digital tokens through a

smart contract on the Ethereum Blockchain (each a "**FNDR Token**"). Pursuant to the Private Placement, Funder will distribute up to 200,000,000 of the 1,000,000,000 FNDR Tokens for total gross proceeds of up to CAD $10,000,000.

Each subscriber under the Private Placement will subscribe for FNDR Tokens through a smart contract using the Ethereum Blockchain. Subscribers may provide consideration for the FNDR Tokens in the form of Ether or Canadian dollars. Funder will conduct know-your-client and suitability reviews for each subscriber, and will also conduct a survey to ensure that subscribers have sufficient understanding of cryptocurrencies and ICOs/ITOs. The suitability analysis conducted by Funder will result in a limit assigned to the investment amount in the smart contract. Unless the subscriber proves otherwise, Funder will assume that the subscriber is not an "eligible investor" or an "accredited investor" and a maximum investment amount of CAD $2,500 will be imposed.

Following the Private Placement, holders of FNDR Tokens will share in distributions from Funder arising from operations of the Platform. Further, the holder of FNDR Tokens will receive all disclosure required pursuant to NI 45-106 and other applicable securities laws.

The OSC Decision

The OSC granted the Registration Relief on the basis that:

1. Funder will seek to become a registrant promptly after the completion of the Private Placement pursuant to National Instrument 31-103 – Registration Requirements, Exemptions and Ongoing Registrant Obligations;
2. Funder will not facilitate any further capital raising efforts through the Platform before becoming a registrant;
3. the Registration Relief is only sought for a limited period of time;
4. Funder will provide full and complete disclosure to investors through its offering memorandum; and
5. Funder will conduct know-your-client and suitability reviews.

The Registration Relief was granted for a twelve month period from the date of the OSC's decision provided that the following conditions are met:

1. Funder will comply with the terms and conditions of the OSC's decision;
2. Funder will conduct know-your-client and suitability reviews for each subscriber and verify subscribers that represent themselves as "eligible investors" or "accredited investors";
3. FNDR Tokens will not be listed and traded on any exchange unless the listing and trading complies with applicable securities laws and is approved by the OSC in advance;
4. Funder will deal fairly, honestly and in good faith with its investors;
5. Funder will establish and apply policies to manage the risks associated with its business;
6. Funder will not provide investment advice to investors; and
7. Funder will report to the OSC quarterly and provide the OSC with details of any investor complaints in a timely manner.

Conclusion

Although the securities regulators have encouraged innovative business and capital-raising models through the creation of the CSA Sandbox, there remain significant hurdles to achieve regulatory approval for ICOs/ITOs in Canada. Although the OSC's decision indicates a growing level of acceptance of platforms for raising capital through the use of digital currencies, it was largely based on the specific facts and circumstances of Funder's application and its conclusion that the ITO was subject to applicable securities law. In addition, the OSC's decision does leave open the question as to how the OSC will treat the offering of coins or tokens which are multi-dimensional, and which are appropriately structured to provide investors with rights which should not meet the definition of a security, often referred to as "utility tokens".

by Raj Dewan, Kosta Kostic, Valenteena Suvaminathan and Brent Thomas, Articling Student

a cautionary note

October 2017

Divergent Regulatory Approaches to Cryptocurrency Offerings: Developments in Canada, the United States, and China

Cory Kent, Sasa Jarvis

Cryptocurrency is a digital currency that utilizes cryptography for security, and is used as a medium of exchange between parties. One of the most well known cryptocurrencies is Bitcoin, though there are a significant number of such currencies available for purchase and sale. The currency itself is represented by virtual 'coins' or 'tokens'.

The issuance of cryptocurrency has become more common as a capital raising mechanism, which has caused considerable attention to be paid to cryptocurrency offerings by both the investing public and the governmental authorities responsible for securities regulation in various jurisdictions around the word. This bulletin considers the statements made by such regulators as they adopt their respective mechanisms for dealing with cryptocurrency as a new investment vehicle.

The Canadian Approach

The Canadian approach to cryptocurrency offerings appears to be to apply the current regulatory system for securities to the offerings, once the test for a security has been met on the basis of the individual set of facts related to the type of cryptocurrency and the offering itself.

On August 24, 2017, the Canadian Securities Administrators ("CSA") released CSA Staff Notice 46-307 *Cryptocurrency Offerings* (the "Notice"), pursuant to which the CSA provided guidance for issuers seeking to raise capital through the sale of cryptocurrency. The staff notice was published in all jurisdictions except Saskatchewan, and it is expected that the Financial and Consumer Affairs Authority of Saskatchewan will advise of its approach to cryptocurrency after September 7, 2017.

Offering Cryptocurrencies

The primary analysis related to offerings of cryptocurrency relate to whether such currency is an investment contract under Canadian law, which is a type of security. Specifically, the test for investment contracts in Canada rests in the decision of the Supreme Court of Canada in *Pacific Coast Coin Exchange v. Ontario (Securities Commission)*[1]. To be an investment contract, the offering must involve an investment of money in a common enterprise with the expectation of profit to come significantly from the efforts of others.

