GENERAL

August 2026

Identity theft in BC: Understanding, preventing, and responding to risks

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

PURPOSE OF THIS DOCUMENT

This document provides guidance on preventing and responding to identity theft in British Columbia. It is intended for:

- **public bodies:** to aid in understanding their obligations for protecting personal information and managing privacy breaches under the *Freedom of Information and Protection of Privacy* Act (FIPPA);
- **private sector organizations:** to aid in understanding their obligations for protecting personal information and managing breaches under the *Personal Information Protection Act* (PIPA); and
- **individuals:** to provide practical steps for protecting their privacy, both before and in the event of a privacy breach, and information on how to file a complaint with the OIPC. If you believe you may be the victim of identity theft, see the "For Individuals," section and "Appendix B: Checklist for individuals" for immediate steps you can take.

WHAT IS IDENTITY THEFT

Identity theft occurs when someone collects or uses personal information without permission to commit fraud or other crimes. It involves the misuse of personal information, such as government-issued identification or financial information, to impersonate another person. Common forms of identity theft include:

- Traditional identity theft: stealing or illegally possessing a real person's personal information; or
- Synthetic identity theft: stealing or illegally possessing a real person's personal information to **combine** with fake personal information to create a new identity. Children may be especially vulnerable to synthetic identify theft, and their personal information can be used for fraudulent activity that is not detected until years later.

In many cases, identity theft results from a privacy breach – the unauthorized access to or collection, use, disclosure, or disposal of personal information. When a public body or organization fails to make reasonable security arrangements to protect the personal information in its custody or control, it creates a risk of unauthorized access that could lead to identity theft.

Common forms of fraudulent or illegal activity facilitated by identity theft include:

- **financial:** unauthorized bank transactions, draining accounts, mortgage fraud, or opening new credit lines;

- **medical:** using a stolen Personal Health Number to obtain medical services or file false insurance claims;
- **evading law enforcement:** misrepresenting to be someone else to law enforcement during an arrest;
- **credit building/repair schemes:** using stolen or synthetic personal information to build a new or repair existing credit history;
- **official documents:** using personal information to fraudulently create, obtain, or alter official or government-issued documents, such as passports, identification, land title, or business documents;
- **employment-related schemes:** using stolen personal information to fraudulently gain employment**;**
- **tax-related:** using a stolen Social Insurance Number to file fraudulent tax returns and claim refunds; and
- **other types:** impersonating a loved one or known contact (via "deepfake") to gain access to other information, unauthorized address changes, taking control of existing online accounts, or the sale of personal information on the dark web.

OVERVIEW OF BC PRIVACY LEGISLATION

In British Columbia, the protection of personal information is governed by FIPPA and PIPA.

- FIPPA applies to public bodies, such as provincial ministries, local governments, health authorities, and post-secondary institutions.
- PIPA applies to private sector organizations, including businesses, non-profits, and trade unions.

These Acts require public bodies and organizations to put reasonable security measures in place to protect personal information and guard against breaches and identity theft. The OIPC oversees compliance with these Acts and can investigate how personal information is protected in British Columbia.

OTHER RELEVANT LEGISLATION

In addition to FIPPA and PIPA, several other laws address identity theft or provide protections for individuals in British Columbia.

Business Practices and Consumer Protection Act (BPCPA)

The BPCPA protects individuals from deceptive or unconscionable acts involving their personal information. Unconscionable acts include applying undue pressure, taking advantage of a person's vulnerability, or imposing grossly unfair contract terms.

As of August 1, 2026, under the BPCPA, credit reporting agencies must provide free credit freezes and security alerts to individuals upon request. They must also provide free monthly access to credit reports and scores. In addition, recent changes to PIPA mean that individuals may now withdraw their consent for credit reporting agencies to disclose their personal information to third parties. These are all tools that individuals can use if they are concerned that someone might be using their identity.

Personal Information Protection and Electronic Documents Act (PIPEDA)

This federal law governs the handling of personal information in commercial activities across Canada. In British Columbia, PIPEDA applies to federally regulated businesses, such as banks, airlines, and telecommunications companies, and to personal information that crosses provincial or national borders.

Criminal Code of Canada

Identity theft is a serious offence under the Criminal Code. Section 402.2 makes it illegal to obtain or possess another person's identity information with the intent to commit a crime. Section 403 defines identity fraud as the use of that information to impersonate someone, whether living or dead, to gain an advantage or cause a disadvantage.

