



FinTech

Comparative Guide

Connecting Knowledge and People
Powered by Mondaq AI

FinTech Comparative Guide

Canada



Edwards, Kenny & Bray LLP

Kelly Samuels
t: +604.661.1003
e: ksamuels@ekb.com



Russell Allsup
t: +604.661.1084
e: rallsup@ekb.com



Other FinTech contributing countries

Cayman Islands

Egypt

France

Germany

Gibraltar

Hong Kong

Hungary

India

Iraq

Kenya

Lebanon

Liechtenstein

Luxembourg

Malta

Mexico

Netherlands

Nigeria

North Macedonia

Norway

Spain

Switzerland

Turkey

UAE


UK

1. Legal and enforcement framework

1.1 In broad terms, which legislative and regulatory provisions govern the fintech space in your jurisdiction?

Canada is a federal state comprised of 10 provinces and three territories, and legislation can be enacted at both the federal and provincial/territorial level. There is no single Canadian regulator that oversees fintech businesses. Rather, a fintech may be subject to a variety of both federal and provincial laws, depending on its activities and the provinces and territories in which it operates.

Provincial securities laws regulate the issuance, sale and trading of securities. 'Security' is broadly defined under securities laws and consequently numerous types of investments – including debt, equity, investment funds and derivatives – are subject to securities laws. Securities laws may apply to fintechs that issue securities to the public, as well as those that are engaged in crowdfunding, roboadvising, forex trading services and peer-to-peer lending platforms, among other activities.



Provincial consumer protection laws regulate certain business sectors and types of consumer transactions. Particularly relevant to fintechs is the consumer protection legislation that governs credit cards, agreements for credit and the disclosure of the cost of consumer credit with respect to fixed and open credit. In addition, specific regulations govern payday loans, which are generally short-term unsecured loans for smaller amounts of money.

The federal Proceeds of Crime (Money Laundering) and Terrorist Financing Act and associated regulations apply to financial service providers and certain other prescribed businesses, referred to as 'reporting entities', that engage in activities that are susceptible for being used for money laundering and terrorist financing. This legislation is intended to assist in detecting and deterring money laundering and the financing of terrorist activities. It also facilitates investigations and prosecutions of money laundering and terrorist activity financing offences.

Federal and provincial privacy laws will apply to fintechs that collect personal information. The federal Personal Information Protection and Electronic Documents Act (PIPEDA) governs how fintechs are permitted to collect, use and disclose personal information, and the obligations of fintechs in the event of a security breach involving personal information under their control. The provinces of British Columbia, Alberta and Quebec have enacted privacy legislation that is substantially similar to PIPEDA and such legislation may apply to fintechs operating in those provincial jurisdictions. Canada has also enacted anti-spam legislation which prohibits the sending of commercial electronic messages, including email and text, and installing software without the recipient's consent.

1.2 Do any special regimes apply to specific areas of the fintech space?

The Canadian Securities Administrators (CSA), the umbrella organisation of the Canadian provincial and territorial securities regulators, has implemented a regulatory sandbox programme to support fintech businesses seeking to offer innovative products and services in Canada. The programme permits firms to register and/or obtain exemptive relief from securities laws requirements, under a quicker and more flexible process than through a standard application, in order to test their products and services on a time-limited basis in the Canadian market. Some provincial regulators have related programmes that operate within their particular jurisdictions to provide guidance and support to fintech businesses, such as the OSC LaunchPad, an initiative of the Ontario Securities Commission and the British Columbia Securities Commission Tech Team. In addition, certain provincial regulators are members of the Global Financial Innovation Network, which aims to provide an efficient way for innovative businesses to interact with regulators across international jurisdictions, including a pilot test trial for firms wishing to test across more than one jurisdiction.

The CSA published Staff Notice 46-307, Cryptocurrency Offerings, in August 2017, outlining how existing securities laws may apply to initial coin offerings, initial token offerings, cryptocurrency investment funds and cryptocurrency trading platforms. The CSA advised that issuers of coins or tokens must determine whether such coins or tokens constitute securities, using a substance over form approach, on a case-by-case basis. Under Canadian securities laws, 'security' is broadly defined and includes an 'investment contract'. The CSA confirmed that many coins and tokens constitute investment contracts using the four-pronged test set out in *Pacific Coast Coin Exchange v Ontario Securities Commission*, [1978] 2 SCR 112, which is the leading Supreme Court of Canada decision on the meaning of 'investment contract'. In addition, Staff Notice 46-307 states that any trading platform that is a marketplace and facilitates trades in securities that are cryptocurrencies must comply with the marketplace requirements of Canadian securities laws. Examples of situations in which an offering of tokens may be subject to securities law.

Amendments to the federal Proceeds of Crime (Money Laundering) and Terrorist Financing Act and Regulations, intended to come into force in 2020, will expand the scope of the regime to apply to entities dealing in virtual currencies.

1.3 Which bodies are responsible for enforcing the applicable laws and regulations? What powers do they have?

Several provincial or federal regulatory bodies and self-regulatory organisations may have jurisdiction over fintechs, depending on the nature of the service they provide and the Canadian jurisdiction in which they operate.

Canada does not have federal securities legislation or a national securities regulator. Rather, provincial securities commissions are responsible for regulating and enforcing securities legislation, the purpose of which is to promote fair and efficient capital markets and ensure investor protection. The commissions have broad powers to investigate allegations of fraud and other misconduct in their respective jurisdictions. Through administrative proceedings before their tribunals, commissions can impose a variety of sanctions, such as monetary sanctions, disgorgement of ill-gotten gains and trading bans. Commissions can also pursue quasi-criminal proceedings before the courts, through which the courts can make a variety of orders, such as imprisonment, property preservation, appointment of receivers and restitution. In addition, two self-regulating organisations, the Investment Industry Regulatory Organization of Canada and the Mutual Fund Dealers Association of Canada, oversee the conduct of investment and mutual fund dealers, respectively. These organisations have powers to impose a broad range of sanctions on dealers who are not in compliance with applicable regulation, including fines and bans on employment in the industry.

Provincial consumer protection agencies are responsible for enforcing consumer protection legislation. These agencies generally have the authority to conduct inspections to determine compliance with the legislation and, where there is contravention, freeze the property of a business, require customer restitution, make compliance orders, order monetary penalties and sue on their own behalf or on behalf of consumers.

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) is 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 and abroad. FINTRAC has authority to issue an administrative monetary penalty to reporting entities that are in violation of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act. In addition, FINTRAC may disclose violations to law enforcement, which could ultimately result in criminal monetary penalties and/or imprisonment.

