



Identomat

COMPLIANCE GUIDE

Telecom & Mobile Services Compliance in Canada

COUNTRY **Canada**

INDUSTRY **Telecom & Mobile Services**

LAST UPDATED **27 October 2026**

KEY REGULATORS **Canadian Radio-television and Telecommunications Commission · Office of the Privacy Commissioner of Canada · Innovation, Science and Economic Development Canada**

Key takeaways

- Any company that sells phone, mobile or internet service in Canada, including a reseller or a mobile virtual network operator (MVNO, a brand that rents another carrier's network), must register with the Canadian Radio-television and Telecommunications Commission (CRTC) before it starts selling.
- Canada's anti-money-laundering law does not cover telecom providers, and no federal rule prescribes which ID a carrier must check when it activates a SIM. Carriers set their own activation checks, but privacy law limits what they may collect: Québec's regulator has accepted photo ID checks at account opening but not routine collection of social insurance numbers for credit checks.
- A carrier may not reveal anything about a customer beyond name, address and listed number without clear, informed consent or a legal power, and it must authenticate callers firmly enough that impersonators cannot hijack accounts or move numbers.
- Online channels are about to change: from 26 April 2027 every provider must let customers change or cancel plans through an app, website or email, and must send written confirmation of each change, so self-service flows need strong authentication.
- Expect more federal powers: security orders over telecom networks have applied since June 2026, and a lawful access bill that would let police confirm whether a person is a subscriber is before the Senate (not yet law).

The Canadian market is open to new telecom entrants online and offline, subject to registration with the CRTC and, for facilities-based carriers, Canadian ownership and control rules. Telecom is regulated federally: the CRTC sets conditions of service, Innovation, Science and Economic Development Canada (ISED) handles spectrum and network security orders, and the Office of the Privacy Commissioner of Canada (OPC) enforces the federal private-sector privacy law.

The biggest obstacle for a new entrant is not licensing but fraud. Regulators treat unauthorised SIM swaps, fraudulent port-outs and call-centre impersonation as the sector's core identity risk.

CONTENTS

- 1 Who regulates this sector
- 2 Licensing and authorisation
- 3 Identity framework (AML rules do not apply)
- 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

Authority	Remit for telecom identity	Level	Official site
Canadian Radio-television and Telecommunications Commission (CRTC)	Registration, conditions of service, confidential customer information rules, Wireless Code, SIM-swap and port-out monitoring, unsolicited calls, administrative monetary penalties	Federal	crtc.gc.ca
Innovation, Science and Economic Development Canada (ISED)	Spectrum licensing; ministerial orders to secure the telecommunications system	Federal	ised-isde.canada.ca
Office of the Privacy Commissioner of Canada (OPC)	Personal Information Protection and Electronic Documents Act (PIPEDA): consent, safeguards, breach reporting, biometrics guidance	Federal	priv.gc.ca
Commission d'accès à l'information du Québec (CAI)	Prior disclosure of biometric identity verification and biometric databases under Québec law	Provincial (Québec)	cai.gouv.qc.ca

2 Licensing and authorisation

Registration. Before an organisation offers or provides telecommunications services, it must register with the CRTC. This covers local voice, Voice over Internet Protocol (VoIP),

internet, long distance and wireless services, for providers of any size; registration is free. International traffic also needs a BITS licence ([CRTC registration page](#); [Telecommunications Act, s. 16.1](#)).

Resellers and MVNOs. The Telecommunications Act lets the CRTC impose conditions of service directly on providers that are not carriers, including conditions on contracts with users and on the protection of users' privacy (s. 24.1). The CRTC has used this power to require resellers to register before receiving wholesale service and to follow its consumer safeguards, including the confidential customer information rules, the Wireless Code and the duty to support number porting ([Telecom Regulatory Policy 2017-11](#)). An online-only MVNO is therefore bound by the same customer-data rules as the network owner.

