



Identomat

COMPLIANCE GUIDE

Banking & Digital Banking Compliance in Canada

COUNTRY **Canada**

INDUSTRY **Banking & Digital Banking**

LAST UPDATED **27 October 2026**

KEY REGULATORS **Office of the Superintendent of Financial Institutions · Financial Transactions and Reports Analysis Centre of Canada · Financial Consumer Agency of Canada**

Key takeaways

- A bank in Canada needs letters patent (a federal charter) from the Minister of Finance and an order from the Office of the Superintendent of Financial Institutions (OSFI) before it can start business; credit unions are mostly licensed by the provinces.
 - Banks must verify every new account holder's identity before the first transaction other than the initial deposit, using one of five methods set out in federal regulations.
 - Fully remote account opening is allowed. If you rely on a photo ID the customer is not holding up in front of staff, you must use technology that checks the document is genuine and then match the person to the photo by live video or a selfie with face matching; looking at the card over a video call is not enough.
 - Penalties rose sharply in March 2026: up to \$20 million per violation for a company, and up to the greater of \$20 million or 3% of group global revenue per notice. Your compliance programme must now be "risk-based and effective", not just documented.
 - Coming next: mandatory enrolment of all reporting businesses with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), and an open banking regime run by the Bank of Canada. Both are law but most of their provisions await a start date set by the government.
-

Canada is open to digital-only banks and remote onboarding. The identity rules are the same whether a customer walks into a branch or opens an account on a phone; what changes online is how a photo ID must be authenticated and how the face match is done.

Prudential supervision sits with OSFI, consumer protection with the Financial Consumer Agency of Canada (FCAC), and anti-money laundering (AML) supervision with FINTRAC. Provincially chartered credit unions and caisses answer to provincial regulators as well as to FINTRAC.

The biggest obstacle for a new entrant is the federal charter: incorporation by letters patent and a separate order to commence business from OSFI. A fintech that instead partners with an existing bank avoids the charter, but the bank stays fully accountable for the AML and outsourcing obligations.

CONTENTS

- 1 Who regulates this sector
- 2 Licensing and authorisation
- 3 AML, KYC and customer due diligence
- 4 Identity verification and onboarding
- 5 Digital channels: what's different
- 6 Data protection and biometrics
- 7 Sector-specific obligations
- 8 Risk indicators and red flags
- 9 Enforcement and penalties
- 10 Recent changes and what to watch
- 11 What this means for identity verification
 - Sources

1 Who regulates this sector

Regulator	Remit	Level	Official site
Minister of Finance	Issues letters patent incorporating a bank (Bank Act s. 22)	Federal	canada.ca/departement-finance
OSFI	Prudential supervision of banks, order to commence business, outsourcing and integrity guidelines, monthly sanctions returns	Federal	osfi-bsif.gc.ca
FINTRAC	Financial intelligence unit and AML supervisor; receives reports and imposes administrative monetary penalties	Federal	fintrac-canafe.canada.ca
FCAC	Market conduct of banks, authorized foreign banks and federal credit unions under the Bank Act consumer framework	Federal	canada.ca/financial-consumer-agency
Bank of Canada	Accreditation and oversight under the Consumer-Driven Banking Act (mostly not yet in force)	Federal	bankofcanada.ca

Office of the Privacy Commissioner of Canada	Private-sector privacy law (PIPEDA), including biometrics	Federal	priv.gc.ca
Financial Services Regulatory Authority of Ontario; BC Financial Services Authority; Autorité des marchés financiers	Provincially chartered credit unions and caisses, trust and loan companies	Provincial (Ontario, BC, Québec)	fsrao.ca , bcfsa.ca , lauteurite.qc.ca
Commission d'accès à l'information du Québec	Québec privacy law and prior disclosure of biometric identity checks	Provincial (Québec)	cai.gouv.qc.ca

Securities dealers within banking groups are separate AML reporting entities with their own identification obligations.

