

Canada

Shane Pearlman

Borden Ladner Gervais, Toronto
spearlman@blg.com

Stephen Redican

Borden Ladner Gervais, Toronto
sredican@blg.com

Suhuyini Abudulai

Borden Ladner Gervais, Toronto
sabudulai@blg.com

Maria Nasr

Borden Ladner Gervais, Toronto
mnasr@blg.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation

Fintech activity is regulated through a combination of federal, provincial and territorial laws, codes of conduct and regulatory guidance, including in areas of financial services, payments, anti-money laundering (AML) law, securities, privacy, consumer protection and provincial lending/market conduct regimes, depending on the product, business model and parties involved.

Payment regulation under the Retail Payment Activities Act

The Retail Payment Activities Act² (RPAA) establishes a federal supervisory framework for payment service providers (PSPs). The regime is activity-based and applies where an individual or entity performs, as a service or business activity that is not incidental to another service or business activity, one or more of the following payment functions:

- providing or maintaining an account that, in relation to an electronic funds transfer, is held on behalf of one or more end-users;
- holding funds on behalf of an end-user until the funds are withdrawn by the end-user or transferred to another person or entity;
- initiating an electronic funds transfer at the request of an end-user;
- authorising an electronic funds transfer, or transmitting, receiving or facilitating a payment instruction relating to an electronic funds transfer; or
- providing clearing or settlement services.

Performing one of these functions does not, by itself, determine that the RPAA applies. The function must relate to an electronic funds transfer made in Canadian or another fiat currency, or using a prescribed unit, and must fall within the RPAA's geographic scope. The regime may apply to both Canadian PSPs and foreign PSPs that direct and provide covered services to end-users in Canada. The provider or activity must also not benefit from an applicable exclusion. These exclusions cover specified entities and activities, including certain regulated financial institutions, incidental payment functions, certain securities-related and closed-loop transactions, qualifying internal transactions among affiliated entities and payment functions performed using designated payment systems.

The Bank of Canada administers and enforces the RPAA. Its supervision focuses on operational risk management, incident response, safeguarding end-user funds and ongoing reporting. Although the regime is intended to reduce specified risks to end-users and foster confidence in payment services, it is not a comprehensive consumer protection or market conduct regime and does not provide a general mechanism for resolving disputes concerning fees, privacy or individual transactions.

Under the RPAA, a PSP must:

¹ This publication includes contributions by Iñaki Gomez, Candice Kloes, Jennifer Ponton, Frédéric Wilson, Graeme Hamilton and Angela Yang of Borden Ladner Gervais.

² SC 2021, c 23, s 177.

- register with the Bank of Canada;
- establish, implement and maintain a risk management and incident response framework that identifies and mitigates operational risks, detects and responds to incidents and supports recovery from incidents;
- assign appropriate governance responsibilities and resources, manage relevant third-party risks and support compliance through monitoring, testing, review and reporting;
- where it holds end-user funds, safeguard those funds against financial loss in the event of the PSP's insolvency and maintain reliable and timely access to them; and
- comply with ongoing reporting obligations, including updates to registration information, annual reporting, advance notice of significant changes or new activities and notification of material incidents to the Bank of Canada and affected persons or entities, as applicable.

AML and anti-terrorist financing (ATF) regime

The Proceeds of Crime (Money Laundering) and Terrorist Financing Act³ (PCMLTFA) and its regulations impose AML/ATF obligations on prescribed reporting entity sectors. Depending on its activities, a fintech business may be regulated as a money services business (MSB) or foreign money services business (FMSB), financial entity, securities dealer, financing or leasing entity or another prescribed reporting entity. The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) is responsible for administering and enforcing the regime.

Under the PCMLTFA and its regulations, reporting entities must:

- register with FINTRAC where the applicable reporting entity category is subject to a registration requirement, including MSBs and FMSBs;
- establish and maintain a compliance programme that satisfies applicable statutory and regulatory requirements, including the appointment of a compliance officer, written policies and procedures, a documented risk assessment, training and an effectiveness review;
- comply with identity verification and beneficial ownership requirements, including ongoing monitoring and enhanced measures for higher-risk clients and activities;
- comply with record-keeping and reporting obligations, including suspicious transaction reports, large cash transaction reports, large virtual currency transaction reports, electronic funds transfer reports, listed person or entity property reports and sanctions-related reporting, where applicable; and
- comply with the Travel Rule for electronic funds transfers and virtual currency transfers, which generally requires prescribed originator and beneficiary information.

Effective 26 March 2026, amendments to the PCMLTFA materially strengthened FINTRAC's compliance and enforcement framework. Reporting entities must now maintain compliance

3 SC 2000, c 17.

programmes that are reasonably designed, risk-based and effective. The amendments also increased maximum administrative monetary penalties and introduced compliance orders and mandatory compliance agreements for prescribed violations. FINTRAC is developing guidance on these changes. Once additional regulations come into force, a separate universal enrolment regime will require reporting entities not already subject to registration to enrol with FINTRAC, with further implementation guidance from FINTRAC expected.

Sanctions

Canada's federal sanctions regime, which applies to persons in Canada and Canadians outside Canada, is established under the United Nations Act,⁴ Special Economic Measures Act⁵ and Justice for Victims of Corrupt Foreign Officials Act ('Sergei Magnitsky Law').⁶ Depending on the applicable regulations, sanctions may target listed individuals and entities, or impose broader country-wide or sectoral restrictions, including prohibitions concerning particular jurisdictions, financial services, transactions, goods, technology or other activities.