Ownership. A facilities-based carrier must be Canadian-owned and controlled unless its revenues are below 10% of the national total ([Telecommunications Act, s. 16](#)).

3

Identity framework (AML rules do not apply)

The Proceeds of Crime (Money Laundering) and Terrorist Financing Act lists the businesses it covers in section 5: banks, credit unions, life insurers, securities dealers, money services businesses and other prescribed sectors. Telecommunications providers are not on the list ([PCMLTFA, s. 5](#)). A telecom group that also remits funds or deals in virtual currency, for example through a mobile wallet, is covered as a money services business for that activity.

For voice, data and internet services, identity is governed instead by three layers:

CRTC confidential customer information rules

Conditions of service under sections 24 and 24.1: everything a provider holds about a customer except name, address and listed number is confidential, and IP addresses and unlisted mobile numbers are expressly included. Disclosure requires express consent that is meaningful, clear and informed, a legal power, or a listed exception ([Telecom Decision 2022-238](#)).

PIPEDA safeguards and consent

Personal information must be protected by safeguards appropriate to its sensitivity, and express consent should generally be sought for sensitive information ([PIPEDA, Schedule 1, Principles 4.3 and 4.7](#)). The OPC applies these principles to telecom account authentication.

CRTC fraud supervision

Since 2020 the CRTC has required mobile carriers to report unauthorised SIM swaps and ports and to confirm implementation of industry countermeasures, rather than setting a published rule.

Nothing in this framework sets a customer identification programme comparable to the AML regime. The [Wireless Code](#), which applies however a service is bought (in person, online or by phone), contains no identity verification duty. It does regulate security deposits (the provider must record its reasons), requires the account holder's or an authorised user's express consent to key changes, lets a provider disconnect without notice where it reasonably suspects fraud, and requires immediate suspension when a device is reported lost or stolen. Identity checks at activation are therefore each provider's risk decision, limited by privacy law (section 4).

4

Identity verification and onboarding

Authentication is the regulated moment. Regulators have focused on what happens after onboarding, when someone asks to access, change or move an account. The OPC's guidelines say the stringency of authentication should match the risk to the organisation and the individual. In [PIPEDA Findings #2021-004](#) (Fido Solutions, a Rogers subsidiary), fraudsters were let into an account on five calls, even after the customer added a PIN and secret questions, because staff bypassed a protocol of date of birth and postal code, PIN or voice biometrics, knowledge questions and, as a last resort, an in-store ID check. The OPC found a systemic safeguards breach and required clear protocols, high-risk account flags, training and compliance monitoring.

Biometrics. Voice, face and other biometrics are accepted authentication tools, but consent rules are strict. In [PIPEDA Findings #2022-003](#), the OPC accepted Rogers' Voice ID as an appropriate response to the high-threat environment carriers face, but required express consent before any voiceprint is created and an easy opt-out. Québec adds prior disclosure to the CAI (section 6).

What may be collected at activation. In [CAI decision 111310-S](#) (8 June 2023, Rogers Communications), Québec's privacy regulator held that visually inspecting a customer's photo ID at account opening, even without keeping a copy, is a collection of personal information, and that it is necessary to verify identity. A social insurance number (SIN) or driver's licence number, chosen by the customer from a list of accepted identifiers, was

also found necessary for fraud prevention, absent a less intrusive alternative. Routine SIN collection for credit checks was not, because credit files can be found with name, address and date of birth. The CAI issued recommendations, not orders, and declined to rule on whether Québec law binds a federal carrier.

Third parties and data minimisation. A provider using an outside verification service should engage it as its agent under contract, and may not use publicly available data to confirm confidential customer information ([Telecom Decision 2022-238](#)).