2 Licensing and authorisation

A federal bank is incorporated when the Minister of Finance issues letters patent on an application under the [Bank Act, S.C. 1991, c. 46](#), s. 22(1). Incorporation alone does not allow trading: under s. 48(1) a bank "shall not carry on any business" until the Superintendent of Financial Institutions has approved the commencement and carrying on of business by order. A foreign bank that wants to operate a branch in Canada needs its own OSFI order as an authorized foreign bank (s. 534(1)).

Deposit-taking is tied to deposit insurance: under s. 413(1) a bank may accept deposits in Canada only as a member institution of the Canada Deposit Insurance Corporation, or under an exemption that keeps deposits under \$150,000 to no more than 1% of its Canadian deposits (s. 413(3)).

Credit unions and caisses populaires are mostly chartered by their province. A digital-only bank needs the same charter and order as a branch network; there is no separate online banking licence.

Non-bank payment partners register separately with the Bank of Canada under the [Retail Payment Activities Act](#).

Banks, authorized foreign banks, credit unions, caisses, trust and loan companies are reporting entities under the [PCMLTFA, S.C. 2000, c. 17](#) (current to 30 September 2026), and are "financial entities" under the [PCMLTF Regulations, SOR/2002-184](#). The Act prohibits anonymous accounts, including accounts for clients whose identity the bank has not verified under the Regulations (s. 9.2).

Compliance programme

A named compliance officer, written policies approved by a senior officer, a documented risk assessment covering clients, products, delivery channels and geography, training, and an effectiveness review every two years (Regulations s. 156). Since 26 March 2026 the programme must be "reasonably designed, risk-based and effective" (PCMLTFA s. 9.6(1.1)).

Customer identification

Verify the identity of each person for whom an account is opened and each other person authorised to give instructions, and of corporations and other entities through records confirming their existence (Regulations ss. 86, 109, 112).

Beneficial ownership

Obtain directors and everyone owning or controlling 25% or more, plus ownership and control structure, and take reasonable measures to confirm it (s. 138). Material discrepancies with the federal corporate register of individuals with significant control must be reported to Corporations Canada within 30 days unless resolved (s. 138.1).

Politically exposed persons

Determine at account opening, and periodically after, whether a holder or authorised user is a politically exposed person, head of an international organisation, family member or close associate; also for transfers or virtual currency of \$100,000 or more (s. 116).

Ongoing monitoring

Monitor every business relationship at a frequency set by risk, keep identification and ownership information current and reassess risk (s. 123.1). High-risk clients trigger enhanced verification and monitoring under s. 157.

Record keeping

Keep records for at least five years after the account closes or the last transaction (s. 148), retrievable for FINTRAC within 30 days of a request (s. 149).

Reporting thresholds

Report	Trigger	Deadline
Suspicious transaction report	Reasonable grounds to suspect money laundering, terrorist financing or sanctions evasion; no minimum amount; attempted transactions included (PCMLTFA s. 7)	As soon as practicable (STR Regulations s. 9(2))
Large cash transaction report	Cash of \$10,000 or more in one transaction, or in several within 24 consecutive hours (Regulations ss. 7(1)(a), 126)	15 days (s. 132(3))
Electronic funds transfer report	International transfer of \$10,000 or more initiated or finally received (s. 7(1)(b), ©)	5 working days (s. 132(1))
Large virtual currency transaction report	Virtual currency equivalent to \$10,000 or more received (s. 7(1)(d), s. 129)	5 working days (s. 132(2))
Listed person or entity property report	Property of a listed terrorist entity or sanctioned person (PCMLTFA s. 7.1)	In addition to the disclosure that sanctions and terrorism laws require

Below the reporting tiers there are identification tiers for non-account holders: \$3,000 or more for money orders and foreign exchange, and \$1,000 or more for international transfers or virtual currency transfers (s. 86(a)(iii)).