Reporting entities under the PCMLTFA may have separate and concurrent obligations to:

- file a suspicious transaction report with FINTRAC where there are reasonable grounds to suspect that a completed or attempted transaction relates to a sanctions-evasion offence;
- submit a Listed Person or Entity Property Report to FINTRAC where terrorist or sanctioned property must be disclosed under applicable legislation; and
- comply with any additional disclosure or reporting obligations under the relevant sanctions legislation or regulations, including reporting suspected sanctions violations to the Royal Canadian Mounted Police.

Sanctions-related disclosure and reporting obligations may apply concurrently. Under most regulations made under the United Nations Act and the Special Economic Measures Act, persons in Canada and Canadians outside Canada must disclose, without delay, any property in their possession or control that they have reason to believe is owned, held or controlled by or on behalf of a listed or designated person, together with information about any transaction or proposed transaction involving that property. Disclosure must be made to the Royal Canadian Mounted Police or, where permitted by the applicable regulation, to the Director of the Canadian Security Intelligence Service.

Reporting entities under the PCMLTFA have additional obligations. Where a reporting entity is required to disclose terrorist or sanctioned property under the Criminal Code of Canada or applicable sanctions legislation, it must also submit a Listed Person or Entity Property Report to FINTRAC. Separately, it must file a suspicious transaction report where there are reasonable grounds to suspect that a completed or attempted transaction relates to the commission or attempted commission of a sanctions evasion offence. These FINTRAC reporting obligations are additional to, and do not replace, the underlying disclosure requirements under Canadian sanctions legislation.

4 RSC, 1985, c U-2.

5 SC 1992, c 17.

6 SC 2017, c 21.

Securities laws

Securities and derivatives regulation in Canada falls principally within provincial and territorial jurisdiction. The Canadian Securities Administrators (CSA) coordinates policy and regulatory initiatives among the provincial and territorial regulators, while the Canadian Investment Regulatory Organisation (CIRO) is the national self-regulatory organisation overseeing investment dealers, mutual fund dealers and trading activity on Canadian debt and equity marketplaces.

The application of securities laws to a fintech business depends on the nature of its products and services, the manner in which they are offered and the jurisdictions in which the business operates. The following provides an overview of how common fintech businesses are regulated through Canadian securities regulations.

Robo-advisers

Registered portfolio managers that provide discretionary investment management services through online or automated platforms remain subject to the same applicable registration, conduct and compliance requirements as portfolio managers using traditional service-delivery models.

CSA Staff Notice 31-342, Guidance for Portfolio Managers Regarding Online Advice confirms that NI 31-103 is technology-neutral and that there is no separate exemption for online advice. Online advisers (such as robo-advisers) must therefore comply with core adviser obligations, including know-your-client, know-your-product and suitability requirements, as well as applicable supervision, disclosure, record-keeping and compliance obligations, with registered advising representatives retaining responsibility for the advice and suitability determinations provided to clients.

Online lenders

Peer-to-peer and other online lending platforms may be subject to certain requirements under securities law, where the lending arrangement involves a distribution of securities or investment opportunities to investors. Depending on the structure of the arrangement, applicable requirements may include dealer registration, compliance with prospectus requirements or reliance on available prospectus exemptions, and restrictions on distributions to eligible or accredited investors.

Crowdfunding

The CSA has introduced a harmonised national framework, National Instrument 45-110 – Start-up Crowdfunding Registration and Prospectus Exemptions ('NI 45-110'), which provides a prospectus exemption that permits eligible issuers to distribute eligible securities through an online funding portal, as well as a dealer-registration exemption for funding portals that satisfy the applicable conditions.

NI 45-110 is intended to facilitate capital raising by startups and other early-stage issuers. Among other measures, it increased the investment limits applicable to distributions under the startup crowdfunding prospectus exemption and raised the maximum aggregate amount that an issuer

group may raise under the exemption in a 12-month period from CAD 500,000 to CAD 1.5m. A purchaser may generally invest up to CAD 2,500 in a distribution or up to CAD 10,000 where a registered dealer has determined that the investment is suitable for the purchaser.

Distributed ledger technology and blockchain

Fintech businesses that use distributed ledger technology, including public or permissioned blockchains, may be subject to securities or derivatives laws where their activities involve offering or distributing, trading in or advising in securities or derivatives; operating a marketplace or clearing agency; or otherwise carrying on an activity regulated under applicable securities or derivatives legislation. The applicable requirements depend on the substance of the assets, arrangements and activities involved, rather than the technology used.

Crypto trading platforms and crypto asset offerings

Canadian securities laws may apply either because a crypto asset is itself a security or derivative or because the arrangement through which it is offered, traded or held constitutes a security or derivative, including a 'crypto contract'. This analysis is fact-specific and focuses on the substance of both the asset and the surrounding arrangement rather than their form or description.

In recent years, the CSA has issued guidance on crypto asset offerings, disclosure by crypto asset reporting issuers and the application of securities legislation to crypto asset trading platforms. Depending on their activities and operating models, these platforms may be subject to dealer registration; CISO membership; marketplace or clearing-agency requirements or exemptive relief; and requirements relating to custody, client asset protection, disclosure and conduct. The CSA has also amended the investment fund regulatory framework to address funds that invest directly or indirectly in crypto assets. The CSA has further noted that fintech businesses involved in crypto assets should consider whether they must be registered as exchanges or alternative trading systems.