If the sale of cryptocurrency constitutes an investment contract in accordance with the test outlined in *Pacific Coin*, then the requirement to distribute such securities under a prospectus or under an exemption from prospectus requirements applies. Further, issuers who distribute coins or tokens in connection with such an offering may be trading in securities for a business purpose, requiring dealer registration or an exemption from such dealer registration requirements.

Cryptocurrency Exchanges

The exchanges upon which cryptocurrency can be bought and sold often operate without oversight or regulation, and can be found around the world. The CSA warns that coins or tokens that constitute securities being issued to trade on such cryptocurrency exchanges could result in the issuer violating restrictions on secondary training pursuant to National Instrument 45-102 Resale of Securities.

The U.S. Approach

The United States appears to be independently adopting a similar approach as to Canada's, in that the current regulatory system for securities is starting to recognize cryptocurrency as potentially being a security, and therefore already being subject to a comprehensive set of requirements related to registration, disclosure, and similar matters.

While the U.S. Securities and Exchange Commission (the "SEC") has not come out with a comprehensive bulletin in the way the CSA had regarding the specific test for determining whether a cryptocurrency was a security, the SEC has published a bulletin meant to act as guidance for investors as well as a Report of Investigation under Section 21(a) of the Securities Exchange Act of 1934, related to an investigation conducted of The DAO, an entity which began offering and selling their own tokens (the "DAO Tokens") to raise capital.

In past publications issued by the SEC, a major theme related to cryptocurrency has been the warning of investors of potential fraud perpetrated through the use of Bitcoin and other virtual currencies. The SEC indicated that it has a concern that the rise of virtual currencies is allowing fraudsters to facilitate Ponzi and other schemes, or engage in fabricated investments or transactions, specifically noting a recent case it prosecuted in which an alleged Ponzi scheme was advertised as a Bitcoin "investment opportunity"[2]. The SEC has taken enforcement action against such schemes, and issued several investor alerts over the past number of years.

More recently, the analysis provided by the SEC appears to contemplate the treatment of coins or tokens sold pursuant to Initial Coin Offerings or Initial Token Offerings as a security[3]. Among other items, the most recent investor bulletin related to Initial Coin Offerings outlines that the offer and sale of such coins may need to be registered with the SEC or be performed pursuant to an exemption, and further that investment professionals and the firms that transact, offer, or advise on investments of cryptocurrency, may be required to be licensed or registered, if such cryptocurrency constitutes a security[4].

The SEC's investigation of the DAO provides a valuable case study in how the SEC approaches the issue of cryptocurrency offerings within its regulatory system.

The DAO Investigation

The DAO was created as a for-profit entity that creates and holds assets through the sale of DAO Tokens to investors, and those assets would then be used to fund the projects undertaken by DAO. The holders of the DAO Tokens were anticipated to receive earnings from the projects, and had the right to vote on those projects on the basis of their DAO Token holdings. Further, the holders of DAO Tokens could sell their DAO Tokens on various online platforms that supported this trading. The DAO Tokens were sold to investors in exchange for approximately 12 million Ether, which is another virtual currency used on the Ethereum blockchain, which the SEC indicated had a value of approximately US$150 million.

Similarly to the approach taken by the CSA, the SEC had sought to establish whether the DAO Tokens were a security on the basis of whether they could be characterized as an investment contract[5]. The test for investment contracts in the United States was adopted by the U.S. Supreme Court in SEC v WJ Howey Co.[6], which was considered by the Supreme Court of Canada in Pacific Coin, leading to the two tests being very similar. The test articulated in Howey is the investment of money in a common enterprise with a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others.

Ultimately, the SEC found that the test articulated above was satisfied. The concept of money does not need to be cash, and the SEC determined that the sale of DAO Tokens for Ether met the first stage of the test, namely that an investment was made. The SEC's analysis further included investors who were purchasing the DAO tokens were investing in a common enterprise and they expected to earn profits from that enterprise, which could include both dividends or other periodic payments and also an increase in the value of their investment. This profit was further to be derived from the managerial efforts of others, including those who managed the DAO and put forward project proposals that could generate profits for the DAO's investors. Additional evidence of reliance that was specifically mentioned by the SEC was the marketing efforts put forward by the managers of the DAO, and specifically with how they held themselves out to be experts in Ethereum, which was the blockchain protocol upon which the DAO operated. The persons who selected the projects that would be voted on were held out to investors to be experts in the area, which further indicated to the SEC that DAO Token holders were acting in reliance on such persons. Finally, the SEC found that the limited voting rights afforded to the DAO Token holders were not enough to vitiate the reliance on third parties. The DAO was therefore obligated to register the offer and sale of the DAO Tokens under the Securities Act of 1933, unless a valid exemption applied.