4

Identity verification and onboarding

Section 105(1) of the Regulations lists the only permitted ways to verify a person's identity:

- **Government-issued photo ID:** a federal, provincial or foreign (not municipal) government document with name and photo, confirming both match the person.
- **Government body:** information received on request from a federal or provincial body authorised to verify identity, matching name and address or name and date of birth.
- **Credit file:** a Canadian credit file at least three years old drawn from more than one source, matching name, address and date of birth.

- **Dual process:** any two of name and address, name and date of birth, or confirmation of a deposit, credit or loan account, each from a different reliable source; neither the customer nor the bank can be a source.
- **Affiliate or member:** confirmation that an affiliated reporting entity, or a member of the same credit union central, already verified the person.

Documents must be authentic, valid and current (s. 105(5)). For an account, verification must be complete before the first transaction other than an initial deposit; for a credit card, before activation (s. 105(7)).

A bank may use an agent under a written agreement, or rely on another reporting entity's earlier verification, but must obtain the underlying information as soon as feasible and remains responsible (ss. 106, 107). The Regulations set no identity assurance level or liveness standard.

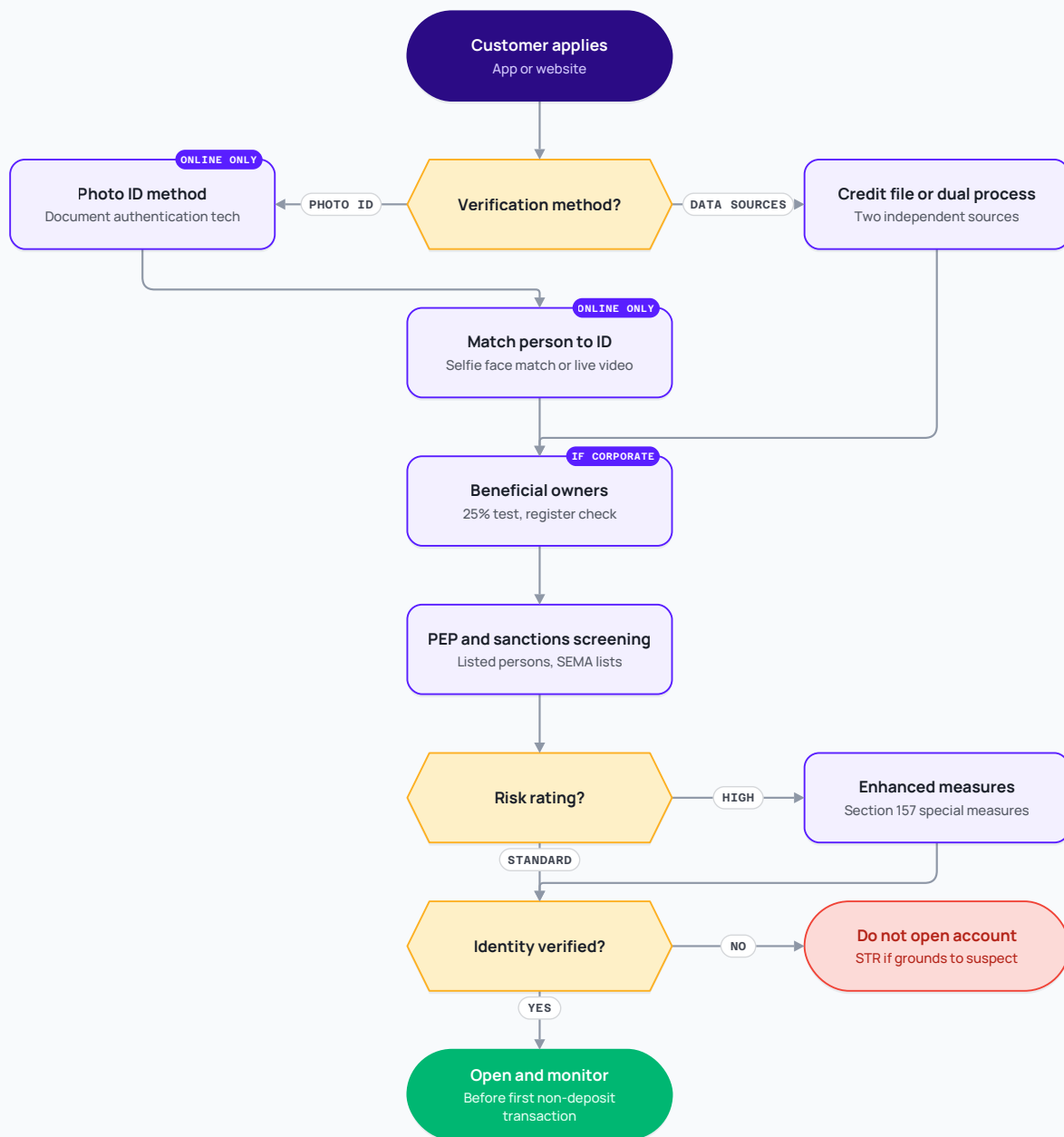


Figure 1. Remote account opening at a Canadian bank under the PCMLTF Regulations.

5

Digital channels: what's different

Bottom line: the identification methods are channel-neutral, but a photo ID used remotely must be authenticated by technology and matched to the person by live video or selfie face matching, which in a branch is done by staff examining the document.

Requirement	In person / branch	Online / remote	Difference
Remote onboarding permitted	Yes	Yes, all five s. 105 methods	Same
Authenticating a photo ID	Examine the physical document and its security features	Technology that assesses the document's authenticity	Differs
Matching person to photo	Staff compare face with photo	Live video comparison or selfie with facial recognition	Differs
When verification is due	Before first non-deposit transaction	Before first non-deposit transaction	Same
Statutory right to a basic account	On request in person with two documents	Only in a manner prescribed by regulation	Differs
Risk assessment	Delivery channel is a required factor	New onboarding technology assessed before launch	Differs