Crypto and other digital assets

Canada does not regulate crypto assets under a single, comprehensive statute. Their legal treatment instead depends on the nature of the asset, the rights and obligations attached to it, the manner in which it is offered, traded or held and the activities carried on by the relevant business.

In 2026, CISO introduced a Digital Asset Custody Framework for its dealer members. The framework distinguishes between crypto assets and tokenised assets. A crypto asset is a digital asset that is not a tokenised asset, while a tokenised asset is a digital representation of a traditional financial asset that confers legal rights and obligations equivalent to those associated with the underlying asset or instrument. Tokenised assets may include digital representations of deposits, debt, equity and other financial instruments, as well as certain fiat-referenced stablecoins.

Tokenisation does not displace the legal regimes applicable to the underlying asset or instrument and may engage additional regulatory requirements. The digital form of these assets also introduces

distinct custody risks, including risks associated with private-key management, transfers and transaction finality.

Pursuant to the Currency Act,⁷ crypto assets are not treated as legal tender in Canada. The CSA and CIRO have acknowledged that certain well-established virtual currencies, such as bitcoin, that function as a means of payment or exchange on a decentralised network are generally not securities or derivatives on that basis alone. They are rather akin to an intangible ‘commodity’, the value of which fluctuates based on the market.

Nonetheless, a crypto asset may itself constitute a security or derivative under provincial or territorial legislation. In addition, the contractual arrangement through which a crypto asset is offered, traded or held may independently constitute a security or derivative, including a ‘crypto contract’. In assessing these arrangements, Canadian securities regulators focus on their substance rather than their form or description.

Separate AML/ATF regime requirements may also apply. A person or entity providing prescribed virtual currency services may be required to register with FINTRAC as an MSB or FMSB. Where applicable, the business must comply with the PCMLTFA and its regulations, including requirements relating to its compliance programme, identity verification, record-keeping, transaction reporting and the Travel Rule.

Stablecoins

The CSA generally refers to stablecoins as value-referenced crypto assets (VRCAs) and has stated that VRCAs may constitute securities and/or derivatives in certain jurisdictions. Under CSA Staff Notice 21-333 Crypto Asset Trading Platforms: Terms and Conditions for Trading Value-Referenced Crypto Assets with Clients, the CSA may provide written consent, on an interim basis and subject to specified conditions, for a registered crypto asset trading platform, or a platform operating under a pre-registration undertaking, to allow clients to buy or deposit certain fiat-backed VRCAs or enter into related crypto contracts. This interim approach does not constitute approval of a VRCA, a guarantee of its safety, or a determination that the VRCA or its issuer complies with, or falls outside, applicable securities legislation.

The federal Stablecoin Act⁸ establishes a separate framework, administered by the Bank of Canada, for issuers of stablecoins designed to maintain a stable value relative to a single fiat currency. Once the relevant provisions are brought into force, issuers within the Stablecoin Act’s scope will be required to register with the Bank of Canada and comply with requirements concerning redemption, reserve assets, governance and operational policies, information provision and regulatory reporting. The Stablecoin Act also prohibits issuers from paying interest or yield to stablecoin holders and from representing a stablecoin as legal tender, a deposit or an insured product. The Stablecoin Act has been enacted, but is not yet in force, and its operation will depend on forthcoming regulations.

⁷ RSC, 1985, c C-52.

⁸ SC 2026, c 3, s 600.

Unlike the CSA's interim platform-focused approach, the Stablecoin Act establishes an issuer-focused federal framework. Its enactment does not, by itself, determine whether a particular stablecoin or related arrangement constitutes a security or derivative under provincial securities legislation.

Consumer-driven banking

Canada has enacted the Consumer-Driven Banking Act⁹ (CDBA) as the legislative foundation for a regulated consumer-driven banking, or 'open banking', framework. Overseen by the Bank of Canada, the framework will allow individuals and businesses to direct participating entities to share prescribed financial data securely with accredited service providers through application programming interfaces (APIs). The CDBA received Royal Assent on 26 March 2026, but significant provisions are not yet in force. Proposed Consumer-Driven Banking Regulations, published on 27 June 2026, remain subject to finalisation.

The Bank of Canada will administer accreditation, maintain a public registry of participating entities and accredited third-party service providers and supervise compliance. Once the relevant provisions and implementing regulations are in force, participants will be subject to requirements concerning consent, authentication, security, liability, complaints, record-keeping, regulatory reporting and data sharing. Under the proposed regulations, participants would also be required to:

- retain prescribed compliance records electronically, generally for five years;
- report breaches of security safeguards involving consumer data to the Bank of Canada and notify affected consumers where there is a risk of significant harm;
- maintain records of consumers' express consent;
- verify a counterparty's status and any applicable conditions through the Bank of Canada's registry before sharing data; and
- meet technical service standards, including proposed monthly API availability of 99.5 per cent and reasonable response times consistent with generally accepted standards.

The CDBA also contemplates prohibiting screen scraping, which involves accessing financial data using a consumer's online banking credentials. However, the prohibition is not yet being brought into force, and its timing and scope remain subject to further policy development. Canada's initial framework is expected to focus on secure, consumer-authorised, 'read-only' data sharing rather than payment initiation or other account actions.

Prudential banking regulatory framework

At the federal level, the Office of the Superintendent of Financial Institutions (OSFI) supervises and regulates banks, insurance companies and trust and loan companies. OSFI generally does not directly regulate standalone fintechs unless they are themselves federally regulated financial institutions (FRFIs). However, OSFI's expectations are relevant where fintechs partner with or

9 SC 2026, c 3, s 224.

provide services to FRFIs, including in relation to lending, custody, payments, deposit products or technology outsourcing.