FOR PUBLIC BODIES AND ORGANIZATIONS

Under FIPPA and PIPA, public bodies and organizations have a legal duty to protect personal information in their custody or control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, or disposal.

The OIPC has established that what is "reasonable" security depends on the specific circumstances of each case. Public bodies and their service providers must scale their security measures to the sensitivity of the personal information under their control and the corresponding harm that could result if a breach occurs.[1] This means that highly sensitive personal information, such as Social Insurance Numbers, Personal Health Numbers, and financial records, require more rigorous safeguards than less sensitive data. Personal information that may not be particularly sensitive on its own, such as a name or address, can

[1] For guidance on types of security measures to adopt, consider using ISO 27001, the NIST Cybersecurity Framework (CSF) 2.0, or a sector-specific standard, such as UL-2900-2-1.

become sensitive when combined with other information, particularly where there is a risk of identity theft. Organizations should consider how personal information may be combined with other information when determining appropriate safeguards.

Recommended security measures

To meet the legal standard for security, the OIPC recommends a combination of administrative, technical, and physical protections. Some examples include:

- **administrative:** public bodies and organizations establish clear privacy policies and train all employees on secure data handling, including how to recognize phishing and social engineering. Any contracts with third-party service providers include specific clauses requiring the provider to maintain an equivalent level of security for information in their care;
- **technical:** these safety measures should include:
    - **access controls:** access to personal information is restricted to employees who require it to perform their duties, and access is granted based on roles or job functions. This is managed through unique user login credentials and the maintenance of audit logs, which are reviewed regularly to detect unauthorized or unusual access. Where appropriate and proportional to the sensitivity of the information, enhanced authentication mechanisms, such as multi-factor authentication, are used to strengthen access controls;
    - **encryption and devices:** industry-standard encryption is used for all sensitive information, particularly when stored on mobile devices or transmitted over public networks. Public bodies and organizations must also make sure that devices are regularly updated and patched, and that endpoint security is maintained; and
    - **data minimization:** personal information is collected, used, and retained only as necessary for business purposes.
- **physical:** physical records are stored in locked filing cabinets or secure rooms with restricted access. Workstations are positioned so that personal information is not visible to unauthorized individuals. For areas containing highly sensitive information, additional safeguards such as key-card or fob access, security codes, or visitor logs are in place as appropriate. When personal information is no longer required for legal or business purposes, it is destroyed securely through cross-cut shredding or permanent digital deletion.

Please see the OIPC's guidance on Securing personal information: A self-assessment for public bodies and organizations for detailed information.

Breach response protocol

The OIPC has published resources for public bodies and organizations that experience a privacy breach.[2] In these resources, the OIPC sets out a four-step response process when a privacy breach is suspected or confirmed:

Step 1: Contain the breach

Immediately take steps to stop the unauthorized access or disclosure. This may include recovering lost records, shutting down a compromised system, or revoking system access.

Step 2: Evaluate the risks

Determine what information was breached and how many individuals are affected. Assess whether the breach has created a real risk of significant harm to those individuals. Significant harm includes identity theft, financial loss, or damage to reputation.

Step 3: Notify

Under FIPPA, public bodies must notify the OIPC and affected individuals without unreasonable delay if there is a real risk of significant harm. While PIPA does not currently mandate notification for organizations, the OIPC strongly recommends it in similar circumstances to allow individuals to protect themselves from identity theft.

Step 4: Prevent future breaches

Once the immediate crisis is managed, investigate the cause of the breach. Update security policies, fix technical vulnerabilities, and provide additional staff training to prevent a recurrence.

Support for affected individuals

When a privacy breach poses a risk of identity theft, a key part of mitigating the potential harm caused by the breach is for public bodies and organizations to provide affected individuals with resources to help them protect their information.

To determine if there is a real risk of significant harm, public bodies and organizations need to consider several factors, including:

- the sensitivity of the personal information;
- the amount and types of information involved;
- the likelihood that the information could be misused;
- the circumstances of the breach, such as how the information was exposed; and

[2] See Privacy breaches: tools and resources for public bodies, Privacy breach checklist for public bodies, and Privacy breach checklist for private organizations.

- whether it could be combined with other information in a way that increases the risk of harm.

The OIPC provides specific privacy breach checklists for both public bodies and organizations to help evaluate these factors.[3]

Identity theft often involves connecting multiple types of personal information from different sources, and unauthorized access to that information may go undetected. This may make it difficult to trace a case of identity theft back to a specific system. For this reason, public bodies are encouraged to consider whether a breach *might* have occurred whenever there's evidence of identity theft and respond accordingly.