Beneficial ownership, PEP, sanctions	Required	Required	Same
Reliance on agents or other entities	Written agreement; bank stays responsible	Written agreement; bank stays responsible	Same

Photo ID without the customer present

FINTRAC's guidance [Methods to verify the identity of persons and entities](#) allows the photo ID method for a person who is not physically present only with a process that authenticates the document, for example technology comparing a phone-camera capture against security features such as holograms, barcodes or embedded chips. The bank then confirms the name and photo are the applicant's through live video or a selfie with facial recognition; viewing the ID over a video conference alone is not enough. The two steps may happen at different times.

Non-documentary routes

The credit file and dual-process methods need no document capture and work entirely online. A scan of a photo ID may count as one of the two dual-process sources, and

FINTRAC accepts credit bureau tradelines as separate sources if each comes from a different originator other than the verifying bank.

Channel risk and new technology

Delivery channels are a mandatory risk assessment factor, and a bank must assess and document the risk before introducing new technology that affects clients or delivery channels, such as a new identification tool (Regulations s. 156(1)©(ii), (2)). Remote onboarding is not in itself an enhanced due diligence trigger; it becomes one only if the bank's own assessment rates it high risk.

The basic account right is a branch right

Bank Act s. 627.17(1) obliges a bank to open a retail deposit account for a person who asks in person and presents two documents from a reliable source, and s. 105(6) of the Regulations deems that compliant. Other channels are covered only in a prescribed manner (s. 627.17(3)), so a digital bank need not accept these alternative documents online.

6 Data protection and biometrics

Banks are subject to the [Personal Information Protection and Electronic Documents Act \(PIPEDA\)](#) for their commercial activities. The Office of the Privacy Commissioner's [Guidance for processing biometrics, for businesses](#) treats biometric information capable of uniquely identifying a person, including a face template used for matching, as sensitive in every context, even if retained only briefly. Express consent is generally the appropriate form, and organisations are expected to consider less intrusive alternatives, which supports offering a non-biometric route such as the credit file or dual-process method.