Under OSFI's Third-Party Risk Management Guideline (the 'OSFI Guideline'), FRFIs are expected to manage risks arising from all third-party arrangements while retaining accountability for any business activities, functions or services outsourced to a third party. The OSFI Guideline adopts a risk-based approach and expects FRFIs to manage third-party risk in a manner proportionate to the level of risk and complexity of their third-party ecosystem. It also introduces the concept of 'criticality', which refers to the importance of a third-party arrangement to the FRFI's operations, strategy, financial condition or reputation, and focuses on the impact of a risk event regardless of the likelihood of that event occurring.

In assessing risk and criticality, FRFIs should consider factors such as:

- the likelihood of a third party or its subcontractors failing to meet expectations due to insolvency or operational disruption;
- the third party's use of subcontractors;
- the FRFI's ability to assess the third party's controls;
- the substitutability and financial health of the third party; and
- other relevant risks associated with the arrangement.

OSFI also expects FRFIs to assess the risk and criticality of a third-party arrangement throughout its lifecycle, including before entering into the arrangement; regularly during the arrangement at a frequency and scope proportionate to its criticality; and after any material change to the arrangement.

Privacy, cybersecurity and data governance

Canada's Personal Information Protection and Electronic Documents Act¹⁰ (PIPEDA) is the federal private-sector privacy law governing the collection, use and disclosure of personal information in the course of commercial activities. Among other requirements, organisations must obtain meaningful consent and may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances. They must also protect personal information using physical, organisational and technological safeguards that are proportionate to the sensitivity of the information.

The proposed Bill C-36, Protecting Privacy and Consumer Data Act¹¹ (PPCDA) would introduce additional privacy obligations, including provisions addressing the use of personal information in automated decision-making. The PPCDA uses the term 'automated decision system' to describe technology that assists or replaces human judgement in decision-making. This definition

¹⁰ SC 2000, c 5.

¹¹ Bill C-36, an Act to enact the Protecting Privacy and Consumer Data Act, to amend the Personal Information Protection and Electronic Documents Act and to make amendments to other Acts, 1st Session, 45th Parliament, 2026, online: First Reading (15 June 2026).

encompasses rules-based systems, regression analysis, predictive analytics, machine learning, deep learning, neural networks and other techniques.

Under the PPCDA, an individual would be entitled to request an explanation of a decision, recommendation or prediction made using an automated decision system where it could have a significant impact on the individual. The explanation would be required to identify the personal information used by the system, the source of that information and the principal factors that led to the decision, recommendation or prediction. Organisations would also be required to make readily available, in plain language, a general account of how they use automated decision systems to make decisions, recommendations or predictions about individuals that could have significant impacts on them.

In the open banking context, one of the most significant features of the proposed PPCDA is the data mobility right. If enacted, this right would allow an individual to request that an organisation transfer personal information collected from or about the individual to another organisation designated by the individual, provided that both organisations are subject to an applicable data mobility framework. The privacy and consumer-driven banking regimes are therefore intended to operate together. Privacy legislation would establish the individual's legal right to direct the transfer of their personal information, while the consumer-driven banking framework would provide the sector-specific legal, technical and operational infrastructure through which that transfer occurs.

Consumer protection and lending laws

Consumer protection in Canada is a shared federal, provincial and territorial responsibility. Federal legislation governs matters such as competition, deceptive marketing, product safety, packaging and labelling and consumer protection in federally regulated sectors, including banking and telecoms. Provincial and territorial laws generally regulate consumer contracts, unfair practices, credit disclosure, remedies and the licensing of specified businesses, particularly where consumer credit is involved.

In the fintech context, consumer protection and lending laws are particularly relevant to online lending, buy-now-pay-later products, digital credit products, payment services and embedded finance arrangements. Depending on the product and province, fintech businesses may need to comply with cost of credit disclosure requirements, licensing or registration requirements for lending or brokering activities, rules governing internet agreements and electronic disclosure and restrictions on fees, interest, cancellation rights and collections practices. Where fintechs partner with FRFIs, the applicable federal financial consumer protection framework may also be relevant, including disclosure, complaint handling and market conduct obligations.

Payments Canada and payments infrastructure

Payments Canada, the operating name of the Canadian Payments Association, is the member-funded organisation responsible for Canada's principal national payment clearing and settlement infrastructure. It owns and operates Lynx, Canada's real-time gross settlement system for high-value payments, and the Automated Clearing Settlement System (ACSS), which clears retail payment items, including cheques, pre-authorised debits, direct deposits and certain point-of-sale payments. Payments Canada is also developing the Real-Time Rail (RTR), a real-time exchange, clearing and

settlement system for instant, data-rich payments that is scheduled to launch in the fourth quarter of 2026.

Under the Canadian Payments Act¹² (CPA), Payments Canada is mandated to establish and operate national payment systems; facilitate their interaction with other payment systems; and promote their efficiency, safety and soundness while taking users' interests into account. Banks, authorised foreign banks and the Bank of Canada are mandatory members. Recent amendments expanded membership eligibility to include registered PSPs under the RPAA; certain local credit unions; and operators of clearing and settlement systems designated under the Payment Clearing and Settlement Act¹³ (PCSA). This infrastructure regime is distinct from, but interacts with, the RPAA framework discussed above, as registered PSPs under the RPAA may become eligible for Payments Canada membership, but must still satisfy applicable system participation requirements.