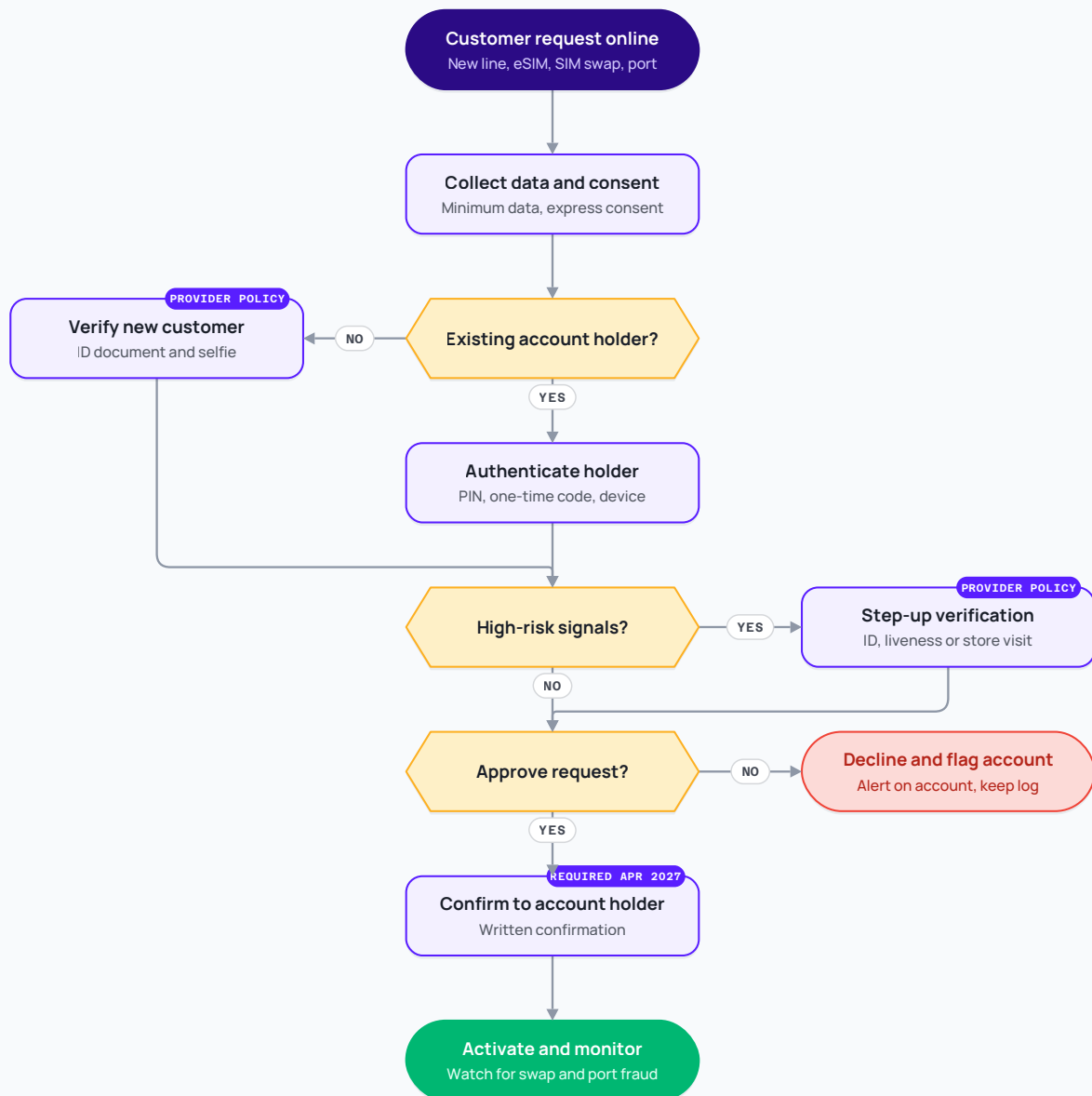


Figure 1. Illustrative online flow for a new line, eSIM transfer, SIM swap or port-out at a Canadian wireless provider. Steps tagged as provider policy are risk controls, not prescribed by regulation.