The Office of the Privacy Commissioner of Canada (OPC) oversees compliance with PIPEDA. The provinces of British Columbia, Alberta and Quebec each have a provincial privacy commissioner, who oversees compliance with the provincial privacy legislation in those provinces. In general, the privacy commissioner in each jurisdiction is empowered to investigate all complaints under the applicable privacy legislation in order to determine whether an individual's privacy rights have been contravened, and to conduct audits or investigations of businesses subject to PIPEDA and/or the provincial privacy legislation. Certain breaches of PIPEDA and provincial privacy legislation may give rise to monetary fines.

Payments Canada, established by the federal Payments Act, operates the payment clearing and settlement infrastructure in Canada, and oversees the rules for this infrastructure. In addition, there are codes of conduct and standards in the payments industry. While these rules, codes of conduct and standards are generally applicable only to certain federally regulated financial institutions, fintechs should consider whether compliance is desirable – particularly if their products use existing payment clearing and settlement infrastructure.

1.4 What is the regulators' general approach to fintech?

Traditionally, the banking and financial services sectors are heavily regulated at both the federal and provincial levels. While this regulation is important to protect consumers and mitigate risk to the Canadian financial system, it can also be a barrier to entry to the financial services sector by fintech businesses and consequently deter innovation and competition.

The current federal government has made it clear that innovation in the new digital economy is a priority and has provided funding for innovation programmes through its Innovation and Skills Plan. In addition, several governmental agencies and policy makers have issued statements in support of fintech. The Competition Bureau Canada conducted an extensive study of the fintech industry, which culminated in the publishing of its Market Study Report, which made several recommendations to Canada's regulators and policy makers regarding the fintech sector. The report specifically suggests that, while regulation is necessary to meet policy objectives such as consumer protection and financial stability, regulation governing fintech businesses would benefit from modernisation in order to promote greater competition and innovation for Canadian consumers.

Regulators appear to be taking a considered and deliberate approach to fintech, recognising the benefits that fintech can generate for consumers and business. Several governmental agencies and regulators have released consultation papers and are considering how best to amend or modernise the regulatory regime to address fintech. For example, the Canadian Department of Finance has launched consultations on open banking and a new oversight framework for retail payments. Payments Canada has commenced modernisation of the core clearing and settlement systems in Canada, including development of a new real-time retail payment system. Provincial securities regulators are currently seeking input from stakeholders on how best to regulate crypto-asset trading platforms.

1.5 Are there any trade associations for the fintech sector?

The Financial Innovation & Technology Association of Canada aims to:

- develop, support and promote the ecosystem for financial technology and financial innovation in Canada;
- advocate for balanced policy initiatives for financial innovation companies;
- have a national voice for financial innovation across Canada; and
- promote its members domestically and internationally.

The National Crowdfunding & Fintech Association provides education, market intelligence, industry stewardship, networking and funding opportunities and services to its community members, and works with industry, government, partners and affiliates to the fintech and funding industry in Canada.

The Digital Finance Institute (DFI) is a think tank for fintech, artificial intelligence and blockchain which aims to address issues in respect of the nexus between financial innovation, digital finance policy and regulation, financial inclusion and women in financial technology. The DFI is working to help create a fintech association, and is currently seeking feedback before taking steps to launch. The aim of this new association is to bring together stakeholders involved in fintech, such as law firms, accounting firms, finance firms, venture capital firms, start-ups, fintech companies, government agencies and universities.



2. FinTech market

2.1 Which sub-sectors of the fintech industry have become most embedded in your jurisdiction?

Canada has a wide variety of active fintech businesses and most sub-sectors of the fintech industry have become embedded in Canada. Money transfer and payments are likely the most embedded and widely adopted sub-sectors of the fintech industry. Personal finance, wealth management and robo-advising are also well embedded. Finally, lending services, which comprise non-financial institutions and platforms, can be considered well embedded within Canada.

2.2 What products and services are offered?

A very broad range of products and services are offered in all areas of fintech.

2.3 How are fintech players generally structured?

Fintech players are most typically structured as limited liability companies incorporated at either the provincial or federal level.

2.4 How are they generally financed?

While there have been a limited number of fintech businesses which have financed through initial public offerings, fintech businesses are more typically funded through alternative early stage funding sources, as opposed to raising money in the capital markets or through taking on traditional bank debt.

Investment by venture capital funds is a key source of funding for many of Canada's top fintech companies. According to the PwC/CB Insights MoneyTree™ Canada Report Q4 & Full-Year 2018, venture capital funding in Canada totalled C\$456 million for fintech in 2018, up from C\$441 million in 2017.

Investment through the 'exempt market' (other than venture capital funds) is another common early stage funding source. Generally, if a company plans to offer securities to the public, it must do so under a prospectus. However, some exemptions from this rule permit a company to raise capital without the time and expense of preparing a prospectus. Common exemptions include issuing securities pursuant to an offering memorandum, or to 'accredited' investors that meet certain criteria imposed by the provincial securities commissions, including meeting certain income or financial asset tests.

Financing may also come through a strategic partnership. There are several examples of Canadian banks partnering with fintech companies in order to access innovative products and solutions to provide to their customers.

Federal and provincial government funding and investment programmes are also available for innovative businesses – for example, through the Business Development Bank of Canada and the Strategic Innovation Fund.



2.5 How are they positioned within the broader financial services landscape?

The Canadian banking system is dominated by five large chartered banks. These institutions are conservatively operated and strictly regulated. However, recent amendments to the legislation regulating Canadian banks removed restrictions on certain types of relationships among banks and fintech companies, which may lead to greater partnership opportunities between banks and fintechs, whereby banks either source technology from, or develop technology in partnership with, fintechs.

2.6 Do start-ups generally outsource back office functions and is there a developed market for them to access? What are the legal implications of outsourcing?

There is no prohibition in Canada on outsourcing back office functions and there are service providers available for fintechs to access. Outsourcing is a relatively common practice among Canadian businesses generally, but perhaps not for start-ups where expenses must be tightly managed.

No federal or provincial laws in Canada generally regulate outsourcing transactions. What regulations will apply to an outsourcing transaction will depend on the nature of the transaction itself and the industry sector in which the business is operating. For example, the federal Office of the Superintendent of Financial Institutions (OSFI) has published Guideline B-10, Outsourcing of Business Activities, Functions and Processes, which sets out OSFI's expectations for federally regulated entities that outsource or contemplate the outsourcing of one or more of their business activities to a service provider. Although provincially regulated financial entities, such as provincially regulated credit unions, are not specifically subject to Guideline B-10, it is the general practice of provincial regulators to require compliance with Guideline B-10 as well.