Membership in Payments Canada does not, by itself, entitle an institution to participate in every payment system. Prospective participants must separately satisfy the operational, technical, security, settlement and risk management requirements applicable to each system. For the RTR, the participation framework, including eligibility, settlement arrangements and ongoing compliance requirements, is established under the Canadian Payments Association By-law No 10¹⁴ and the related RTR rules.

Interac Corp separately operates Interac e-Transfer, a widely used electronic funds transfer service available through participating Canadian financial institutions. Under the PCSA, the Bank of Canada oversees clearing and settlement systems that have been formally designated for oversight. Lynx is designated as a systemically important payment system, while the ACSS and Interac e-Transfer are each designated as prominent payment systems. Interac e-Transfer has been subject to the Bank of Canada's oversight since 10 August 2020 and must comply with the Bank of Canada's risk management standards for prominent payment systems. Oversight is system-specific and does not automatically extend to every system operated by Payments Canada or Interac Corp.

Competition law

Fintech businesses operating in Canada may also be subject to the federal Competition Act,¹⁵ which applies broadly across industries and addresses both criminal offences and conduct subject to civil review.

In the fintech context, the Competition Act is particularly relevant to misleading advertising and other deceptive marketing practices, agreements and other arrangements between market participants; abuse of dominance; and merger review.

The Competition Bureau, led by the Commissioner of Competition (the 'Competition Commissioner'), investigates potential contraventions and may seek remedies before the Competition Tribunal or a court, where applicable. Private parties may also seek leave to bring applications before the Competition Tribunal in respect of certain reviewable practices, including

12 RSC, 1985, c C-21.

13 SC 1996, c 6, Sch.

14 SOR/2026-133.

15 RSC, 1985, c C-34.

misleading advertising, abuse of dominance, anti-competitive collaborations, price maintenance, exclusive dealing, tied selling and refusal to deal.

The Competition Act prohibits representations to the public that are materially false or misleading, assessed by reference to both their literal meaning and the general impression they convey. It also addresses specific marketing practices, including drip pricing (also known as 'junk fees'), ordinary selling price and other savings claims, false testimonials and performance claims that are not based on adequate and proper testing. These provisions may be relevant to representations concerning fees, pricing, savings, product performance, security, speed, accessibility and other features of fintech products or services.

Non-compliance with the deceptive marketing provisions of the Competition Act can result in significant consequences. This includes prohibition and corrective notice orders and, for a corporation, an administrative monetary penalty of up to the greater of CAD 10m or three per cent of its annual worldwide gross revenues. A subsequent order may attract a higher fixed maximum. Where a false or misleading representation is made knowingly or recklessly, the conduct may attract criminal liability, including, on conviction on indictment, a fine in the discretion of the court, imprisonment for up to 14 years or both.

The Competition Act also prohibits certain agreements between competitors, including agreements to fix prices, allocate customers or markets, or restrict supply, as well as certain wage-fixing and no-poach agreements between unaffiliated employers. Other agreements or arrangements may be reviewed civilly where they are likely to prevent or lessen competition substantially. The civil regime applies to agreements between competitors and may also apply to agreements between non-competitors where a significant purpose of the agreement or arrangement, or any part of it, is to prevent or lessen competition in a market and the agreement or arrangement is likely to prevent or lessen competition substantially.

Other civilly reviewable practices include abuse of a dominant position and certain vertical arrangements, such as price maintenance, tied selling, exclusive dealing and refusal to deal. These provisions may be relevant to fintech businesses that operate digital platforms; control access to commercially important data or infrastructure; impose exclusivity requirements; or restrict interoperability or access by customers, suppliers or competitors.

Mergers that exceed prescribed thresholds generally require pre-closing notification to the Competition Bureau. However, the Competition Commissioner may review and challenge both notifiable and non-notifiable mergers where they are likely to prevent or lessen competition substantially. Notified mergers may generally be challenged within one year after closing, while mergers that were not notified may generally be challenged within three years after closing. The Competition Tribunal may order remedies, including blocking, dissolving or imposing conditions on a merger.

Canada's approach to artificial intelligence (AI) regulation

Canada does not currently have a comprehensive private-sector AI statute in force, although the establishment of a federal Minister of Artificial Intelligence and Digital Innovation and the release

of Canada's national AI strategy, AI for All, reflect the federal government's continuing focus on AI governance, adoption and innovation.

In the absence of a comprehensive federal AI statute, private-sector use of AI is regulated through generally applicable privacy, consumer protection, human rights, intellectual property (IP) and sector-specific laws, supplemented by voluntary standards, codes of conduct and regulatory guidance. For fintech businesses, the applicable requirements depend principally on the function performed by the AI system and the regulatory regime governing that function. For example, AI-enabled fraud monitoring may engage PCMLTFA and sanctions requirements; automated credit scoring and lending decisions may engage consumer protection, lending, privacy and human rights laws; robo-advice and investor profiling may engage securities regulation; and AI used in payment services or consumer-driven banking may intersect with the RPAA, privacy, cybersecurity and consumer-driven banking requirements.

AI products and services used by FRFIs may also engage OSFI's expectations concerning model risk, technology and cyber risk, operational resilience and third-party risk management. In July 2026, OSFI published a technology risk bulletin addressing the implications of generative and agentic AI under its existing guidance. Its model risk management guideline, which expressly encompasses AI and machine learning methods, is scheduled to take effect on 1 May 2027.