The Chinese Approach

On September 4, 2017, reports emerged that China was banning the practice of capital raising through the sale of cryptocurrency. China in particular has been a jurisdiction in which a significant number of Initial Coin Offerings have been conducted, particularly recently, as data emerging from a government organization that monitors such activity stated that between January and July of 2017, there had been 65 Initial Coin Offerings raising a combined 2.62 billion yuan (estimated to be approximately US$394.6 million) from 105,000 individuals[7]. Some reports drew conclusions related to the fall of value of Bitcoin and Ethereum, two of the most popular cryptocurrencies available, after the news of China's ban emerged[8].

Comparison of Regulatory Approaches

Each of the SEC and the CSA did not categorize all cryptocurrency as being a security, but rather outlined the tests that apply to the determination of whether something is a security, and specifically whether it is an investment contract. The SEC specifically stated in the DAO investigation report "[w]hether or not a particular transaction involves the offer and sale of a security – regardless of the terminology used – will depend on the facts and circumstances, including the economic realities of the transaction.[9]" The result of such an approach is that there could be cryptocurrencies that on the facts may not be considered a security, and so the regulatory system in place would presumably not apply, however the exact set of facts that would need to exist to eliminate one or more of the factors in the Howey test or the Pacific Coin test is not readily apparent at this time.

China has taken a different approach, opting not to allow investors to engage with cryptocurrency. It is uncertain whether such restrictions will prove to be permanent or will be loosened over time, however there is significant disparity with this approach in comparison to that adopted by Canada and the United States, which does serve to impact the global community of investors in cryptrocurrency as well as the issuers offering such virtual currency.

South Korea initially appeared to be taking a different approach from China, as reports emerged that it will seek to strengthen regulations related to the offer, sale, and trade of virtual currencies, and will punish Initial Coin Offerings conducted in violation of the capital markets legislation in the jurisdiction. The regulations were anticipated to be in the form of strengthening user authentication procedures and banks' suspicious transactions reports, monitoring overseas transactions of service providers who use digital currencies to transfer money, and introducing new regulations related to domestic trading of virtual currencies[10]. In September 2017, the Financial Services Commission in South Korea released a statement that ICOs were banned as a fundraising tool, and that penalties would be issued on financial institutions or any other parties involved in issuing cryptocurrency through an ICO[11].

Conclusion

At present, there is no unified global approach to the regulation of cryptocurrency, and while some of the jurisdictions such as Canada and the United States may have minor differentiations in their approaches, other jurisdictions such as China can significantly diverge. As each jurisdiction decides on its approach, it is clear that governments and regulatory authorities are aware of the growing popularity and use of cryptocurrency as a capital raising mechanism, and that such attention by the authorities will mean enforcement of regulation and at times perhaps even the introduction of new regulations that issuers, investors, and virtual currency exchanges, will have to contend with.

by Cory Kent and Sasa Pudar

[1] [1978] 2 SCR 112, [1977] 2 ACWS 1063 (SCC) [Pacific Coin].

[2] US, US Securities and Exchange Commission, Investor Alert: Ponzi Schemes Using Virtual Currencies (Sec Pub No 153-7/3) (July 23, 2013), online: <https://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf>.

[3] US, US Securities and Exchange Commission, Investor Bulletin: Initial Coin Offerings (July 25, 2017), online: <https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings>.

[4] Ibid.

[5] US, US Securities and Exchange Commission, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO (Release No 81207) (July 25, 2017) at 11, online: <https://www.sec.gov/litigation/investreport/34-81207.pdf> [DAO Investigation].

[6] 328 US 293 (1946) [Howey].

[7] John Ruwitch & Jemima Kelly, "China hits booming cryptocurrency market with coin fundraising ban" (September 4, 2017), Reuters, online: <https://www.reuters.com/article/us-china-finance-digital/china-hits-booming-cryptocurrency-market-with-coin-fundraising-ban-idUSKCN1BF0R7>.

[8] "China just banned initial coin offerings, calling them illegal fundraising" (September 4, 2017), Business Insider, online: <http://www.businessinsider.com/r-china-bans-initial-coin-offerings-as-illegal-fundraising-2017-9>.

[9] DAO Investigation supra note 5 at 17-18.

[10] Yoon Yung Sil, "Regulating Bitcoin Trading: Financial Authorities to Strengthen Regulations on Digital Currency Trading" (September 4, 2017), Business Korea, online: <http://www.businesskorea.co.kr/english/news/money/19180-regulating-bitcoin-trading-financial-authorities-strengthen-regulations-digital>.