Bottom line: the privacy and authentication rules are channel-neutral, but from 26 April 2027 every provider must offer online self-service to change or cancel plans, with written confirmation, which moves high-risk account changes into the digital channel.

Requirement	In store / call centre	Online / app	Difference
Confidentiality of customer information	CCI rules apply	CCI rules apply	Same
Authentication before account access or changes	Safeguards matched to risk	Safeguards matched to risk	Same
Ability to modify or cancel a plan without an agent	Not required	Mandatory from 26 Apr 2027	Differs
Written confirmation of each change	Not required by the self-service policy	Required for every self-service action	Differs
Biometric verification	Express consent; Québec CAI disclosure	Express consent; Québec CAI disclosure	Same
Device locking after sale	Up to two business days under stay	Up to two business days under stay	Same
Breach reporting	Real risk of significant harm test	Real risk of significant harm test	Same

Mandatory self-service Adopted, effective 26 Apr 2027

Section 27.01 of the Telecommunications Act (in force 30 October 2025) requires self-service cancellation and plan changes. [Telecom Regulatory Policy 2026-78](#) defines it as an app, website, email or similar mechanism that works without a live agent, applies it to all providers and requires written confirmation of each action. Providers warned of fraud risk; the CRTC left security design to them.

Remote SIM swaps and port-outs

The industry association's 2020 filing describes the typical attack: fraudsters gather a victim's details, open an account (usually prepaid) with a new provider, and port the number away to intercept one-time codes. Before 2020 a port was validated with the phone number plus an account number, PIN or device identifier; the association also stated that providers collect no name or ID for prepaid service ([CRTC file 8665-C12-202000280](#)). At the CRTC's request carriers launched an "Enhanced Process" in August 2020, which TELUS described as two-way SMS validation; it was rolled back within a week after up to 40 to 50% of legitimate ports failed for some carriers, then relaunched in November 2020 ([CRTC letter, 24 August 2020](#)). The CRTC reported a 95% fall in unauthorised ports and SIM swaps between October 2020 and May 2021 ([CRTC letter, 8 July 2021](#)) and has since required monthly counts by brand, split by prepaid and postpaid, whenever a carrier records six or more a month, most recently for July to December 2023 and in a January 2024 request ([staff letter, 16 June 2023](#)).

Porting rules limit how far a losing carrier can slow a port to check identity. A simple wireless-to-wireless port must be completed within 2.5 business hours ([Telecom Decision 2005-72](#)), and CRTC staff have reminded providers that a port may be refused only if the number is not working because of a suspension or termination, not, for example, because of an unpaid balance ([staff letter to PhoneBox, 19 November 2025](#)). Where a reseller is involved, [Telecom Decision 2026-272](#) (16 October 2026) bars same-day expedited ports, putting accuracy and fraud prevention ahead of speed. Authentication therefore belongs in the flows before a port.

6 Data protection and biometrics

Federal law. Under PIPEDA, express consent should generally be sought for sensitive information (Principles 4.3.4 and 4.3.6), and breaches creating a real risk of significant harm must be reported to the OPC and affected individuals, with a record kept of every breach (ss. 10.1 and 10.3). The CRTC's rules add an express-consent requirement for disclosure where PIPEDA would sometimes accept implied consent ([Telecom Decision 2022-238](#)).

Biometrics guidance. The OPC's [Guidance for processing biometrics, for businesses](#) (adopted, page dated 11 August 2025) treats express consent as the general rule for biometric information, including templates, and asks organisations to show that less intrusive means would not work and that the programme is proportionate.

Québec. Section 44 of the [Act to establish a legal framework for information technology, CQLR c. C-1.1](#) (current to 15 October 2026) prohibits verifying identity through a biometric

process unless the process was disclosed to the CAI in advance and the person gives express consent. Only the minimum characteristics may be recorded, and they must be destroyed once verification is complete. Section 45 requires a biometric database to be disclosed at least 60 days before it goes into service, and the CAI may suspend or order its destruction.