Quebec's Act respecting the protection of personal information in the private sector¹⁶ is relevant where fintech products process personal information about individuals in Quebec, particularly in connection with profiling or automated decision-making. It imposes specific transparency obligations for profiling technologies and rights relating to decisions based exclusively on automated processing, including rights to information about the decision and to submit observations for review.

Other relevant regulatory developments

Recent legislative developments relevant to Canada's fintech sector include the proposed PPCDA, discussed above, Ontario's forthcoming consumer protection regime and the proposed establishment of a federal Financial Crimes Agency.

Ontario's Consumer Protection Act 2023¹⁷ has received Royal Assent, but is not yet in force. Once proclaimed in force, it will replace the existing Consumer Protection Act 2002¹⁸ and introduce revised requirements governing unfair practices, consumer contracts, credit agreements, disclosure obligations and consumer remedies. The scope and practical application of the new regime will also depend on forthcoming regulations. For fintech businesses dealing with Ontario consumers, the new framework is relevant to online contracting, digital credit products, payment services, subscription or recurring-payment models, disclosure practices, cancellation rights and other consumer-facing features of financial technology products.

At the federal level, the Canadian Government has introduced legislation to establish a Financial Crimes Agency as a specialised federal law enforcement body responsible for investigating serious

¹⁶ CQLR, c P-39.1.

¹⁷ SO 2023, c 23, Sch 1.

¹⁸ SO 2002, c 30, Sch A.

and complex financial crimes, and contributing to the recovery of proceeds of crime. The legislation has not yet been enacted. The proposed definition of 'financial crime' is broad, encompassing offences relating to financial assets, including digital assets, financial services and markets, proceeds of crime and Canada's federal AML/ATF regime. For fintech businesses, the proposed agency signals heightened enforcement attention to risks involving digital assets, payment services, fraud, money laundering, sanctions evasion and other forms of technology-enabled financial crime.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated

As discussed above, Canada does not regulate crypto assets under a single comprehensive statute. The applicable legal framework depends on the nature of the asset, the manner in which it is offered, traded or held and the activities carried on by the relevant business. Crypto assets are not legal tender in Canada. Certain well-established virtual currencies, such as bitcoin, may not qualify as securities or derivatives where they function as a means of payment or exchange on a decentralised network. However, crypto assets and related arrangements may become subject to provincial or territorial securities and derivatives laws where they constitute securities, derivatives or crypto contracts, including where a platform retains custody or control of the asset on a client's behalf and the client's contractual right to the asset constitutes a security or derivative.

Accordingly, crypto asset businesses may be subject to several overlapping regulatory regimes, including provincial and territorial securities laws and CSA or CIRO guidance relating to crypto trading platforms, investment funds with crypto exposure, crypto asset offerings and digital asset custody. Depending on the business model and activities involved, payment, privacy, consumer protection, sanctions and other regulatory requirements may also apply.

Investor protection is addressed primarily through securities regulation, including registration, disclosure, custody, segregation of client assets, suitability or appropriateness obligations, risk acknowledgment, product due diligence and restrictions on leverage or margin, depending on the platform and product. AML/ATF and Travel Rule obligations under the PCMTLFA applicable to crypto asset transactions are addressed separately in point 7.

Canada has explored, but has not launched, a central bank digital currency (CBDC). The Bank of Canada conducted research and public consultations concerning a potential digital Canadian dollar, including its possible design, technological architecture, economic and financial system implications and associated legal and regulatory requirements. The Bank of Canada has since scaled down its work on a retail CBDC and shifted its focus to broader payments system research and policy development. The Bank of Canada continues to monitor global CBDC developments and broader payments system issues.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets

As discussed in point 1, PSPs and digital wallet providers operating in Canada may be subject to several overlapping federal and provincial regimes, depending on the activities they perform, the products offered and the parties involved. The most directly relevant federal framework is the

RPAA, which requires certain non-bank PSPs performing retail payment activities to register with the Bank of Canada and comply with operational risk management, incident response, safeguarding of end-user funds and reporting obligations.

The RPAA applies on an activity-based rather than an entity-based basis. The payment functions within scope include providing or maintaining an account for end-users in relation to an electronic funds transfer; holding end-user funds until they are withdrawn or transferred; initiating electronic funds transfers at an end-user's request; authorising or transmitting payment instructions; and providing clearing or settlement services. A business that performs one or more of these functions as a service or business activity may be subject to the RPAA if its retail payment activities have the required connection to Canada and no statutory exclusion applies.

This analysis is particularly relevant to payment processors and digital wallet providers, which are identified in official RPAA guidance as examples of PSPs that may be subject to the regime. Other payment-related business models, such as merchant acquiring, payment facilitation, stored-value wallets or embedded payments, may also fall within the regime where the provider performs one or more regulated payment functions. Depending on the business models and activities, PSPs and digital wallet providers may also need to consider the AML/ATF regime, consumer protection, privacy and cybersecurity, OSFI third-party risk management and Payments Canada access requirements discussed in point 1.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support

Canada's securities regulators support fintech innovation through nationally coordinated initiatives and programmes administered by individual provincial regulators. At the national level, the CSA operates the CSA Financial Innovation Hub ('FinHub'), which supports innovation in Canada's capital markets where it may benefit investors. Through FinHub, the CSA engages with emerging technologies and innovative business models, assesses their regulatory implications and considers whether existing securities regulation should be adapted to accommodate market developments.