Fintechs that outsource should consider privacy legislation in connection with any customer or employee data that is being provided to service providers. The federal Personal Information Protection and Electronic Documents Act provides that a business that has collected personal information remains responsible for such information where transferred to third parties for processing, and requires the business to use contractual or other means to provide a comparable level of protection while the information is being processed by third parties. Outsourcing agreements should therefore contain provisions addressing confidentiality and requiring the parties to comply with all applicable privacy laws.

3. Technologies

How are the following key technologies in the fintech space regulated and what specific legal issues are associated with each?

3.1 Internet (e-commerce)

Most provinces and territories of Canada have enacted legislation governing electronic transactions and electronic commerce. This legislation is 'media neutral' and has the objective of removing statutory barriers to the use of, and helping to facilitate the adoption of, information in electronic form.



Among other things, electronic commerce legislation sets out provisions relating to the collection, storage and retention of documents in electronic form; and generally provides that a document, including a contract, in electronic form satisfies the requirement that a document be 'in writing'. The enforceability of click-wrap agreements, such as the use of an 'I Agree' button or icon, has been upheld by various levels of courts, including the Supreme Court of Canada in *Dell Computer Corp v Union des consommateurs*, which affirmed *Kanitz v Rogers Cable Inc*, an Ontario case that upheld the enforceability of click-wrap agreements. In addition, electronic commerce legislation provides that if there is a requirement under law for the signature of a person, that requirement is satisfied by an electronic signature.

Several provinces have enacted consumer protection legislation that applies to online consumer contracts, and provides consumers with rights and remedies in respect of sales agreements formed through internet communications. In addition, the federal Competition Act contains provisions addressing false or misleading representations and deceptive marketing practices in promoting the supply or use of a product.

Fintechs that collect personal information in the course of carrying on an e-commerce business must comply with the federal Personal Information Protection and Electronic Documents Act (PIPEDA) or its provincial equivalents, if applicable. PIPEDA requires businesses to:


- obtain informed consent for the collection, use and disclosure of personal information;
- have in place appropriate safeguards to protect personal information; and
- in certain circumstances, report any security breach involving the personal information to the privacy commissioner and affected individuals.

In addition, under Canada's anti-spam legislation, fintechs are required to obtain consent from customers before sending them commercial electronic messages, such as emails or texts; although implied consent can be inferred in some instances, such as where there is an existing business relationship as described in the legislation.

3.2 Mobile (m-commerce)

Most provinces and territories of Canada have enacted legislation governing electronic transactions and electronic commerce. This legislation is 'media neutral' and has the objective of removing statutory barriers to the use of, and helping to facilitate the adoption of, information in electronic form. Among other things, electronic commerce legislation sets out provisions relating to the collection, storage and retention of documents in electronic form; and generally provides that a document, including a contract, in electronic form satisfies the requirement that a document be 'in writing'. The enforceability of click-wrap agreements, such as the use of an 'I Agree' button or icon, has been upheld by various levels of courts, including the Supreme Court of Canada in *Dell Computer Corp v Union des consommateurs*, which affirmed *Kanitz v Rogers Cable Inc*, an Ontario case that upheld the enforceability of click-wrap agreements. In addition, electronic commerce legislation provides that, if there is a requirement under law for the signature of a person, that requirement is satisfied by an electronic signature.

Several provinces have enacted consumer protection legislation that applies to online consumer contracts, and provides consumers with rights and remedies in respect of sales agreements formed through internet communications. In addition, the federal Competition Act contains provisions addressing false or misleading representations and deceptive marketing practices in promoting the supply or use of a product.



Fintechs that collect personal information in the course of carrying on an m-commerce business must comply with PIPEDA or its provincial equivalents, if applicable. PIPEDA requires businesses to:

- obtain informed consent for the collection, use and disclosure of personal information;
- have in place appropriate safeguards to protect personal information; and
- in certain circumstances, report any security breach involving the personal information to the privacy commissioner and affected individuals.

In addition, under Canada's anti-spam legislation, fintechs are required to obtain consent from customers before sending them commercial electronic messages, such as emails or texts; although implied consent can be inferred in some instances, such as where there is an existing business relationship as described in the legislation.

3.3 Big data (mining)

Fintechs that collect and/or use big data must comply with PIPEDA or its provincial equivalents, if applicable. PIPEDA requires businesses to:

- obtain informed consent for the collection, use and disclosure of personal information;
- have in place appropriate safeguards to protect personal information; and
- in certain circumstances, report any security breach involving the personal information to the privacy commissioner and affected individuals.

Pursuant to PIPEDA, a business collecting personal information must make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used.

Fintechs are also required to comply with Canada's anti-spam legislation, which prohibits the sending of commercial electronic messages, including email and text, and the installation of software without the recipient's consent.


The collection of personal information also engages the deceptive marketing provisions of the federal Competition Act. In collecting data, fintechs should consider the representations that they make to the individuals from whom they are collecting the information, and ensure that these are not false or misleading so as to lead such individuals to provide information that they would not otherwise have provided or to purchase products and services that they would not otherwise have purchased. In addition, fintechs that use big data to sell products and services to consumers must ensure they are not using deceptive practices, such as submitting fake reviews or disguising advertisements by making them similar to other content viewed by consumers online.

3.4 Cloud computing

Fintechs that collect personal information in the course of carrying on a cloud computing business must comply with PIPEDA or its provincial equivalents, if applicable. PIPEDA requires businesses to:

- obtain informed consent for the collection, use and disclosure of personal information;
- have in place appropriate safeguards to protect personal information; and
- in certain circumstances, report any security breach involving the personal information to the privacy commissioner and affected individuals.

Some Canadian jurisdictions prohibit government agencies and their service providers from moving personal data outside Canada, with limited exceptions. Fintechs involved in cloud storage that contract with government agencies should therefore ensure they are aware of any applicable data residency requirements.