Reform. Bill C-36, which would enact the Protecting Privacy and Consumer Data Act, is at second reading in the House of Commons **Bill, not enacted**.

7 Sector-specific obligations

Network security orders

Part 1 of [S.C. 2026, c. 9](#), in force since Royal Assent on 15 June 2026, added security of the telecommunications system to the Act's policy objectives and lets the Governor in Council and the Minister of Industry order providers to drop specified products, adopt security plans, implement standards or suspend service to specified persons (ss. 15.1 and 15.2); orders may be kept confidential. Part 2, the Critical Cyber Systems Protection Act, will come into force on a date set by order **Adopted, effective date not yet set**.

Call traceback and caller ID authentication

Since 25 June 2026 every voice provider must join the CRTC's call traceback process, respond within two business days, keep call data for at least 10 calendar days and include STIR/SHAKEN caller ID attestation data where feasible ([Compliance and Enforcement and Telecom Decision 2026-52](#)).

Lawful access to subscriber information

Under the confidential customer information rules, a provider may give subscriber details to the state only with consent, under a legal power or within narrow exceptions such as imminent danger to life. The Supreme Court of Canada has held that subscriber information linked to an IP address attracts a reasonable expectation of privacy, so a police request for voluntary disclosure is a search that needs lawful authority ([R. v. Spencer, 2014 SCC 43](#)). Bill C-22 would let police and CSIS demand confirmation of whether a person or identifier is a subscriber, and would allow regulations requiring designated core providers to retain metadata for up to six months; it would not require providers to verify subscribers' identity (section 10).

TELECOM IDENTITY-FRAUD INDICATORS FROM CANADIAN REGULATORS

- **Unauthorised port-out:** a number moved to a new account, usually prepaid, opened at another provider by someone posing as the holder.
- **Unauthorised SIM swap:** a new SIM or eSIM issued to someone other than the account holder, usually to intercept one-time codes.
- **Information harvesting by phone:** a caller gives a wrong name or partial details and lets the agent fill in the rest, then reuses them on later calls.
- **Repeated failed authentication:** wrong PINs or wrong answers to knowledge questions followed by a request to change the PIN or email.
- **Agents bypassing protocol:** staff skipping authentication steps, especially where sales targets create pressure.
- **Point-of-sale device fraud:** subscription fraud and theft of new devices, which providers link to devices sold unlocked.
- **Spoofed caller ID:** calls showing false numbers used to extract personal information.
- **Numbers resold through chains:** telephone numbers passed between several third parties before activation, making the end user hard to trace.

Sources: CRTC SIM-swap letters, [PIPEDA #2021-004](#), CRTC [2026-210](#), [2026-52](#) and [2026-61](#).

Regime	Maximum penalty	Basis
General CRTC scheme (Act, regulations, CRTC decisions such as the CCI rules and the Wireless Code)	Corporations \$10,000,000, then \$15,000,000 for a subsequent contravention; individuals \$25,000, then \$50,000	Per violation (s. 72.001); officers and directors who direct or acquiesce are liable (s. 72.008)

Network security orders (ss. 15.1, 15.2)	Same amounts	Per violation, each day a separate violation (ss. 72.131, 72.132)
Unsolicited telecommunications rules	Individuals \$1,500; corporations \$15,000	Per violation, each day a separate violation (ss. 72.01, 72.03)
PIPEDA breach reporting and record-keeping	\$10,000 on summary conviction; \$100,000 on indictment	Knowing contravention of ss. 10.1 or 10.3(1) (s. 28)

CRTC penalties are set by reference to the nature and scope of the violation, compliance history, any benefit obtained and ability to pay, and their stated purpose is to promote compliance rather than punish (s. 72.002) ([Telecommunications Act, Part V](#)).