Québec adds specific rules. Under the [Act to establish a legal framework for information technology, CQLR c. C-1.1](#), s. 44, a person's identity may be verified by a biometric process only if the process has been disclosed in advance to the Commission d'accès à l'information and with the person's express consent, using the minimum characteristics needed; the biometric record must be destroyed once verification is complete. Creating a biometric database must be disclosed to the Commission at least 60 days before it goes into service (s. 45). The [Act respecting the protection of personal information in the private sector](#) classes biometric information as sensitive and requires express consent before sensitive information is used for a new purpose (s. 12).

The two regimes fit together: the five-year AML retention rule applies to the s. 108 identification record, which is document and verification data, not the face template that Québec requires to be destroyed.

7

Sector-specific obligations

Consumer protection framework

FCAC supervises compliance with the Financial Consumer Protection Framework in Part XII. 2 of the Bank Act and the [Financial Consumer Protection Framework Regulations, SOR/2021-181](#). A consumer may cancel a retail deposit account within 14 business days of opening, without charge (Regulations s. 5). A bank refusing a retail deposit account must give a written statement (Bank Act s. 627.19), and may refuse only on listed grounds such as reasonable grounds to suspect fraud or a material misrepresentation of identity (s. 627.18).

Bank partnerships, banking as a service and outsourcing

OSFI's [Guideline B-10, Third-Party Risk Management](#) (dated 30 April 2023) states that a federally regulated institution remains accountable for activities and data handled by third parties and must run a third-party risk framework covering due diligence, contracts, monitoring and incident reporting. Under the PCMLTFA the bank is also the reporting entity: a fintech partner or identity vendor acting as its agent is covered by s. 106 of the Regulations, and the bank answers to FINTRAC for any failure. OSFI's [Integrity and Security Guideline](#) (31 January 2024) adds that accountability for security cannot be contracted out.

Sanctions

Banks screen against lists under the [Special Economic Measures Act](#) and the Criminal Code, report listed persons' property to FINTRAC (PCMLTFA s. 7.1) and file monthly returns OSFI-525 and OSFI-590 with [OSFI](#).

Consumer-driven banking

The [Consumer-Driven Banking Act, S.C. 2026, c. 3, s. 224](#) **Partly in force** replaced the 2024 Act of the same name and makes the Bank of Canada responsible for accrediting participants in open banking. Most operative provisions await an order in council.

FINTRAC INDICATORS FOR FINANCIAL ENTITIES (SELECTION)

- **Unverifiable ID:** the identification document cannot be authenticated, or details conflict across documents.
- **Evasive onboarding:** client refuses or avoids required information, or gives vague, hard-to-verify answers.
- **Ownership refusal:** false or conflicting beneficial ownership information for an entity account.
- **Pass-through accounts:** funds moved in and out the same day or soon after clearing.
- **Activity mismatch:** volume far above the activity projected at account opening.
- **Funnel pattern:** deposits by non-account holders, or funds consolidated from several accounts then sent abroad.
- **Structuring:** amounts kept below identification or reporting thresholds, alone or with others.
- **Dormant reactivation:** an inactive account suddenly starts receiving and sending funds.

Source: FINTRAC, [Money laundering and terrorist financing indicators, Financial entities](#), modified 24 November 2025.

FINTRAC imposes administrative monetary penalties per violation. Each violation is classified as minor, serious or very serious, and since 26 March 2026 the ranges are \$1 to \$40,000, \$1 to \$4,000,000 and \$1 to \$20,000,000 respectively ([AMP Regulations, SOR/2007-292](#), s. 5). Failing to file a suspicious transaction report is classified as very serious. For all violations on one notice, the cap for an entity is the greater of \$20,000,000 and 3% of gross global revenue, measured across affiliated entities (PCMLTFA s. 73.1(3), (4)).