In addition, the federal Office of the Superintendent of Financial Institutions (OSFI) has published Guideline B-10, Outsourcing of Business Activities, Functions and Processes, which sets out OSFI's expectations for federally regulated entities (FREs) that outsource or contemplate the outsourcing of one or more of their business activities to a service provider. FREs include banks, federally regulated trust and loan companies, and certain insurance companies, among others. Although provincially regulated financial entities, such as provincially regulated credit unions, are not specifically subject to Guideline B-10, it is the general practice of provincial regulators to require compliance with Guideline B-10 as well. Thus, if a fintech will be providing services to FREs or their provincial equivalents, they should be aware of the need to comply with Guideline B-10. Guideline B-10 contains obligations with respect to such matters as:

- confidentiality, security and separation of property;
- location of records;
- business continuity planning;
- access and audit rights;
- rules and limitations on subcontracting by the service provider; and
- monitoring and overseeing the outsourcing arrangement.

These items must typically be addressed in any outsourcing contract between the service provider and the FRE.

3.5 Artificial intelligence

Canada currently does not have an artificial intelligence (AI) specific regulatory framework. However, the Canadian federal government has issued a Directive on Automated Decision-Making, which took effect on 1 April 2019, with compliance required by no later than 1 April 2020. The objective of the directive is to ensure that automated decision systems – defined as technology that either assists or replaces the judgement of human decision makers – are used in a manner that reduces risks to Canadians and federal institutions, and leads to more efficient, accurate, consistent and interpretable decisions made pursuant to Canadian law. The directive sets out requirements for federal governments that wish to use an automated decision system where the intended recipient is an individual or business external to the government of Canada that is using services provided by a government department. Requirements include:

- completing an algorithmic impact assessment prior to the production of any automated decision system;
- providing notice in plain language and prominently on relevant websites that the decision rendered will be undertaken in whole or in part by an automated decision system;
- providing a meaningful explanation to affected individuals of how and why the decision was made;
- monitoring the outcomes of automated decision systems to safeguard against unintentional outcomes; and
- confirming that the data collected for, and used by, the automated decision system is relevant, accurate, up to date and in accordance with applicable laws.

Although compliance with the directive is the responsibility of the federal government, any fintech which intends to provide services to the federal government that could be construed as an automated decision system should confirm that its product complies with the directive by 1 April 2020.

In addition, since AI systems collect and use large amounts of data, fintechs operating in the AI space that are collecting, using or disclosing personal information must ensure they are doing so in compliance with PIPEDA or its provincial equivalents, if applicable. PIPEDA requires businesses to:

- obtain informed consent for the collection, use and disclosure of personal information;
- have in place appropriate safeguards to protect personal information; and
- in certain circumstances, report any security breach involving the personal information to the privacy commissioner and affected individuals.

In addition, under Canada's anti-spam legislation, businesses must obtain consent from recipients before sending commercial electronic messages, such as emails or texts, or installing computer software on the recipient's device.

3.6 Distributed ledger technology (Blockchain, cryptocurrencies)

Canada currently does not have a distributed ledger technology specific regulatory framework. However, provincial securities laws, which regulate the issuance, sale and trading of securities, may be applicable to fintechs that operate business relating to crypto-assets. 'Security' is broadly defined under securities laws and consequently numerous types of investments, including certain crypto-assets.

The Canadian Securities Administrators (CSA), the umbrella organisation of the Canadian provincial and territorial securities regulators, published Staff Notice 46-307, Cryptocurrency Offerings, in August 2017, outlining how existing securities laws may apply to initial coin offerings, initial token offerings, cryptocurrency investment funds and cryptocurrency trading platforms. The CSA advised that issuers of coins or tokens must determine whether such coins or tokens constitute securities, using a substance over form approach, on a case-by-case basis. Under Canadian securities laws, 'security' is broadly defined and includes an 'investment contract'. The CSA confirmed that many coins and tokens constitute investment contracts using the four-pronged test set out in *Pacific Coast Coin Exchange v Ontario Securities Commission*, [1978] 2 SCR 112, which is the leading Supreme Court of Canada decision on the meaning of 'investment contract'. In addition, Staff Notice 46-307 states that any trading platform that is a marketplace and facilitates trades in securities that are cryptocurrencies must comply with the marketplace requirements of Canadian securities laws.

In June 2018, the CSA published Staff Notice 46-308, Securities Law Implications for Offerings of Tokens, to provide further clarification to issuers wishing to complete offerings of tokens, particularly tokens referred to as 'utility tokens'. Staff Notice 46-308 provides guidance on when an offering of tokens may or may not involve an offering of securities and, in particular, provides several examples of situations in which an offering of tokens may be subject to securities law.

Amendments to the federal Proceeds of Crime (Money Laundering) and Terrorist Financing Act and Regulations, intended to come into force in 2020, will expand the scope of the regime to apply to entities dealing in virtual currencies.

If personal information is being stored on a distributed ledger, privacy laws may be relevant, in which case the fintech operating the distributed ledger must ensure compliance with PIPEDA or its provincial equivalents, if applicable. PIPEDA requires businesses to:

- obtain informed consent for the collection, use and disclosure of personal information;
- have in place appropriate safeguards to protect personal information; and
- in certain circumstances, report any security breach involving the personal information to the privacy commissioner and affected individuals.

In addition, fintechs must comply with Canada's anti-spam legislation, which prohibits the sending of commercial electronic messages, including email and text, and the installation of software without the recipient's consent.



4. Activities

How are the following key activities in the fintech space regulated and what specific legal issues are associated with each?

4.1 Crowdfunding, peer-to-peer lending

There are different types of crowdfunding, such as donation, pre-selling of products and securities (or equity) crowdfunding. Under Canadian law, a person who receives bonds, shares or other securities in exchange for giving money to a business is considered to be an investor and securities laws will apply. A business seeking to raise capital by issuing securities must file a prospectus with the securities regulator or have an exemption from such prospectus requirements. In addition, a person cannot be in the business of trading securities unless such person is registered in the province or territory where it is carrying on this business or has an exemption from the registration requirement under securities laws.

Certain Canadian provinces and territories have adopted crowdfunding exemptions from the prospectus requirement, which permit start-ups and small businesses to raise relatively small amounts of capital from investors using securities crowdfunding without filing a prospectus, provided that certain conditions are met. Some jurisdictions also permit funding portals to facilitate trades of securities without having to register as a dealer, provided that certain conditions are met; although a funding portal can also be operated by a registered dealer. Fintechs that seek to raise capital through crowdfunding or that wish to operate a crowdfunding portal will need to be aware of any crowdfunding regimes available in the jurisdiction in which they are operating, including Multilateral Instrument 45-108, Crowdfunding, and Multilateral CSA Notice 45-316, Start-up Crowdfunding Registration and Prospectus Exemptions. These exemptions are not harmonised across Canada and there are differences in the regimes applicable in some provinces and territories.