[11] "South Korea bans all new cryptocurrency sales" (September 28, 2017), CNBC, online: < https://www.cnbc.com/2017/09/28/south-korea-bans-all-new-cryptocurrency-sales.html>.

a cautionary note

September 2017

McMillan Advises on First Initial Coin Offering Granted Exemptive Relief by Canadian Securities Regulators

Kosta Kostic, Cory Kent, Sandra Zhao, Sasa Jarvis, Valenteena Samra

McMillan recently advised Impak Finance Inc. ("**Impak**") on the first initial coin offering ("**ICO**") to be granted exemptive relief, on August 15, 2017 by the Autorité des Marchés Financiers (the "**AMF**"). Similar in some ways to an initial public offering ("**IPO**"), ICOs are being used by financial technology ("**fintech**") businesses to issue cryptocurrency and raise funds for various purposes. On August 24, 2017, the Canadian Securities Administrators (the "**CSA**") published *CSA Staff Notice 46-307 – Cryptocurrency Offerings* (the "**Staff Notice**") to provide guidance on the applicability of securities laws to ICOs. The Staff Notice states that securities laws will apply to an ICO if it is an offering of a "security".[1] The Staff Notice was published in all jurisdictions of Canada except Saskatchewan. It is expected that the Financial and Consumer Affairs Authority of Saskatchewan will advise of its approach to cryptocurrency after September 7, 2017.

Background

What is a cryptocurrency?

A "cryptocurrency" is a digital currency that is exchanged electronically. The cryptocurrency itself is represented by virtual 'coins' or 'tokens'. Unlike fiat currency which is issued by a government body, cryptocurrency is not issued by a central authority. At a basic level, cryptocurrencies are just entries on a distributed ledger with account numbers and balances (known as a "**blockchain**"). All transactions are recorded on the blockchain. There is no central authority keeping track of the blockchain – it is decentralized. Any user can keep track of the blockchain. To this end, the integrity of the blockchain is upheld by virtue of the many users keeping track of the same blockchain.

When users exchange cryptocurrency, a sender will send out a transaction message to the entire peer-to-peer network of computers (known as "**nodes**") including: (1) the sender's account number, (2) the recipient's account number and (3) the amount of cryptocurrency exchanged. As new transactions are created, the transactions go into a pool of pending transactions waiting to be verified by a node (known as a "**miner**"). Miners select a set of transactions (known as a "**block**") from the pool and compete to add the transactions to the blockchain.

The miners will validate the transaction message to determine that the request is authentic and that the sender's account holds a sufficient amount of cryptocurrency to satisfy the transfer. Every account number is associated with a 'private key' (only known to the account holder) and 'public key' available to all the nodes. The private key is used to create the 'digital signature' by encrypting the transaction message. The miners test the digital signature using the associated public key and try to decrypt it. If successfully decrypted, this proves that the digital signature was created by the true account holder.

Miners compete to solve a complex mathematical problem known as a 'hash function'. The hash function is extraordinarily special in that there is no trick to solving it faster, other than by increasing computing power. The first miner to solve the hash function gets to add their block of transactions to the end of the blockchain and all other miners update to this new version of the blockchain. The transaction is settled once it is added to the blockchain. Thereafter, a new hash function is created and the process repeats.

Miners incur great costs to build computers to solve the hash functions. The miners are incentivized to do this because every time a miner adds a new block of transactions to the blockchain, the miner is rewarded with a certain number of newly-issued cryptocurrencies.

What is an ICO?

Similar to an IPO, an ICO or initial token offering ("**ITO**") is a means by which fintech businesses raise funds for a new cryptocurrency venture. In an ICO or ITO, an investor exchanges fiat currency or another type of cryptocurrency for coins or tokens issued by the company. These coins or tokens can have different functions. For example, Impak released a new digital currency is to be used in the Impak's own platform, impak.eco. Investors then use the coins to participate in the impact economy, and donate to projects that have a positive impact on society.

Cryptocurrencies and CSA Staff Notice 46-307

The legislative scheme used by securities regulators in Canada is a 'catch-then-exclude' mechanism whereby a security is defined broadly to catch all transactions and then exemptions carve-out situations where regulation is not justified. Cryptocurrencies may be characterized as an 'investment contract' and thus may be caught within the definition of a security.

The CSA published the Staff Notice on August 24, 2017 addressing ICOs/ITOs. While there are technical differences between coins and tokens for the purposes of the Staff Notice, coins and tokens are treated similarly, as the analysis focused on the triggering of securities laws in Canada. The Staff Notice encouraged ICOs/ITOs but raised investor protection concerns due to issues around volatility, transparency and the potential for cryptocurrencies to be used in unethical practices or illegal schemes.

The Staff Notice states that ICOs/ITOs are similar to IPOs in many ways. The coins/tokens can be analogized to shares of a company because the value of a coin/token may increase or decrease depending on the success of the business conducting the ICO/ITO.

The Test

In determining whether or not an 'investment contract' exists, the Staff Notice advised that businesses should apply the following four-prong test from the decision of the Supreme Court of Canada in *Pacific Coast Coin Exchange v. Ontario (Securities Commission)*[2] to determine whether the ICO/ITO involves:

1. an investment of money
2. in a common enterprise
3. with the expectation of profit
4. to come significantly from the efforts of others?

The Staff Notice stated that, in many cases, when the totality of the offering or business is considered, cryptocurrencies should properly be considered securities. However, the Staff Notice stated that every ICO/ITO is unique and must be assessed on its own characteristics.