After any violation FINTRAC must require a compliance agreement; refusal or a missed deadline leads to a published compliance order, whose breach carries up to the greater of \$30,000,000 or 3% of revenue (ss. 73.16 to 73.18).

Recent bank actions under the earlier, lower penalty scale:

- [The Toronto-Dominion Bank](#): \$9,185,000 imposed 9 April 2024 for five violations, including 20 unfiled suspicious transaction reports out of 178 files reviewed, inadequate risk assessment, special measures and ongoing monitoring.
- [First Nations Bank of Canada](#): \$601,139.80 imposed 22 September 2025 for five violations, including failure to report suspicious transactions and failure to take special measures for high-risk clients.
- Exchange Bank of Canada: \$2,457,750 imposed November 2024; the Federal Court confirmed the violations on 18 December 2025 and varied the amount to \$1,027,975 ([FINTRAC public notices](#)).

10

Recent changes and what to watch

- **26 March 2026:** **In force** Strengthening Canada's Immigration System and Borders Act, S.C. 2026, c. 4, Part 9: penalties raised up to \$20 million per violation and 3% of global revenue, mandatory compliance agreements and orders, and an "effective" programme standard.
- **Date to be fixed:** **Adopted, effective date not yet set** Mandatory enrolment of reporting entities with FINTRAC on a public roll (PCMLTFA ss. 11.4001 onwards, added by S.C. 2026, c. 4).
- **Forward Regulatory Plan 2025 to 2027:** **Proposed, not yet pre-published** Department of Finance regulations to implement enrolment, a restriction on large cash transactions and a restriction on third-party cash deposits.
- **26 March 2026:** **Partly in force** Consumer-Driven Banking Act, S.C. 2026, c. 3, with the Bank of Canada as accrediting authority; operative provisions await an order in council.
- **2026:** **Bill, not enacted** Bill C-36, An Act to enact the Protecting Privacy and Consumer Data Act and to amend PIPEDA, is at second reading in the House of Commons. Private-sector privacy rules for onboarding data would change if it passes.
- **1 October 2025:** **In force** Updated rules on verifying identity through an agent or mandatary, requiring a written agreement before use (Regulations s. 106; FINTRAC guidance section 8).
- **2024:** **In force** Suspicious transaction reporting extended to suspected sanctions evasion (PCMLTFA s. 7©, added by S.C. 2024, c. 15).

What this means for identity verification

- **Map each flow to one s. 105 method.** A remote photo ID flow needs both document authentication technology and a face match; a database flow needs a three-year credit file or two independent dual-process sources. Hybrid flows must still satisfy one method completely.
- **Accept foreign documents.** Foreign government photo ID qualifies, which helps newcomers without a Canadian credit file.
- **No prescribed standard.** No certification or liveness standard is named; FINTRAC cites embedded chips, holograms and barcodes as features technology can check.
- **Gate the first transaction.** The account may be opened and funded by an initial deposit, but no other transaction until verification is complete.
- **Record method-specific data.** Section 108 requires the document type, number, jurisdiction and expiry, or the source and reference number for data methods, and the date verified, kept five years after closure.
- **Re-verify on doubt.** Identity need not be re-verified unless there are doubts about the information used (Regulations s. 155), but ownership and client information must be refreshed through risk-based ongoing monitoring.

How Identomat helps

Identomat runs identity verification, screening and monitoring for regulated businesses on one platform, with workflows you configure for each market. For the requirements in this guide, that means:

- ID document capture and verification, including NFC chip reading, to authenticate a government photo ID when the customer is not present.
- Face match with biometric liveness, or video KYC, to confirm the applicant is the person on the document before the first transaction.
- KYB and beneficial owner verification for business accounts, capturing the 25% ownership and control information banks must confirm.
- AML screening against sanctions, PEP and adverse-media lists at onboarding and through ongoing monitoring.
- No-code workflow builder and an audit trail of each check, with cloud, on-premises or hybrid deployment to fit data residency needs.