Canadian securities regulators have taken the position that loan arrangements entered into using peer-to-peer (P2P) lending platforms may be 'securities' and P2P lending companies could be trading in securities and therefore must register as dealers with securities regulators in the provinces where they operate. Further, if their services also involve issuing new securities, P2P lending companies must either file a prospectus in respect of those securities or be able to rely on an exemption. P2P lending companies in Canada have worked to fit into the regulatory model by registering with regulators and sidestepping the prospectus requirement using existing exemptions. For many, this has meant restricting investing opportunities to a limited class of institutional investors and high-net-worth individuals who qualify as 'accredited investors'. Others have worked with regulators to find different approaches to access a larger market of borrowers and investors – for example, through operating as an exempt market dealer and relying on the offering memorandum exemption.

4.2 Online lending and other forms of alternative finance

Fintechs that provide online lending services or other forms of alternative finance services will need to comply with any applicable provisions of consumer protection legislation in respect of disclosure of the cost of consumer credit with respect to fixed and open credit. In addition, some jurisdictions have enacted specific regulations that govern payday loans, which are generally short-term unsecured loans for small amounts of money. Among other things, such payday regulations may:

- require payday lenders to be licensed;
- impose limitations on the amount of any loan to a consumer relative to net pay;
- set requirements with respect to loan cancellation rights of the consumer; and
- impose requirements on signage.

In addition, the federal Criminal Code, which applies across Canada, provides that it is a criminal offence to enter into an agreement or arrangement to receive, or actually to receive, 'interest' on credit in excess of 60% per annum of the total value of the credit advanced. The broad definition of 'interest' in the code captures ordinary commercial interest as well as a broad range of fees, fines and expenses. Accordingly, fintechs offering online lending services or other forms of alternative finance will need to ensure that total interest (as defined in the code) does not exceed this criminal interest rate.

If, in the course of providing online lending or alternative finance services, the fintech is collecting, using or disclosing personal information, it must ensure that it is doing so in compliance with the federal Personal Information Protection and Electronic Documents Act (PIPEDA) or its provincial equivalents, if applicable. PIPEDA requires businesses to:

- obtain informed consent for the collection, use and disclosure of personal information;
- have in place appropriate safeguards to protect personal information; and
- in certain circumstances, report any security breach involving the personal information to the privacy commissioner and affected individuals.


In addition, under Canada's anti-spam legislation, businesses must obtain consent from recipients before sending commercial electronic messages, such as emails or texts, or installing computer software on the recipient's device.

4.3 Payment services (including marketplaces that route payments from customers to suppliers (eg, Uber and AirBnb))

The current oversight of payments in Canada is focused on the core national payment clearing and settlement systems, including:

- the Large Value Transfer System, which facilitates the transfer of irrevocable payments between Canadian financial institutions; and
- the Retail System, which clears paper-based and electronic payments, and through which the majority of payments in Canada are cleared.

Legislation and codes of conduct impose operational requirements – such as mechanisms to safeguard consumer funds upon insolvency, specific disclosure rules and complaint-handling procedures – on specific regulated financial service providers, such as banks and payment card networks. However, other non-traditional retail payment service providers (PSPs) are not currently subject to this comprehensive oversight framework. Given the rapid pace of innovation in the retail payments space and the entrance of non-traditional PSPs into the Canadian payments ecosystem, the federal government has confirmed that it intends to put into place a new oversight framework for retail payments that will be focused on payment activities rather than the type of entity performing them. Accordingly, it is expected that fintechs involved in the payments industry that are currently unregulated may be subject to the new regulatory framework when it comes into force.



In addition, fintechs operating a payment service may be required to register with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) as a money services business. A business will be considered a money services business if it provides certain prescribed services to the public, including transferring funds from one individual or organisation to another using an electronic funds transfer network or any other method. As a money services business, a fintech will be required to:

- implement a compliance regime;
- keep certain records and ascertain client identification;
- report suspicious transactions and terrorist property to FINTRAC; and
- report certain large cash transactions and international funds transfers to FINTRAC.

4.4 Forex

Canada does not have federal securities legislation or a national securities regulator. Rather, provincial securities commissions are responsible for regulating and enforcing securities legislation in each of their respective jurisdictions. Collectively the provinces and territories have formed the Canadian Securities Administrators (CSA), which is primarily responsible for developing a harmonised approach to securities regulation across Canada. Many substantive aspects of securities regulation – including registration and prospectus requirements, exemptions and continuous disclosure requirements – are harmonised through the use of national instruments. Securities regulators also rely on two national self-regulatory organisations, the Investment Industry Regulatory Organization of Canada (IIROC) and the Mutual Fund Dealers Association, to govern the activities of certain securities dealers.


In Canada, forex trading is regulated as trading in either securities or derivatives, and regulation may vary under applicable provincial and territorial securities and derivatives legislation. Persons seeking to offer forex trading services must be registered in the provincial jurisdiction in which they intend to do business, and if they intend to offer trading on margin, must also be a member of IIROC.

Fintechs offering forex trading services where forex trading is considered trading in a security must comply with various provincial securities instruments regarding registration and prospectus requirements, unless exemptions are available. In addition, traders must ensure that they avoid misrepresentations in secondary market transactions.

4.5 Trading

A person (including an individual or a firm) that is in the business of trading securities must be registered with the securities regulator in each province or territory where it does business, unless an exemption applies. The registration regime that applies to all provinces and territories is set out in National Instrument 31-103, Registration Requirements, Exemptions and Ongoing Registrant Obligations, and related rules. National Instrument 31-103 sets out the different categories of registration and the requirements and qualifications of registrants in respect of each. Registrants are permitted to offer products and services based on their category of registration. In addition, detailed regulations apply to marketplaces that bring together buyers and sellers of securities and meet certain other enumerated conditions.

Canadian securities regulators have taken the position that securities laws may apply to fintech businesses that issue cryptoassets, such as tokens or certain cryptocurrencies if based in Canada or that issue cryptoassets to Canadian residents, as well as to platforms that facilitate the trading of cryptoassets.



In CSA Staff Notice 46-307, Cryptocurrency Offerings (published in August 2017), the CSA outlined how existing securities laws may apply to initial coin offerings, initial token offerings, cryptocurrency investment funds and cryptocurrency trading platforms. In March 2019, the CSA published Consultation Paper 21-402, Proposed Framework for Crypto-Asset Trading Platforms, proposing new rules governing platforms that facilitate the purchase, sale or transfer of cryptoassets, and seeking comments from industry stakeholders in respect of same. The proposed rules, which have not been finalised, would apply to those platforms which are subject to securities legislation that operate in Canada or which serve Canadian investors.