If a cryptocurrency offering is considered an offering of securities, the business conducting the offering will need to meet the prospectus, registration and/or market place requirements.

Prospectus

To date, no business has used a prospectus to complete an ICO/ITO in Canada. The CSA anticipates that businesses looking to sell cryptocurrencies may do so under prospectus exemptions such as the 'accredited investor' exemption or the 'offering memorandum' exemption.

The CSA is aware that some fintech businesses publish 'whitepapers' with respect to their ICOs/ITOs. Although whitepapers are a form of disclosure document for investors, they often do not meet the specific disclosure requirements to be properly considered a prospectus/offering memorandum. It is important to note that investors can sue for misrepresentation in the prospectus/offering memorandum and investors may have civil remedies against fintech businesses failing to comply with the securities laws.

Registration

Businesses completing ICOs/ITOs may be trading in securities for a business purpose (the "**business trigger**"), which would therefore require dealer registrations. Fintech businesses that meet the business trigger must meet certain obligations to investors, including the know-your-client requirement ("**KYC**") and the suitability requirement. These obligations may require businesses conducting ICOs/ITOs to collect information regarding an investor's identity, investment objectives and risk tolerance. The Staff Notice acknowledged that it is possible to fulfill the KYC and suitability obligations through an automated online process.

Marketplace

The exchanges upon which cryptocurrency can be bought and sold often operate without oversight or regulation, and can be found around the world. A cryptocurrency exchange that offers cryptocurrencies that are securities must determine whether it is a marketplace. If the exchange is doing business in a jurisdiction in Canada, it must apply to that jurisdiction's securities regulatory authority for recognition or an exemption from recognition.

The Staff Notice states that fintech businesses should seek legal and/or other professional advice to assess whether or not securities laws apply to avoid placing the ICO/ITO offside securities laws. For example, coins or tokens that constitute securities being used to trade on cryptocurrency exchanges could result in the issuer violating restrictions on secondary trading pursuant National Instrument 45-102 *Resale of Securities*.

Cryptocurrency Investment Funds

The CSA is also aware of 'investment funds' as defined under securities laws being set up to invest in cryptocurrencies. The Staff Notice encouraged fintech business looking to establish cryptocurrency investment funds to consider the following:

1. prospectus requirements, as well as investment fund rules and the suitability of the investment,
2. due diligence on any cryptocurrency exchange that the investment fund uses to purchase or sell cryptocurrencies, specifically looking at the policies and procedures around identity verification, anti-money laundering, counter-terrorist financing and recordkeeping,
3. appropriate registration requirements,
4. valuation methods used to value the cryptocurrencies in the investment fund's portfolio, and
5. expertise of custodians holding portfolio assets to ensure expertise are relevant to holding cryptocurrencies.

With respect to the expertise of custodians, the CSA provided guidance in the form of a non-exhaustive list of items as to what expertise may be required of custodians dealing with cryptocurrency, including experience with hot and cold storage, experience with security measures to protect the cryptocurrency from theft, and the ability to segregate cryptocurrency from other holdings as needed.

CSA Sandbox

The recently launched CSA Sandbox is an initiative to support fintech businesses seeking to offer innovative products, services and applications in Canada. The CSA Sandbox allows businesses to register and/or obtain exemptive relief from securities requirements, under a faster and more streamlined process than through a standard application.

Conclusions from the Staff Notice

While acknowledging the emergency of a new mechanism for capital raising, the Staff Notice provided issuers of cryptocurrency with a warning that their activities may violate prospectus requirements, registration requirements, and the general disclosure requirements that were created to protect investors in capital markets. While regulation of cryptocurrency remains in its infancy, increased scrutiny of transactions involving the issuance of virtual coins or tokens is expected to ultimately bridge a regulatory scheme for such cryptocurrency in line with securities requirements.

The Impak ICO

McMillan recently acted for Impak in its CSA Sandbox application for exemptive relief with respect to Impak's ICO. Pursuant to its ICO, Impak proposes to issue a new digital currency (known as "**MPK**") to fund the development of an online social network by way of a private placement in reliance on the offering memorandum exemption.

In consultation with the other members of the CSA Sandbox, the AMF granted Impak exemptive relief from the dealer registration and prospectus requirements in connection with proposed MPK ICO. The AMF stated that, in the absence of a prospectus relief, the first trade of MPK will be a distribution.

The AMF granted the registration relief under the following conditions:

- Impak will conduct KYC and suitability reviews and verify accredited investors,
- Impak will not provide investment advice to investors,
- Impak will deal fairly, honestly and in good faith with its investors, and
- Impak will establish procedures to manage the risks associated with its business.

The AMF stated that the prospectus requirement will apply to a first trade in MPK, unless the first trade is made between an Impak user and an impact organization (i.e., businesses, non-governmental organizations, not-for-

profit corporations and social enterprises) in either of the following cases:

(i) an Impak user pays in MPK for goods and services offered by an impact organization, or
(ii) an impact organization rewards the Impak user for such purchase.