[Request a meeting](#)

DISCLAIMER

This article is intended for informational purposes only and does not constitute legal advice. It is a compilation of information from various sources and reflects the information available as of the last updated date indicated above. Laws, regulations, and regulatory guidance may change, so readers should consult qualified legal professionals for advice specific to their circumstances.

Sources

- **Proceeds of Crime (Money Laundering) and Terrorist Financing Act, S.C. 2000, c. 17**, ss. 7, 7.1, 9.2, 9.6, 73.1, 73.16 to 73.18, 74, 75 and amendments not in force, current to 30 September 2026, laws-lois.justice.gc.ca
- **Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, SOR/2002-184**, ss. 7, 84 to 88, 105 to 112, 116, 123.1, 126, 129, 132, 138, 138.1, 148, 149, 155 to 157, current to 30 September 2026, laws-lois.justice.gc.ca
- **Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations, SOR/2001-317**, s. 9, laws-lois.justice.gc.ca

- Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations, SOR/2007-292, s. 5, current to 30 September 2026, laws-lois.justice.gc.ca
- Strengthening Canada's Immigration System and Borders Act, S.C. 2026, c. 4, Part 9 and s. 124, assented 26 March 2026, laws-lois.justice.gc.ca
- Bank Act, S.C. 1991, c. 46, ss. 22, 48, 413, 534, 627.17 to 627.19, 627.74, current to 30 September 2026, laws-lois.justice.gc.ca
- Financial Consumer Protection Framework Regulations, SOR/2021-181, s. 5, current to 30 September 2026, laws-lois.justice.gc.ca
- Consumer-Driven Banking Act, S.C. 2026, c. 3, s. 224, s. 181, current to 30 September 2026, laws-lois.justice.gc.ca
- Special Economic Measures Act, S.C. 1992, c. 17, laws-lois.justice.gc.ca
- Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, laws-lois.justice.gc.ca
- FINTRAC, Methods to verify the identity of persons and entities, sections 2 and 8, modified 3 December 2024, fintrac-canafe.canada.ca
- FINTRAC, Money laundering and terrorist financing indicators, Financial entities, modified 24 November 2025, fintrac-canafe.canada.ca
- FINTRAC, Public notice of administrative monetary penalties, fintrac-canafe.canada.ca; notices on The Toronto-Dominion Bank (2 May 2024) [pen-2024-05-02](https://www.fintrac-canafe.ca/pen-2024-05-02) and First Nations Bank of Canada (16 October 2025) [pen-2025-10-16](https://www.fintrac-canafe.ca/pen-2025-10-16)
- OSFI, Guideline B-10, Third-Party Risk Management, 30 April 2023, osfi-bsif.gc.ca
- OSFI, Integrity and Security Guideline, 31 January 2024, osfi-bsif.gc.ca
- OSFI, Reporting on anti-money laundering, anti-terrorist financing and sanctions, modified 12 September 2024, osfi-bsif.gc.ca
- Department of Finance Canada, Forward Regulatory Plan 2025 to 2027: Amending Regulations under the PCMLTFA (Strong Borders Act), 19 December 2025, canada.ca
- Retail Payment Activities Act, S.C. 2021, c. 23, s. 177, current to 30 September 2026, laws-lois.justice.gc.ca
- Financial Consumer Agency of Canada, Supervising financial institutions, modified 23 July 2026, canada.ca
- Office of the Privacy Commissioner of Canada, Guidance for processing biometrics, for businesses, priv.gc.ca
- Québec, Act to establish a legal framework for information technology, CQLR c. C-1.1, ss. 44, 45, up to date at 15 October 2026, legisquebec.gouv.qc.ca
- Québec, Act respecting the protection of personal information in the private sector, CQLR c. P-39.1, s. 12, up to date at 15 October 2026, legisquebec.gouv.qc.ca
- Parliament of Canada, LEGISinfo, Bill C-36 (45th Parliament, 1st Session), parl.ca