4.6 Investment and asset management

Canada does not have federal securities legislation or a national securities regulator. Rather, provincial securities commissions are responsible for regulating and enforcing securities legislation in each of their respective jurisdictions. Collectively, the provinces and territories have formed the CSA, which is primarily responsible for developing a harmonised approach to securities regulation across Canada. Many substantive aspects of securities regulation – including registration and prospectus requirements, exemptions and continuous disclosure requirements – are harmonised through the use of national instruments. Securities regulators also rely on two national self-regulatory organisations, the Investment Industry Regulatory Organization of Canada (IIROC) and the Mutual Fund Dealers Association (MFDA), to govern the activities of certain securities dealers.

A person (including an individual or a firm) that is in the business of trading securities or advising clients on securities must be registered with the securities regulator in each province or territory where it does business, unless an exemption applies. The registration regime that applies to all provinces and territories is set out in National Instrument 31-103, Registration Requirements, Exemptions and Ongoing Registrant Obligations, and related rules. National Instrument 31-103 sets out the different categories of registration and the requirements and qualifications of registrants in respect of each. Registrants are permitted to offer products and services based on the category of registration. For example, mutual fund dealing representatives can only offer to sell mutual funds.


Registrants which are registered under the ‘investment dealer’ category must be members of IIROC and will be subject to further rules as prescribed by IIROC. Investment dealers are individuals or firms that are permitted to sell a wide range of investment products, such as shares, bonds, mutual funds, exchange-traded funds and other investment funds. IIROC oversees all investment dealers and trading activity on debt and equity marketplaces in Canada by setting and enforcing rules regarding the proficiency, business and financial conduct of dealer firms and their registered employees.

Similarly, registrants which are registered under the ‘mutual fund dealer’ category must be members of the MFDA and will be subject to further rules as prescribed by the MFDA.

4.7 Risk management

Fintechs that collect personal information in the course of provision of risk management services must comply with PIPEDA or its provincial equivalents, if applicable. PIPEDA requires businesses to:

- obtain informed consent for the collection, use and disclosure of personal information;
- have in place appropriate safeguards to protect personal information; and
- in certain circumstances, report any security breach involving the personal information to the privacy commissioner and affected individuals.



In addition, the federal Office of the Superintendent of Financial Institutions (OSFI) has published Guideline B-10, Outsourcing of Business Activities, Functions and Processes, which sets out OSFI's expectations for federally regulated entities (FREs) that outsource or contemplate the outsourcing of one or more of their business activities to a service provider. FREs include banks, federally regulated trust and loan companies, and certain insurance companies, among others. Although provincially regulated entities, such as provincially regulated credit unions, are not specifically subject to Guideline B-10, it is the general practice of provincial regulators to require compliance with Guideline B-10 as well. Thus, if a fintech will be providing services to FREs or their provincial equivalents, they should be aware of the need to comply with Guideline B-10. Guideline B-10 contains obligations with respect to such matters as:

- confidentiality, security and separation of property;
- location of records;
- business continuity planning;
- access and audit rights;
- rules and limitations on subcontracting by the service provider; and
- monitoring and overseeing the outsourcing arrangement.

These items must typically be addressed in any outsourcing contract between the service provider and the FRE.

4.8 Robo advice

A person (including an individual or a firm) that is in the business of trading securities or advising clients on securities must be registered with the securities regulator in each province or territory where it does business, unless an exemption applies. The registration regime that applies to all provinces and territories is set out in National Instrument 31-103, Registration Requirements, Exemptions and Ongoing Registrant Obligations, and related rules. Canadian securities regulators have stated (see CSA Staff Notice 31-342 Guidance for Portfolio Managers Regarding Online Advice, published 24 September 2015) that there is no 'online advice' exemption from the normal conditions of registration for a portfolio manager, and that the registration and conduct requirements set out in National Instrument 31-103 are technology neutral. The CSA has stated that online advisers which have been approved to carry on business in Canada differ from 'roboadvisers' operating in the United States, which may provide their services to clients with little or no involvement of a human advising representative. Rather, online advisers in Canada are viewed as providing hybrid services, whereby they use an online platform for the efficiencies it offers, while human advising representatives remain actively involved in and responsible for decision making. A fintech wishing to undertake roboadvising activities in Canada will be required to file substantial documentation with the securities regulators, including the proposed know-your-customer questionnaire and processes, which will then be reviewed by regulators in order to determine how the fintech will meet its obligations under National Instrument 31-103.

4.9 Insurtech

The traditional insurance industry is heavily regulated in Canada at both the federal and provincial level. Given that one of fintech's biggest advantages in the insurance sector is enabling traditional insurance companies to gain risk insights through existing data, the largest potential legal issue facing insurtech businesses likely relates to the collection and use of big data.

Much of the data being gathered for insurtech purposes will constitute personal information and is therefore subject to PIPEDA or its provincial equivalents, if applicable. PIPEDA requires businesses to:

- obtain informed consent for the collection, use and disclosure of personal information;
- have in place appropriate safeguards to protect personal information; and

- in certain circumstances, report any security breach involving the personal information to the privacy commissioner and affected individuals.

In addition, under Canada's anti-spam legislation, businesses must obtain consent from recipients before sending commercial electronic messages, such as emails or texts, or installing computer software on the recipient's device.

5. Data security and cybersecurity

5.1 What is the applicable data protection regime in your jurisdiction and what specific implications does this have for fintech companies?

The primary statute that governs data protection in the private sector is the federal Personal Information Protection and Electronic Documents Act (PIPEDA), which regulates the collection, use and disclosure of personal information, except in those provinces that have enacted legislation that is substantially similar to PIPEDA. Currently, British Columbia, Alberta and Quebec have enacted substantially similar legislation. However, PIPEDA will generally apply to businesses that disclose personal information across provincial borders or to a destination outside of Canada. Certain additional legislation in respect of specific sectors, such as with respect to personal health information, has also been enacted by some provinces. A separate regulatory regime applies to public bodies at both the federal and provincial level.

Under PIPEDA, businesses that collect personal information are responsible for the information under their control (including information transferred to third parties), and must designate an individual to be accountable for the businesses compliance with PIPEDA. In addition, businesses must:

- obtain informed consent to the collection, use and disclosure of personal information;
- protect personal information in their possession against loss, theft or unauthorised access, disclosure, copying, use or modification; and
- limit the collection of personal information to that which is necessary for the applicable purpose.