Recent actions. In June 2026 the CRTC required Bell Canada, Rogers and TELUS to show cause why penalties of up to \$10,000,000 each should not be imposed for fees that may breach the ban on activation fees in force since 12 June 2026: Bell's \$40 device-handling charge, TELUS's \$15 fee for a SIM or eSIM, and Rogers' \$40 device set-up charge, \$25 online shipping charge and SIM fee ([Telecom Notice of Consultation 2026-155](#)). The written record closed in September 2026 and no decision had been issued as of 27 October 2026 ([Notice 2026-155-2](#)). In August 2026 it opened a show-cause proceeding into Bell Canada's fraud-justified 60-day device locking ([Notice 2026-210](#)).

10 Recent changes and what to watch

- **22 October 2026:** Bill C-22, the Lawful Access Act, 2026, passed the House of Commons on 18 June and was referred to Senate committee **Bill, not enacted**. It would allow confirmation of service demands to telecom providers and enact the Supporting Authorized Access to Information Act, with capability and record-keeping duties for electronic service providers.
- **16 October 2026:** CRTC Decision 2026-272 bars same-day expedited ports involving resellers and requires underlying carriers to notify resellers of completed port-outs within two business days **In force**.
- **14 August 2026:** CRTC Notice 2026-210 granted a temporary industry-wide stay of the Wireless Code unlocking rule, allowing devices to stay locked for up to two business days after sale **Optional relief, pending decision**. The consumer-code harmonisation hearing (Notice 2026-134) begins 30 November 2026.

- **25 June 2026**: mandatory call traceback participation for all voice providers **In force** .
- **15 June 2026**: S.C. 2026, c. 9 received Royal Assent **Partly in force** .
Telecommunications Act security powers apply now; the Critical Cyber Systems Protection Act awaits an order. The same day, Bill C-36 on private-sector privacy was introduced **Bill, not enacted** .
- **24 April 2026**: Telecom Regulatory Policy 2026-78 requires self-service plan changes and written confirmations **Adopted, effective 26 Apr 2027** . Separately, Notice 2026-61 (2 April) is considering limits on resale of telephone numbers
Consultation, record closed 3 Jun 2026 .

11 What this means for identity verification

Collect only what each purpose needs at activation (inspect rather than copy ID; avoid routine SIN collection), and concentrate controls on SIM or eSIM reissue, port-out, PIN, email or address changes and cancellation, where regulators have found account takeover.

From April 2027 plan changes must work without an agent, so agent judgement needs a digital equivalent: possession factors that do not depend on the SIM at risk, step-up document and liveness checks for high-risk actions, and confirmations sent to contact details already on file.

Biometrics need consent before capture. Obtain express consent before any template is created, offer an opt-out, and in Québec disclose the process and any template database to the CAI in advance.

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:

- Step-up identity verification before SIM swaps, eSIM transfers and port-outs, with ID document capture, face match and biometric liveness.
- Remote onboarding for new lines with ID document verification, including NFC chip reading where supported.
- Phone and email verification to confirm contact details used for written confirmations of account changes.
- No-code workflow builder to set risk-based rules for self-service actions, with an audit trail for each check.
- Cloud, on-premises or hybrid deployment to fit data residency and privacy requirements.

[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

- **Telecommunications Act, S.C. 1993, c. 38** (current to 30 September 2026, last amended 15 June 2026), ss. 16, 16.1, 24, 24.1, 27.01 to 27.05, 72.001 to 72.136, Justice Laws Website, laws-lois.justice.gc.ca
- **An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, S.C. 2026, c. 9** (assented 15 June 2026), Parts 1 and 2, s. 16, laws-lois.justice.gc.ca
- **Proceeds of Crime (Money Laundering) and Terrorist Financing Act, S.C. 2000, c. 17, s. 5**, laws-lois.justice.gc.ca