If there is reason to suspect that identity theft has or is likely to occur, public bodies and organizations should offer identity theft protection services to those at risk. They should also take precautions to respond proactively to risk and contain potential harm rather than waiting for irrefutable proof of damage from a breach. These services can include:

- alerts when new credit accounts or inquiries are made in the individual's name;
- monitoring for the sale or trade of personal information on the dark web and in underground forums;
- access to specialists who help victims recover their identity and correct their records if fraud occurs;
- monitoring of financial accounts for unusual transactions or changes to personal information;
- monitoring of public records for unauthorized changes to addresses or other personal details;
- specialized monitoring services for children to detect misuse of their personal information; and
- services that help reduce the public availability of personal information online.

The selection of services and length of time the services are provided should be based on the sensitivity and breadth of the personal information, as well as the level of risk:

- a period of one to two years is standard for most breaches; and
- a minimum of five years of coverage is recommended in cases where there is evidence to show that affected individuals' personal information is on the dark web.

[3] Privacy Breach Checklist for Public Bodies, Privacy Breach Checklist for Private Organizations .

Public bodies and organizations should provide clear, written instructions to affected individuals on how to:

- obtain the offered identity theft monitoring services;
- place security alerts with Equifax and TransUnion, the two main credit reporting agencies in Canada;
- monitor bank and credit card statements for unauthorized activity; and
- report the incident to the Canadian Anti-Fraud Centre and local police or RCMP detachment.

If a public body or organization has reason to believe that identity theft has, or is likely, to occur, the OIPC expects them to notify affected individuals directly and encourage them to use the offered services. Website notices should only be used as a last resort if direct contact information is unavailable. Making sure individuals are aware of and using these services is an essential part of the legal duty to mitigate harm.

FOR INDIVIDUALS

While public bodies and organizations have a duty to protect the information in their custody, individuals can also take proactive steps to reduce their risk of identity theft.

Steps to help prevent identity theft

To reduce your risk of identity theft, you can:

- Make sure that any physical documents containing sensitive information, such as Social Insurance Numbers, Personal Health Numbers, or financial details, are stored securely. When these documents are no longer needed, it is safer to shred them rather than placing them in recycling or garbage bins;
- use unique, strong passphrases[4] for every online account and avoid using the same passphrase across multiple platforms. Consider using passkeys, when available, and a password manager to store your unique passwords. Whenever possible, enable multi-factor authentication (MFA) to add an extra layer of security;

[4] The Canadian Centre for Cybersecurity recommends using passphrases as they are longer and easier to remember than a password made up of random, mixed characters https://www.cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032.

- keep your devices secure with reputable antivirus software and regular updates to prevent malware and hacking. These updates often include critical security patches that fix vulnerabilities, making it harder for unauthorized users to access your data;
- avoid using public Wi-Fi for financial transactions or accessing sensitive accounts. Public networks are often unencrypted, which can allow others to intercept your information. If you must access these accounts while away from home, use a Virtual Private Network (VPN) or your mobile device's data hotspot instead;
- be cautious of unsolicited emails or text messages asking for personal information, as these are often phishing attempts designed to steal log-in credentials and account information;
- only provide your personal information when it is necessary for a specific service. Before sharing sensitive details like your Social Insurance Number, ask why it is being collected, how it will be protected, and if there is an alternative form of identification you can provide instead; and
- regularly review your bank and credit card statements for any unauthorized transactions or suspicious activity. You can also request a free copy of your credit report from Equifax and TransUnion to review for suspicious credit activity and to make sure that no unauthorized accounts have been opened in your name.

Steps to take if you believe your information has been compromised

If you receive a breach notification from a public body or organization or suspect that your identity has been stolen, it is best to take immediate action to mitigate the risk of further harm. For example, you could:

- immediately change the passphrases for your email and any other online accounts that may have been involved in the breach. If you use the same log-in credentials for multiple accounts, update those as well and enable multi-factor authentication (MFA) to prevent unauthorized access;
- immediately contact your bank and credit card issuers to report any unauthorized transactions. You may also ask to have your accounts flagged for extra security or, if necessary, closed and replaced with new account numbers and PINs;
- contact both Equifax (1-800-465-7166) and TransUnion (1-800-663-9980) to place a security alert on your credit file. This requires creditors to take extra steps to verify your identity before opening new accounts;
- notify your local police department or RCMP detachment and obtain a file number, as this may be required by banks or insurance companies. You may also report the theft to the Canadian Anti-Fraud Centre (1-888-495-8501), which tracks identity theft and fraud across the country; and

- if your government-issued identification is missing or compromised, contact the issuing agency to have it cancelled and replaced. This includes contacting ICBC for your driver's licence and Health Insurance BC for your Personal Health Number. If your Social Insurance Number (SIN) is involved, contact Service Canada and the Canada Revenue Agency (CRA) to report the potential for tax-related fraud.