PIPEDA also requires businesses to give notice to the privacy commissioner and to affected individuals of any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.

5.2 What is the applicable cybersecurity regime in your jurisdiction and what specific implications does this have for fintech companies?

PIPEDA requires businesses to maintain security safeguards which protect personal information, regardless of the format in which it is held, against loss or theft, as well as unauthorised access, disclosure, copying, use, or modification. Safeguards may include:

- physical measures, such as locked storage and restricted access;
- organisational measures, such as limiting access to a 'need-to-know' basis; and
- technological measures, such as the use of passwords and encryption.

Canada's Anti-spam Law contains provisions which govern the installation of software in the course of commercial activities. These provisions are aimed at viruses and spyware being installed by installers within Canada.



In addition, the federal Office of the Superintendent of Financial Institutions and the Canadian Securities Administrators each provide guidance to address cybersecurity risks for organisations which fall under their jurisdiction.

6. Financial crime

6.1 What provisions govern money laundering and other forms of financial crime in your jurisdiction and what specific implications do these have for fintech companies?

Canada's anti-money laundering regime is largely established by the federal Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated regulations, which have the objective of implementing measures to detect and deter money laundering and the financing of terrorist activities, and to facilitate investigations and prosecution of offences in respect of same. In addition, money laundering and certain other financial crimes are offences under Canada's Criminal Code.

The PCMLTFA requires 'reporting entities' to:

- implement a compliance regime;
- keep certain records and ascertain client identification;
- report suspicious transactions and terrorist property to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC); and
- report certain large cash transactions and international funds transfers to FINTRAC.


Other requirements may apply depending on the type of reporting entity. Reporting entities include financial entities (eg, banks, credit unions, trust companies and loan companies), securities dealers, and money services businesses. Fintech businesses will need to determine, based on their business activities, whether they are considered reporting entities for the purposes of the PCMLTFA.

In addition, money services businesses in Canada must register with FINTRAC. A business will be considered a money services business if it provides certain prescribed services to the public, including transferring funds from one individual or organisation to another using an electronic funds transfer network or any other method.

The Department of Finance released amendments to the Proceeds of Crime (Money Laundering and Terrorist Financing Regulations) in July 2019, which will largely come into force on 1 June 2020. Notably, the amendments impose obligations on reporting entities with respect to virtual currency transactions and the definition of 'money services business' has been expanded to include those that deal in virtual currency. Consequently, once the amendments are in force, a business dealing in virtual currency, such as a business providing virtual currency exchange services, will be required to register as a money services business and comply with the related obligations under the regulations, such as having a compliance regime and ascertaining client identification.

7. Competition

7.1 Does the fintech sector present any specific challenges or concerns from a competition perspective? Are there any pro-competition measures that are targeted specifically at fintech companies?



The Canadian banking system is dominated by five large chartered banks. These institutions are conservatively operated and strictly regulated, which has resulted in a banking system that is regarded as one of the most stable in the world. A possible concern, however, is a lack of competition in the marketplace, exacerbated in part by the heavy regulation of the industry and the fact that Canadian consumers typically view their own banks favourably and may not be willing to switch service providers.

In December 2017 the Competition Bureau Canada, an independent law enforcement agency which ensures that Canadian businesses and consumers prosper in a competitive and innovative marketplace, published a market study report following an 18-month study of the fintech industry. The report provided a number of recommendations to Canada's regulators regarding how to foster fintech innovation and competition in order to benefit Canadian consumers. A key takeaway from the report is that regulation should be minimally intrusive in order to ensure that it does not inhibit market competition. A progress report published in September 2019 examined recent regulatory and policy changes that indicate progress in reducing barriers to innovation and entry of fintech into the marketplace.

One potential anti-competitive practice identified by the Competition Bureau in the progress report is the practice of 'de-risking' by Canadian banks. Banks can terminate or refuse to provide banking services to clients engaged in payment or money transfer services in order to minimise the banks' own risk of non-compliance with Canada's anti-money laundering and counter-terrorist financing (AML/CT) regime. A fintech business will suffer serious implications to its business if it is unable to access banking services. Thus, by de-risking, banks can potentially prevent the entry of new competition into the marketplace. Canada's Department of Finance has undertaken consultations on the practice of de-risking as part of its current review of Canada's AML/CT regime.

8. Innovation

8.1 How is innovation in the fintech space protected in your jurisdiction?

The main IP rights available to protect innovation in Canada include copyright, patents, trade secrets and trademarks.

If a fintech product involves software, copyright will extend to the source code as a literary work. Copyright is the exclusive legal right to produce, reproduce or publish an original literary work. Generally, pursuant to the Copyright Act (Canada), copyright will automatically arise in the source code at the time of creation. It is also possible to register the copyright with the Canadian Intellectual Property Office to obtain a certificate which serves as evidence that the copyright exists and that the person registered is the owner of the copyright. Copyright will not prevent other parties from replicating the functionality of a fintech's software using different code, and contractual arrangements may be necessary to govern ownership of software functionality.

Patents may be available to protect new financial technology. Patents are granted to applicants by the Canadian government pursuant to the Patent Act (Canada), and provide a time-limited exclusive right within Canada to make, use and sell an invention. The process for filing and obtaining a patent is complex, and an innovation must meet strict criteria in order to be patentable. Seeking advice from a patent agent is advisable.

Trade secrets are a form of IP right that may be used to protect a broad range of business information, such as the underlying technology of a software product, and can be a useful alternative to patent rights if the invention does not qualify for patent protection, or as a supplemental means of protection. There is no formal process for obtaining trade secret protection in Canada. Rather, the information will be protected and a trade secret will arise if:

- the information remains confidential and not generally known to the public;
- the business took reasonable steps to keep the information secret, such as through non-disclosure agreements; and
- the information is valuable because it is secret.

Canada has no legislation governing trade secrets. Rather, trade secrets are enforced through common law torts of breach of confidence or fiduciary duty and, where applicable, breach of contract.

A fintech's branding can be protected by way of trademark. Common law rights in a trademark may arise without formal registration through use of the mark. However, registration pursuant to the Trademarks Act (Canada) affords significant benefits.

8.1 How is innovation in the fintech space protected in your jurisdiction?

A number of incentive programmes are available in Canada to encourage investment in Canadian-based businesses and development of technology within Canada.

The Scientific Research and Experimental Development programme uses tax incentives to encourage Canadian businesses to conduct research and development (R&D) in Canada. Eligible businesses can obtain tax credits in respect of qualified R&D expenditures.

