OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

Identity theft: Quick reference for public bodies and organizations

August 2026

Purpose of this guidance

Identity theft occurs when someone collects or uses personal information without permission to commit fraud or other crimes. This can involve traditional theft of real information or "synthetic" identity theft that combines real and fake information. In many cases, identity theft results from a privacy breach. This document outlines the steps that public bodies and private sector organizations can take to prevent privacy breaches, respond quickly and effectively when one does happen, and offers suggestions on how they can help people affected by identity theft.

Our guidance, *Identity theft in BC: Understanding, preventing, and responding to risks*, offers more information on the topics covered here, as well as relevant provincial and federal laws.

Security measures

BC's privacy laws require public bodies and organizations to put safeguards in place to protect personal information from the types of breaches that can lead to identity theft. Under the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA), public bodies and organizations are obligated to protect personal information by making reasonable security arrangements against unauthorized access, collection, use, disclosure or disposal. What counts as "reasonable" depends on the sensitivity of the information and the harm a breach could cause. Highly sensitive data – such as social insurance numbers, personal health numbers or financial records – requires more rigorous safeguards. Some common types of safeguards include[1]:

Administrative: clear privacy policies; staff training on secure data handling and recognizing phishing/social engineering; ensuring contracts with third-party providers require equivalent security standards.

Technical: access controls based on role/job function with unique logins and audit logs; industry-standard encryption for sensitive data, especially on mobile devices or public networks; data minimization (collect and retain only what is necessary).

Physical: locked storage and restricted access for physical records; workstations positioned to avoid exposing information to unauthorized viewers; secure destruction when information is no longer needed.

[1] See Securing personal information: A self-assessment for public bodies and organizations for more detailed information.

Privacy breach response

If a breach is suspected or confirmed, the OIPC recommends following this four-step process[2]:

1. **Contain the breach**: Immediately stop the unauthorized access or disclosure – this may include recovering lost records, shutting down compromised systems, or revoking access.
2. **Evaluate the risks:** Determine the information that was breached, how many people are affected, and whether there's a real risk of significant harm, including identity theft.
3. **Notify:** Under FIPPA, notify the OIPC and affected individuals without unreasonable delay if there's a real risk of significant harm. PIPA doesn't currently mandate this for organizations; however, the OIPC recommends it as best practice, as the office can provide expert guidance in the aftermath of a breach.
4. **Prevent future breaches**: Investigate the cause; update security policies; fix vulnerabilities, and provide additional staff training.

Support for affected people

Where a breach poses a risk of identity theft, take a proactive approach – don't wait for irrefutable proof of damage from a breach. Offer affected individuals identity theft protection services, which may include:

- alerts on new credit accounts or inquiries;
- dark web/underground forum monitoring;
- access to recovery specialists;
- monitoring of financial accounts and public records for unauthorized changes
- specific monitoring for children; and
- services reducing availability of personal information online.

Duration: One to two years is standard for most breaches; a minimum of five years is recommended where there's evidence that the information is on the dark web.

Notify affected individuals directly wherever possible, with clear written instructions on how to access the offered services.

These guidelines are for information purposes only and do not constitute a decision or finding by the Office of the Information and Privacy Commissioner for British Columbia. These guidelines do not affect the powers, duties, or functions of the Information and Privacy Commissioner regarding any complaint, investigation, or other matter under FIPPA or PIPA.

[2] For more information, see Privacy breaches: tools and resources for public bodies, Privacy breach checklist for public bodies, and Privacy breach checklist for private organizations.