- **Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5** (current to 30 September 2026), ss. 10.1, 10.3, 28 and Schedule 1, laws-lois.justice.gc.ca
- **Telecom Decision CRTC 2022-238**, privacy requirements and confidential customer information rules, 6 September 2022, crtc.gc.ca
- **Telecom Regulatory Policy CRTC 2026-78**, Enhancing self-service mechanisms, 24 April 2026, crtc.gc.ca
- **Compliance and Enforcement and Telecom Decision CRTC 2026-52**, mandatory call traceback participation, 27 March 2026, crtc.gc.ca
- **Telecom Notice of Consultation CRTC 2026-61**, strengthening numbering usage management practices, 2 April 2026, crtc.gc.ca
- **Telecom Notice of Consultation CRTC 2026-155**, show cause on fees that are a barrier to switching, 30 June 2026, crtc.gc.ca
- **Telecom Notice of Consultation CRTC 2026-210**, device unlocking show cause and temporary stay, 14 August 2026, crtc.gc.ca
- **CRTC letters on unauthorised mobile number transfers and SIM swapping**, 17 July 2020, 24 August 2020, 22 June 2021, 8 July 2021, 16 June 2023 and 18 January 2024, [17 Jul 2020](https://crtc.gc.ca/2020/20200717.html), [24 Aug 2020](https://crtc.gc.ca/2020/20200824.html), [22 Jun 2021](https://crtc.gc.ca/2021/20210622.html), [8 Jul 2021](https://crtc.gc.ca/2021/20210708.html), [16 Jun 2023](https://crtc.gc.ca/2023/20230616.html), [18 Jan 2024](https://crtc.gc.ca/2024/20240118.html)
- **CRTC public record, file 8665-C12-202000280 (Fraudulent Wireless Customer Transfers)**, including the Canadian Wireless Telecommunications Association letters of 14 February and 17 September 2020 (abridged) and TELUS confirmations of 10 August and 5 November 2020, crtc.gc.ca
- **The Wireless Code** (Appendix 1 to Telecom Regulatory Policy CRTC 2017-200, as amended), CRTC, crtc.gc.ca
- **Telecom Regulatory Policy CRTC 2017-11**, application of regulatory obligations directly to non-carriers, 17 January 2017, crtc.gc.ca
- **Telecom Decision CRTC 2005-72**, Implementation of wireless number portability, 20 December 2005, crtc.gc.ca
- **Telecom Decision CRTC 2026-272**, porting process changes involving resellers, 16 October 2026, crtc.gc.ca
- **CRTC staff letter to Connex Global Communications (PhoneBox)**, phone number transfer procedure, 19 November 2025, crtc.gc.ca
- **Telecom Notice of Consultation CRTC 2026-155-2**, procedural determinations, 14 August 2026, crtc.gc.ca
- **Commission d'accès à l'information du Québec, décision 111310-S, Rogers Communications inc.** [CAI decision 111310-S], 8 June 2023, cai.gouv.qc.ca
- **R. v. Spencer**, 2014 SCC 43, [2014] 2 S.C.R. 212, Supreme Court of Canada, decisions.scc-csc.ca
- **CRTC, Register as a Telecommunications provider**, crtc.gc.ca
- **PIPEDA Findings #2021-004**, Fido Solutions Inc., 30 March 2021, priv.gc.ca
- **PIPEDA Findings #2022-003**, Rogers Communications Inc. Voice ID, 30 March 2022, priv.gc.ca

- OPC, Guidance for processing biometrics, for businesses, page modified 11 August 2025, priv.gc.ca
- Loi concernant le cadre juridique des technologies de l'information [Act to establish a legal framework for information technology], CQLR c. C-1.1 (à jour au 15 octobre 2026), ss. 44 and 45, Québec, legisquebec.gouv.qc.ca
- Bill C-22 (45-1), An Act respecting lawful access, text as passed by the House of Commons 18 June 2026, and LEGISinfo status, parl.ca
- Bill C-36 (45-1), An Act to enact the Protecting Privacy and Consumer Data Act, LEGISinfo, parl.ca