Canadian-controlled private corporations (CCPCs) may qualify for the small business deduction, which will reduce income tax payable. Other tax advantages are available to CCPCs.

The Strategic Innovation Fund, funded by the federal government, provides financial support to projects that will improve Canada's innovation performance while providing economic, innovation and public benefits to Canadians, and which meet certain criteria.

The National Research Council of Canada Industrial Research Assistance Program assists Canadian small and medium-sized businesses in taking ideas to market by providing advice, connections and funding.


Many federal and provincial grants and funding initiatives, as well as financing programmes, are also available to qualifying businesses.

In addition, the Canadian Securities Administrators, the umbrella organisation of the Canadian provincial and territorial securities regulators, has implemented a regulatory sandbox programme to support fintech businesses seeking to offer innovative products and services in Canada. The programme permits firms to register and/or obtain exemptive relief from securities laws requirements, under a quicker and more flexible process than through a standard application, in order to test their products and services on a time-limited basis in the Canadian market. Some provincial regulators have related programmes that operate within their particular jurisdictions to provide guidance and support to fintech businesses.

9. Talent acquisition

9.1 What is the applicable employment regime in your jurisdiction and what specific implications does this have for fintech companies?

With limited exceptions for federal works and undertakings such as banks, the provinces have jurisdiction with respect to employment law matters.



Each Canadian province has enacted employment standards legislation which provides minimum standards for the basic terms and conditions of employment, including:

- minimum wage levels;
- vacation and holiday pay;
- hours of work;
- leaves of absence (including maternity and parental leave);
- notice periods for termination; and
- in some jurisdictions, severance payments.

Employers and employees are not permitted to contract out of these prescribed minimum standards.

There is no 'employment at will' in Canada. Consequently, unless there is just cause for terminating an employee's employment, he or she is entitled to notice, or pay in lieu of notice, upon termination of his or her employment. The employer has the burden of proof to establish just cause for termination and whether there is just cause will depend on the facts of each particular circumstance.

An employer and an employee may enter into a written employment agreement that, among other matters, sets out the notice period that will apply upon termination without cause, which must not be less than (but may be limited to) the minimum period prescribed by employment standards legislation. If the employment agreement does not provide for an enforceable notice period, then the employee is entitled to a reasonable amount of notice pursuant to common law. Courts have assessed this by taking into account various factors, such as the employee's age, length of service, position, remuneration and inducements, and the current employment market. The length of common law notice periods in Canada tends to be more generous than employment standards minimums.


In addition, employers must comply with provincial human rights legislation, which prohibits discrimination on the basis of certain personal characteristics, such as race, gender and religion, and requires employers to take all reasonable steps to avoid a negative effect based on a personal characteristic.

9.2 How can fintech companies attract specialist talent from overseas where necessary?

Canadian citizens and newcomers to Canada with permanent resident status can work in Canada without a valid work permit. Fintech businesses planning to hire a foreign worker must go through one of several federal or provincial/territorial immigration programmes, such as the Temporary Foreign Workers Program or the International Mobility Program.

Typically, Canadian businesses must obtain a labour market impact assessment (LMIA) from Employment and Social Development Canada (ESDC) before hiring a foreign worker. In order to obtain an LMIA, the business must prove that there is no Canadian (or permanent resident) available to fill the position, and that a foreign worker is therefore required. Processing times for LMIA's can vary from weeks to months. Once obtained, the LMIA is provided to the foreign worker to submit with his or her work permit application.

However, in 2017 the Canadian government introduced the Global Talent Stream (GTS) programme, whereby the ESDC will expedite the processing of an LMIA if the position being hired is included on the ESDC's Global Talent Occupations List or if the hiring business has been referred by a designated referral partner on the basis that the position being requested requires unique and specialised talent to help the business scale up and grow. Under the GTS programme, LMIA applications are processed within two weeks, which is a significant time saving on regular LMIA applications.



The GTS programme is relevant to fintechs because the Global Talent Occupations List includes several technology-related positions, such as computer programmers, software engineers, database analysts and data administrators, information systems analysts and consultants designers, and web designers and developers.

10. Trends and predictions

10.1 How would you describe the current fintech landscape and prevailing trends in your jurisdiction? Are any new developments anticipated in the next 12 months, including any proposed legislative reforms?

Canada's developed financial services sector will likely continue to incentivise many fintech innovations. In particular, Canada has seen strong growth in businesses involving cryptocurrency, artificial intelligence and digital payments. Canada's government has set ambitious innovation goals, with several governmental programmes being created to encourage growth in this sector.

New developments are expected in the form of updated regulatory regimes that will better address the rapid technological innovation seen in the fintech space. Further clarity regarding the regulation of cryptoasset trading platforms is anticipated to be provided by securities regulators. The Canadian federal government has confirmed that it plans to introduce legislation to implement a new retail payments oversight framework, which may result in fintechs that are currently unregulated becoming subject to regulation, depending on their business activities. Amendments to the Proceeds of Crime (Money Laundering and Terrorist Financing Regulations, anticipated to come into force on 1 June 2020, will impose obligations on reporting entities with respect to virtual currency transactions.

In early 2019 the federal government released a consultation paper on a review of the merits of open banking, seeking comments from industry stakeholders. While recent elections in Canada have caused progress on this initiative to lag, industry participants are keen to see movement forward.

11. Tips and traps

11.1 What are your top tips for fintech players seeking to enter your jurisdiction and what potential sticking points would you highlight?

Given the split jurisdiction of federal and provincial regulation, and the fact that it will ultimately be the business activity of a fintech that determines the applicable regulatory framework, fintechs seeking to enter Canada should carefully consider, and obtain qualified advice with respect to, the regulations to which they will ultimately be subject.

Compliance with privacy legislation will be of primary importance, as privacy laws are widely applicable to any fintech which has possession of personal information.

Determining whether securities regulation applies to a fintech's activities is also of key importance, as securities regulation tends to apply to many facets of fintech business activities, including cryptoassets, roboadvising, peer-to-peer lending, trading activities and forex activities, among others. Where a fintech has an innovative idea that it wishes to test in market, discussions with securities regulators at an early stage will be warranted, as eligibility for regulatory sandbox programmes should be considered.

Finally, if a fintech's undertakes payment processing activities, registration with the Financial Transactions and Reports Analysis Centre of Canada as a money services business and compliance with anti-money laundering legislation may be required.



mondaq

Connecting knowledge & people

London | Bristol | Essex | New York | Sydney

t: +44 (0) 20 8544 8300
e: enquiries@mondaq.com