The AMF also imposed the following conditions:

- Impak will make certain quarterly information reasonably available to participants,
- MPK issued in the ICO will not be listed and traded on any exchange, and
- Impak will provide the AMF with any report or information that may be requested.

In addition to the Provinces of Quebec and Ontario, and in reliance on *Regulation 11-102 respecting Passport System*, the AMF's decision is intended to be relied upon in British Columbia, Alberta, Saskatchewan, Manitoba, New Brunswick, and Nova Scotia. The AMF's decision document has been published as of August 15, 2017, and can be under the following link: Impak Finance Inc.

by Kosta Kostic, Cory Kent, Sandra Zhao, Sasa Padur, Valenteena Suvaminathan and Simon Paransky, Summer Law Student

[1] Securities Act, RSO 1990, c S.5, s 1.

[2] (1977), [1978] 2 SCR 112, 80 DLR (3d) 529.

a cautionary note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.

July 2016

Fintech at the Crossroads: Regulating the Revolution

Pat Forgione, Robert M. Scavone, Robert M. Scavone, Tayleigh Armstrong, Kelly Kan, Student-at-Law

Financial technology or "FinTech" – using information and communications technology to better deliver financial services – has undergone explosive growth in recent years. Technology spending by the Canadian financial sector is estimated to reach Cdn$14.8 billion by 2018.[1] FinTech itself is nothing new, of course: from ATMs to online banking, financial institutions have been using technology to deliver services to end users for over 30 years. But what is new is the entry into the market place of the "disruptors" – both new technologies and new players – that promise to deliver a new user experience, especially to the younger demographic that grew up on smartphones and tablets.

FinTech is incredibly diverse and does not have clearly defined boundaries. It can include everything from conventional online banking to big data, peer-to-peer or marketplace lending, mobile payments, digital wallets, crowdfunding, robo-advice and applications of distributed ledger/blockchain technology. FinTech is both responding to and creating a demand for more efficient business models and a seamless user experience that may bypass traditional trusted intermediaries. Financial services once offered exclusively by bricks-and-mortar financial institutions are now being unbundled by emergent start-ups, and the traditional players are scrambling to maintain market share either alone or in partnership with dedicated FinTech firms. Both groups are using new technologies to deliver innovative financial services products directly to consumers.

As with many disruptors that encroach on areas once reserved for highly regulated industries (think Uber and airbnb) , FinTech poses many challenges to regulators struggling to strike the right balance between protecting end users and fostering innovation. The established players may argue that the new kids on the block aren't constrained by the same rules as the incumbents and may lobby regulators to level the playing field by imposing uniform regulation across the board. The new entrants may respond that regulatory compliance is costly and that too much regulation imposes unreasonable barriers to entry that protect vested interests and oligopolies and stifle competition and innovation. How much regulation is too much or too little?

In the coming years, we expect to hear heated debates around whether and how FinTech should be regulated and in particular how best to draft legislation that helps level the regulatory playing field without discouraging innovation and helps foster that innovation without sacrificing the safety and security of end users.

Issues in Regulation

One of the recurrent complaints from incumbents in this space is that FinTech start-ups are subject to less onerous regulation than traditional financial institutions, allowing the new entrants to employ faster go-to-market strategies and reach more customers. Federally regulated financial institutions, for example, must maintain minimum levels of regulatory capital and abide by a host of detailed prudential regulations that protect depositors and borrowers while FinTech start-ups face few of those constraints. The starting point for regulation is often the type of entity that provides a service rather than the service itself, meaning that two businesses offering similar services may be subject to widely different regulatory regimes. Banks that provide funds transfer services to their customers are subject to the registration and reporting requirements of the anti-money laundering legislation

discussed below while services such as PayPal are not. Clearing members of Payments Canada that settle funds through the national cheque clearing system are subject to voluminous rules governing standards and finality of payment while operators of private retail payment networks such as Visa and MasterCard are governed largely by contract. A few years ago the Task Force for Payments Systems Review proposed that at the federal level all payments be regulated under a single system, without regard to the type of entity that facilitates the payment,[2] and the Department of Finance more recently issued a consultation paper on the same theme.[3]Should regulators take the same approach to the whole FinTech ecosystem?

FinTech regulators also face the difficult challenge of balancing the need to ensure the safety and soundness of the financial markets against the need to encourage further innovation that will allow Canadian FinTech businesses to become global competitors.

One specific area of concern is consumer and investor protection. FinTech companies are revolutionizing consumer banking and payments through alternative credit models that link lenders and borrowers directly, cut out the heavily regulated "middlemen" and apply sophisticated algorithms that can analyze the financial condition of prospective borrowers and deliver credit approvals in hours or even minutes rather than days. While this technology can speed up consumer lending, improve user experience and lower consumer costs, it raises some red flags as well. Happy with the slick and frictionless user interface, borrowing consumers may not be aware of the concerns that have been raised regarding cybersecurity and information privacy. Direct lenders may embrace the ease with which they can lend money out at attractive rates of return but not appreciate the risks of investing large sums of cash without the manifold protections mandated by securities regulations. Regulators must consider how best to guard consumer interests without stifling the innovations consumers desire.