Complaints

If you believe that a public body or organization has failed to protect your personal information or has not followed the requirements of FIPPA or PIPA, you have the right to file a complaint with the OIPC. The OIPC can investigate public bodies and organizations for compliance with the law; however, the office does not have the authority to award financial compensation or damages. If you are seeking financial remedy, you need to pursue other options, such as seeking legal advice.

If you decide to complain to the OIPC, you must first submit your complaint in writing to the specific public body or organization involved. It is best to clearly explain what happened, how it has affected you, and what you would like them to do to resolve the issue.

Public bodies and organizations should provide a written response to your concern. If you are unsatisfied with the response, or if they fail to respond within a reasonable timeframe, you may file a complaint with the OIPC.

Your complaint to the OIPC must be submitted in writing and should include:

- a copy of your original letter to the public body or organization;
- a copy of their response (if provided); and
- a brief explanation of why you believe the matter remains unresolved.

CONCLUSION

Protecting personal information is everyone's job. While public bodies and organizations have a legal duty to implement reasonable security measures, individuals are encouraged to monitor their own information regularly and respond quickly if a breach occurs.

For further information, please visit our website at www.oipc.bc.ca or contact:

Office of the Information and Privacy Commissioner for British Columbia
PO Box 9038 Stn Prov Govt
Victoria BC, V8W 9A4
Email: info@oipc.bc.ca
Phone: (250) 387-5629

Callers outside Victoria can contact the office toll-free by calling Service BC and requesting a transfer to (250) 387-5629.

Service BC: Vancouver: (604) 660-2421; Elsewhere in BC: (800) 663-7867

APPENDIX A: RELATED RESOURCES FOR PUBLIC BODIES AND ORGANIZATIONS

Public bodies and private sector organizations

- Securing personal information: A self-assessment for public bodies and organizations

Public bodies:

- Accountable Privacy Management in BC's Public Sector: This document provides step-by-step guidance for British Columbia public bodies on how to implement effective privacy management programs.
- Privacy breaches: tools and resources for public bodies
- Privacy breach checklist for public bodies

Organizations

- Getting Accountability Right with a Privacy Management Program: Guidelines for private sector organizations to build a privacy management program step-by-step.
- Privacy management program self-assessment
- Privacy breaches: tools and resources for the private sector
- Privacy breach checklist for private sector organizations

APPENDIX B: CHECKLIST FOR INDIVIDUALS

This checklist provides practical steps you can take to protect your privacy and respond to identity theft.

Prevention and protection

- ☐ Store physical documents, such as SIN and PHN cards, securely and shred them when no longer needed.
- ☐ Use unique, strong passwords and enable multi-factor authentication for online accounts.
- ☐ Review bank and credit card statements monthly for any unauthorized transactions.
- ☐ Request a free credit report from Equifax and TransUnion.
- ☐ Ask organizations why they need your personal information before providing it.

Steps to minimize impact

- ☐ Contact your bank immediately to flag accounts or issue new cards and PINs.
- ☐ Contact Equifax (1-800-465-7166) and TransUnion (1-800-663-9980) to place a security alert or credit freeze.
- ☐ Report the theft to local police for a file number and notify the Canadian Anti-Fraud Centre (1-888-495-8501).
- ☐ Contact ICBC (Licence), Health Insurance BC (PHN), and Service Canada (SIN) to cancel and replace compromised documents.

The complaint process

- ☐ Submit a written complaint to the public body or organization.
- ☐ Allow the public body or organization 30 business days to provide a written response. If the matter is not resolved, file a complaint with the OIPC.

PO Box 9038 Stn. Prov. Govt. Victoria BC V8W 9A4 | 250-387-5629 |

Toll free in BC: 1-800-663-7867 info@oipc.bc.ca | oipc.bc.ca | @BCInfoPrivacy