Individual provincial regulators also maintain innovation initiatives. In Ontario, the Ontario Securities Commission (OSC) operates OSC TestLab, which facilitates the testing of capital markets innovations and new regulatory approaches, and OSC LaunchPad, which assists eligible fintech businesses in understanding and navigating Ontario securities law requirements. In Alberta, the Alberta Securities Commission's Innovation in Finance team coordinates the regulator's fintech and capital markets innovation initiatives. Separately, Alberta's Financial Innovation Act¹⁹ establishes a broader regulatory sandbox through which eligible financial services and fintech businesses may test innovative products or services under temporary exemptions from specified provincial regulatory requirements. Businesses participating in the sandbox remain subject to terms and conditions intended to protect consumers.

19 SA 2022, c F-13.2

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking

As discussed in point 1, Canada has enacted the CDBA, which provides the legislative foundation for its consumer-driven banking framework. The proposed Consumer-Driven Banking Regulations²⁰ were subsequently published to support the implementation of the CDBA and establish detailed requirements relating to accreditation, consent and authentication, data sharing, security safeguards and breach reporting, record-keeping, transparency, technical standards, national security reviews, regulatory assessments and violations.

The proposed regulations were published in the Canada Gazette, Part I, on 27 June 2026, with the public consultation period closing on 26 August 2026. The framework is expected to be implemented in stages following the final publication of the regulations in the Canada Gazette, Part II. Although the precise commencement dates have not yet been established, the Regulatory Impact Analysis Statement for the proposed regulations indicates that the full suite of regulations is intended to come into force within one year after final publication.

6. Regulation of virtual asset service providers

Canada does not regulate virtual asset service providers (VASP) under a single standalone 'VASP' regime. The applicable requirements are activity-based and may arise under several overlapping federal, provincial and territorial regulatory regimes.

Businesses that exchange, transfer or otherwise deal in virtual currency may be required to register with FINTRAC as an MSB or FMSB and comply with AML/ATF requirements, including the compliance programme, client identification, record-keeping, reporting and Travel Rule obligations under the PCMLTFA. PSPs and digital wallet providers may also be subject to registration and supervisory requirements under the RPAA where they perform retail payment activities. Platforms that offer, trade or custody, or facilitate transactions in crypto assets may be subject to provincial and territorial securities laws, together with applicable CSA and CIRO requirements, and guidance where the relevant assets or arrangements constitute securities, derivatives or 'crypto contracts'.

The principal regulatory and enforcement authorities depend on the activities undertaken. FINTRAC administers and enforces the federal AML/ATF regime, the Bank of Canada supervises PSPs subject to the RPAA and provincial and territorial securities regulators, together with CIRO acting within its mandate, oversee securities and derivatives-related activities. Law enforcement and other regulatory authorities may also become involved where the relevant conduct raises criminal, fraud, sanctions or other compliance and enforcement concerns.

7. AML and the Travel Rule in crypto asset transactions

Under the PCMLTFA and its regulations, Canada has implemented AML/ATF and Travel Rule requirements for certain businesses providing virtual currency services, including a Travel Rule for virtual currency transfers. FINTRAC's published guidance explains how reporting entities are expected to comply with these statutory and regulatory requirements.

²⁰ 2026, 160 Canada Gazette, Part I, online: Consumer-Driven Banking Regulations.

Canada does not use VASP as a standalone registration category. Businesses providing prescribed virtual currency services may be required to register with FINTRAC as an MSB or FMSB, depending on its activities and connection to Canada. Registered MSBs and FMSBs are subject to requirements relating to compliance programmes, identity verification, record-keeping, transaction reporting and the Travel Rule.

The Travel Rule applies to virtual currency transfers for which a prescribed transfer record must be kept and does not distinguish between domestic and cross-border transfers. Identity verification is a related but separate obligation that arises in prescribed circumstances, including when an entity transfers or remits virtual currency equivalent to CAD 1,000 or more or receives virtual currency equivalent to CAD 10,000 or more.

When sending a virtual currency transfer subject to the Travel Rule, the MSB or FMSB must include the originator's and beneficiary's name, address and account or other reference number, if any. When receiving such a transfer, MSBs and FMSBs must take reasonable measures to ensure that the required information accompanies it and must not remove information received with the transfer. If required information is missing, the recipient must take reasonable measures to obtain it and apply written, risk-based policies governing whether the transfer will be permitted, suspended or rejected.

Under the PCMLTFA, MSBs and FMSBs may also be required to report large virtual currency transactions. A report is generally required where a reporting entity receives virtual currency equivalent to CAD 10,000 or more in a single transaction or in multiple transactions aggregated under the applicable 24-hour rule.

FINTRAC administers and enforces the PCMLTFA regime and supervises MSB and FMSB compliance with these obligations.

8. Enforcement and cross-border recognition of tokenisation and structuring of secured transactions involving crypto assets

In Canada, tokenised asset structures generally remain subject to the legal regimes applicable to the underlying asset or instrument. The process and challenges for tokenising real-world assets depend on the asset involved and the rights represented by the token. For example, because Canadian land title registries are not connected to blockchain networks, tokenised real estate would typically be structured through an entity that holds title to the real property, with tokenised units representing contractual or ownership interests in that entity rather than direct title to the land. Personal property security legislation in Canada does not currently expressly include reference to cryptocurrency, and it is most likely to fall under the definition of 'intangible property'. In common law provinces, security over intangible personal property is generally created by a security agreement and perfected by registration under the applicable personal property security legislation. Where crypto assets are used as collateral, practical custody and control measures, such as custody arrangements, wallet controls, control agreements or access to private keys, may also be relevant.