An overview of the current regulatory landscape

There is currently no single Canadian FinTech regulator at either the federal or provincial level, nor any standard-setting technical bodies. The multidisciplinary nature of FinTech means that it is difficult to determine what should be regulated, and by whom. While there is no FinTech-specific regulation in Canada, some existing legislation does apply.

Information Security

Personal information and data security are huge concerns in the FinTech world and the growth of FinTech has significant cybersecurity implications. As FinTech products are increasingly embraced, both corporate and individual consumer financial information is at risk. Emerging tech companies are eager to jump into the financial services industry, but their security measures may be untested and insufficient. Some legislative protections do exist. Currently, businesses must comply with the federal *Personal Information Protection and Electronic Documents Act* or its provincial equivalents and Canada's Anti-Spam Legislation. However, some have expressed concerns that emergent FinTech companies may not be adequately equipped to deal with cybersecurity issues. The CEO of Toronto-Dominion Bank recently maintained that data breaches and solvency issues have "plagued" many new entrants, a claim hotly denied by the entrants themselves.[4]

Anti-Money Laundering

Canada's federal government has made significant strides in recent years to strengthen its anti-money laundering ("AML") regime in accordance with its international obligations. Because some FinTech transactions involving money transfers do not need to be made through financial institutions that are subject to AML laws, regulators

have expressed some concern that such transactions could be used for money laundering without appropriate regulatory scrutiny. Some FinTech companies must comply with the registration, client identification and verification and transaction reporting requirements under the federal *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* administered by the Financial Transactions and Reports Analysis Centre of Canada ("**FINTRAC**"), Canada's financial intelligence unit. Many others, however, do not fall within any of the categories of entities required to report to FINTRAC.

Consumer and Investor Protection

Due to rapid go-to-market strategies, investors and FinTech users may not receive the same amount of information and disclosure as that provided by incumbent financial institutions. However, start-ups must comply with relevant securities laws when raising capital, and with provincial consumer protection law when offering consumer-oriented products, but may be unfamiliar with the complex rules in these areas or assume that they do not apply. A FinTech starting seeking to raise capital through on-line "crowd funding" may be faced with the expensive and time consuming task of preparing a prospectus to be filed under provincial securities law unless an exemption exists. Recently, the Ontario Securities Commission has adopted Multilateral Instrument 45-108, which provides an exemption for "crowd-funding" offerings of up to $1.5 million within a 12 month period in relatively small amounts ($2,500 for each non-accredited investor, up to $10,000 per investor in a calendar year), but the eligibility requirements are complex and may necessitate bringing hundreds of shareholders on board. The Commission has also warned on-line marketplace lenders that the investments they offer to prospective lenders may be regarded as "securities" for the purpose of securities legislation and accordingly attract onerous registration and prospectus requirements unless an exemption is available.[5] Currently there are no exemptions specifically tailored to on-line lending.

In addition, each province has in place detailed requirements under consumer protection legislation mandating disclosure of the cost of borrowing (such as the "annual percentage rate") for consumer loans. These requirements apply to all lenders in this sector, not just financial institutions or finance companies as such. Any on-line lender making loans to consumers would be bound by these complex laws regardless of the electronic medium.

Third-Party Outsourcing Relationships

Building in-house tech solutions is expensive, increasingly pushing financial institutions to outsource their IT functions. With this, however, comes the danger of data leaks and the difficulty of engaging with companies that lack the tools to handle information responsibly. The federal Office of the Superintendant of Financial Institutions has issued guidelines[6] on outsourcing business activities and functions for federally-regulated financial institutions, which provide that the entity retains ultimate accountability.

Next Steps in Regulation

While the FinTech regulatory ecosystem is still in its infancy, it won't stay that way for long. The Canadian government will soon be fostering innovation in existing and start-up companies, while remaining cognizant of their role in providing regulatory protection to end-consumers of FinTech products. Although regulatory compliance can be costly for companies, clarifying applicable legislation and who it applies to, may be useful in long-term. Online payment methods and anti-money laundering are just two of many areas where we are likely to see–or are already seeing– considerable development.

Payments

Consumers are increasingly turning to mobile apps and online platforms to transfer funds, transforming existing payment infrastructures. In Canada, consumers are protected by provincial consumer protection laws and by the policies and business practices of the company, but in the absence of federal regulation, provinces and services providers are inconsistent in their regulation. In the retail payment space, existing rules and regulation have focused on the nature of the provider (i.e., a federally regulated financial institution is subject to different regulations than to a non-financial institution) rather than on the service provided (e.g., both entities may hold or transfer funds on behalf of consumers). In a recent consultation paper Payments Canada noted that stakeholders have called for "organization-agnostic oversight rules, applied consistently based on activity" for the payments system.[7] Adopting this recommendation may provide better protection for system participants and end users through enhanced consistency of rules, regardless of the service provider.

