

Social Insurance Number (SIN) Information for ORGANIZATIONS AND EMPLOYERS

As an organization or employer, you have a key role in the protection of the SIN. You have a duty to protect the personal information that your employees and clients entrust to you. This is to prevent misuse, fraud, and identity theft.

You should only collect and use your employees' or clients' SINs as the law requires. For example, if you are an employer, you have a legal obligation to collect your employees' SINs. This is to report income for tax, employment insurance, and public pension program purposes.

You should avoid collecting and using the SIN for any other reasons that the law doesn't require. This is to reduce the risk of harm to your employees and clients if you experience a privacy breach like a cyberattack.

Collecting the SIN

Employers collecting the SIN from Employees

You must:

ask for an employee's SIN when they start work

Don't ask for a person's SIN until you hire them. You must ask the employee for their SIN within 3 days of the start of the employment. If they don't have a SIN, they can still work if they apply for one. You must never apply for an employee's SIN for them. The employee must provide their SIN to you within 3 days of beginning work, or within 3 days of receiving their SIN.

verify an employee's identity and ensure they are entitled to work in Canada

Don't ask for the SIN card or confirmation of SIN letter as proof of identity. Your employees don't need to show you physical proof

of their SIN. Instead, ask for pieces of identification as proof of identity. If the SIN begins with 9, ask to see the employee's work or study permit. If you suspect the SIN is invalid or being used fraudulently, call Service Canada at 1-866-274-6627.

keep SIN information confidential and secure

Protect employees' SIN and personal information from unauthorized access. Keep it in a secure area or an encrypted computer system. Don't use or disclose it except for reasons required by law. Don't retain SINs and personal information for longer than you need to. When you no longer need to retain it, dispose of it securely.

MORE INFORMATION

- [Information for employers](#)
- [Employers' dos and don'ts: requesting, collecting, using, and storing the SIN](#)
- [Personal Information Retention and Disposal: Principles and Best Practices](#)



Organizations collecting the SIN from Clients

You should:

✔ collect the SIN only when the law requires it

You can't refuse to provide a service or product to someone if they don't provide their SIN, unless the law requires it. You should ask for other documents to verify a client's identity. You should offer alternatives to providing the SIN if you need a credit report.

✔ take privacy and security seriously

Inform your clients about the personal information you are collecting and using. Don't use or disclose your clients' personal information without their consent or for reasons beyond what the law requires. Keep client

information confidential and secure. Don't retain personal information for longer than you need to. When you no longer need to retain it, dispose of it securely. Identify a privacy officer and establish a privacy framework within your organization.

MORE INFORMATION

- [Information for private sector organizations](#)
- [Private sector dos and don'ts: requesting, collecting, using, and storing the SIN](#)
- [Personal Information Retention and Disposal: Principles and Best Practices](#)

Handling Privacy Breaches involving the SIN

Organizations managing a privacy breach involving the SIN should take the following steps:

✔ follow the applicable federal, provincial, or territorial requirements or guidelines for handling privacy breaches and for breach notification

You must follow the requirements of the privacy legislation that applies to your organization. Find out more about the [privacy laws in Canada](#).

✔ assess the damage

Figure out the type and extent of personal information compromised. Find out when it happened and what information was compromised. If the case involves digital files, find out if the data was encrypted. Consider:

- what information could be compromised?
- when and how did it happen?
- where and how was the information stored?
- what security measures were in place?

✔ contact the police and the Canadian Anti-Fraud Centre if any criminal activity occurred

If the privacy breach involved a cyberattack, theft, or fraud, contact the police and the Canadian Anti-Fraud Centre (1-800-495-8501).

✔ contact Service Canada

Service Canada may be able to help you figure out next steps. Service Canada may also be able to help you to reduce the damage to victims of the breach. Contact Service Canada's [Social Insurance Number Program](#).

✔ contact Equifax and TransUnion (Canada's 2 major credit bureaus)

The credit bureaus may be able to offer you their data breach services. Call Equifax at 1-855-233-9226 and TransUnion at 1-800-663-9980.

✔ contact the authority for privacy laws in your jurisdiction

You may need to report the privacy breach by law. You may need to [report the privacy breach to the Office of the Privacy Commissioner](#). You may need to report the privacy breach to an equivalent authority in your province or territory. Find out more about the [privacy laws in Canada](#).

✔ contact the individuals whose information was breached

Notify the affected individuals in writing as soon as possible. The notification should:

- explain the incident
- describe what measures your organization has taken
- explain what type of information may be at risk
- consider offering free credit monitoring services
- provide advice on what affected individuals should do
- provide SIN information and resources
 - [Protecting Your SIN](#)
 - [SIN Code of Practice](#)
- provide contact information for:
 - a representative from your organization
 - credit bureaus
 - Service Canada