On default, enforcement of a security interest would generally proceed under the applicable provincial secured transactions regime and the relevant security documents, subject to any insolvency proceedings, statutory requirements and court supervision. In common law provinces,

secured creditors may generally have remedies such as seizure, disposition of collateral and collection of proceeds. A public auction is not necessarily required if the secured party complies with applicable personal property security legislation, including any commercially reasonable disposition requirements. Direct appropriation of collateral may be available only in limited circumstances and subject to applicable statutory requirements and debtor or third-party rights. Canadian courts generally recognise and enforce foreign governing law and jurisdiction clauses where they are bona fide, legal, sufficiently clear and not contrary to public policy. There is no separate Canadian conflict-of-laws rule specific to crypto asset contracts, although crypto-related case law suggests that enforceability may depend on the wording of the clause, the parties and agreements involved, and any applicable consumer protection, securities law, unconscionability or public policy considerations. This is discussed further in point 9.

9. Litigation and jurisdiction on crypto assets: legal implications of disputes involving crypto assets

Canadian courts have not adopted a crypto-specific framework for crypto asset disputes. In *Shirodkar v Coinbase Global Inc*, the Ontario Court of Appeal provided guidance on the limits of Ontario courts' jurisdiction over international digital asset platforms and underscored that mere access to a global internet platform from Ontario is not enough to ground jurisdiction over foreign corporate defendants. The decision reinforces that the jurisdictional analysis remains entity-specific and fact-specific, particularly where different corporate entities are involved in operating a global platform. The analysis may include which entity contracted with the user, the governing law and forum selection provisions in the applicable user agreement, whether the foreign entity was carrying on business in Ontario and whether there is a real and substantial connection between the dispute and the forum. Accordingly, while crypto-asset disputes may raise practical cross-border issues involving platform structures, asset tracing and enforcement, virtual accessibility alone may not necessarily establish Ontario jurisdiction over foreign crypto platforms.

For enforcement of crypto asset-related contracts, Canadian courts generally apply ordinary contract, civil procedure and remedies principles. Depending on the facts, disputes may involve enforcement of platform terms, user agreements, transfer instructions, custody arrangements, investment or trading arrangements or agreements relating to the purchase, sale or holding of digital assets. Canadian courts have treated crypto assets as property or property-like interests capable of supporting traditional civil remedies, including proprietary claims, preservation orders, tracing-related relief and recovery remedies.²¹ As a result, while crypto assets may raise practical enforcement issues, the legal analysis generally turns on the relevant contractual terms, the parties involved, the nature of the asset and the ordinary requirements for the remedy sought.

Intellectual property (IP) and crypto assets: legal protection, ownership, enforcement and monetisation of IP rights related to digital and virtual assets.

²¹ See, eg, *Copytrack Pte Ltd v Wall* 2018 BCSC 1709 (cryptocurrency treated as property capable of supporting proprietary claims and recovery remedies); *Shair.com Global Digital Services Ltd v Arnold* 2018 BCSC 1512 (civil claims involving digital assets and contractual/equitable remedies); *Cicada 137 LLC v Medjedovic* 2021 ONSC 8581 (interim preservation and tracing-related relief in respect of crypto assets); *Aquilini v Doe* 2022 BCSC 1925 (orders and remedies in crypto fraud claims against unknown defendants); and *Piroozzadeh v Persons Unknown Responsible for the Transformation of Cryptocurrency Accounts* 2023 ONSC 4920 (recovery and tracing-related relief involving crypto assets).

In Canada, innovations and inventions relating to digital and virtual assets are protected under the ordinary IP framework, including patents for eligible technical inventions; copyright for software code and other original works; trademarks for brands; industrial designs for visual features; and trade secrets or confidential information for proprietary algorithms, models, datasets and know-how. Ownership and commercialisation of IP rights are generally determined by statute and contract, including employment agreements, contractor agreements, assignments, licence terms and platform terms. Ownership of a crypto asset or non-fungible token (NFT) does not, by itself, confer ownership of any copyright, trademark or other IP associated with the token or its underlying content. Those rights remain with the applicable rights holder unless they are expressly transferred by assignment or made available under a licence. IP rights may be enforced through platform-based enforcement mechanisms and legal proceedings, which may include infringement and breach of contract claims, and remedies may include injunctions, damages, accounting of profits and delivery up. Because Canadian patents, trademarks and industrial designs are national in scope and generally do not provide protection abroad, businesses typically consider foreign IP protection in jurisdictions where they plan to sell, manufacture, commercialise or enforce their rights, taking into account target markets, business goals, competitor activity, local IP requirements, local filing requirements and cost.

IP relating to digital and virtual assets may be monetised in Canada through licences; assignments; royalties; software-as-a-service arrangements; NFT or token-related commercialisation models; and other IP-based transactions. Any such monetisation may also be subject to generally applicable legal requirements, including securities, consumer protection, privacy, AML/ATF, sanctions and tax laws, depending on the structure and activities involved.



the global voice of
the legal profession®

International Bar Association

Chancery House
53-64 Chancery Lane
London WC2A 1QS
United Kingdom
Tel: +44 (0)20 7842 0090
Fax: +44 (0)20 7842 0091
Email: editor@int-bar.org
www.ibanet.org