Anti-Money Laundering

A significant consideration for financial service regulators will be enhanced protection against money laundering risk. Because FinTech companies may not be directly regulated by traditional regulators, compliance with AML legislation may be inconsistent or non-existent. Many FinTech companies do not have the infrastructure in place or the requisite expertise to adequately investigate users and trace funds. With the increasing use of platforms that facilitate payments and movements of money with more speed and greater anonymity, FinTech companies and those using financial technology will likely come under greater scrutiny to ensure that they have taken adequate steps to mitigate money laundering risk. It is critical that financial services providers understand the extent to which they are subject to AML regulation and how to comply.

On June 17, 2016 the federal Department of Finance released amendments to regulations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* that were published on June 29.[8] The new regulations make material changes in the areas of client identification and verification, especially for clients who are not physically present, and the adoption of electronic signatures. These changes should make processes such as online customer onboarding faster, more seamless and much less dependent on paper documents, thereby fostering growth and innovation in the FinTech space. By the same token, they also serve as a reminder that FinTech companies are not flying under the regulatory radar.

Alternative Approaches to Regulation and Innovation: Sandboxes and Hubs

Some jurisdictions. notably the U.K., Australia and Singapore, have implemented an innovative approach to regulating FinTech service providers that could serve as a model for similar initiatives federally and provincially in Canada, known as the "regulatory sandbox".[9] In this model, qualified entrants are permitted to offer innovative products and services to a select subset of end users to allow them to test the waters without fear of regulatory sanctions. Often regulators will issue no-action letters, confirming that the rules are suspended for a specified period. Once the start-up is established, it leaves the "sandbox" and complies with the general regulatory regime in the "real world".

The U.S. Office of the Comptroller of the Currency recently issued a white paper[10] supporting reasonable financial innovation based on eight core principles. The Consumer Financial Protection Bureau proposed a "no-action letter" policy that bears some similarity to the regulatory sandbox approach. In the UK, the Government Chief Scientific Advisor has issued a FinTech Futures Report that makes 10 key recommendations for government to contribute to and support the evolution of FinTech.

Another promising approach that Canadian regulators might consider to adopt more widely is the "innovation

hub" that offers start-ups dedicated teams to help them navigate the regulatory landscape and obtain the necessary approvals.

These novel approaches show that regulators can do more than apply the brakes to FinTech innovation; they can also put their feet to the accelerator.

McMillan can help you navigate the regulatory landscape as well

McMillan's FinTech team is uniquely positioned to provide solutions to the increasingly complex questions of regulatory compliance in the FinTech sphere. Our team has extensive transactional and regulatory experience in the financial services industry. As a premier legal services provider, we are equipped to provide clients with strategic and innovative legal solutions to the new challenges and opportunities presented by the rise of FinTech. Please feel free to contact us with any questions you might have.

by Pat Forgione, Rob Scavone, Tayleigh Armstrong and Kelly Kan, Student-at-Law

[1] MaRS & Information Venture Partners, "Ten Surprising Facts about Fintech in Canada", online: <www.marsdd.com/wp-content/uploads/2015/02/Ten-Surprising-Facts-about-Fintech-in-Canada.pdf>
[2] See Task for the Payment Systems Review, *The Way We Pay: Transforming the Canadian Payments System*,available here.
[3] Balancing Oversight and Innovation in the Ways We Pay: A Consultation Paper (2015), available here.
[4] Barbara Schechter, " Debate over regulating fintechs heats up in Canada and the U.S", Financial Post, March 31, 2016.
[5] Ontario Securities Commission, News Release, "OSC Sets Out Expectations for Businesses Planning to Operate Peer-to-Peer Lending Websites" (19 June 2015), available here.
[6] OSFI Guideline B-10, *Outsourcing of Business Activities, Functions and Processes* (Revised March 2009), available here.
[7] Payments Canada, *Developing a Vision for Canada›s Payments Ecosystem*, Draft for Consultation, April 20, 2016, p. 4.
[8] *Regulations Amending Certain Regulations Made Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, 2016 SOR/2016-153 June 17, 2016, available here.
[9] For the U.K. example see the Financial Conduct Authority, "Regulatory Sandbox" (Nov. 2015) available here.
[10] E.g. the Australian Securities & Investment Commission's Innovation Hub, details of which are available here.

a cautionary note

Firm Profile

McMillan is a business law firm serving public, private and not-for-profit clients across key industries in Canada, the United States and internationally. With recognized expertise and acknowledged leadership in major business sectors, we provide solutions-oriented legal advice through our offices in Vancouver, Calgary, Toronto, Ottawa, Montréal and Hong Kong. Our firm values – respect, teamwork, commitment, client service and professional excellence – are at the heart of McMillan's commitment to serve our clients, our local communities and the legal profession.