



Office of the Information & Privacy
Commissioner of Alberta



OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
— for —
British Columbia

USE OF SOCIAL INSURANCE NUMBERS BY PRIVATE SECTOR ORGANIZATIONS

APRIL 2005

The social insurance number (SIN) is an identification number created under federal law for the purpose of administering certain specified federal government laws and programs, for example, income tax and the Canada Pension Plan. An individual's SIN is the personal information of the individual to whom it has been assigned.

Inappropriate use of the SIN poses serious privacy risks for individuals. The SIN can be used in crimes such as identity theft and fraud. Along with other personal information, a person may be able to use someone else's SIN to apply for a credit card, open a bank account, rent vehicles or accommodation in the other person's name, possibly leaving the victim responsible for the bill or a bad credit rating.

Computer technology makes it possible to use the SIN to find and match personal information from one database to another. Data matching using the SIN can create a detailed profile about individuals without their knowledge. The availability of detailed data profiles about individuals can place them at a disadvantage in their interactions with public bodies, organizations and other individuals, which could negatively affect them in areas such as employment, personal mobility, financial negotiations and personal relationships.

Private sector organizations covered by the *Personal Information Protection Act* (PIPA) are subject to rules governing their collection, use and disclosure of individuals' personal information. The SIN is personal information under PIPA and therefore its collection, use and disclosure are subject to PIPA.

Please read the important notice at the end of this document about the nature and status of this document.

GENERAL POSITION

The SIN may be requested by organizations because certain laws require its collection. For example, employers must collect the SIN of their employees for taxation purposes. Unless an organization is legally required to ask for the SIN, it should generally refrain from doing so and individuals should generally not give their SIN to an organization unless the organization is legally required to collect it. Before providing their SIN, individuals should ask the organization to specify the legal requirement to collect it.

There may be circumstances where an organization is not legally required to request the SIN but asks for it. We generally discourage individuals from providing their SIN unless it is legally required. However, an individual may provide their SIN to an organization if the individual is satisfied it is reasonable and necessary in the circumstances for the organization to request it and the notice and consent requirements of PIPA are followed.

Employees are required to provide their SIN to their employers for payroll purposes for providing them with records of employment, income tax and other similar purposes.

Because financial institutions such as credit unions, trust companies and securities dealers must report customer income, including income from interest-bearing accounts, they are required by federal law to obtain their customers' SINs for those purposes. However, if a customer's account with a financial institution is not interest-earning, the organization is not required by law to obtain the customer's SIN.

The following section describes PIPA's requirements in more detail as they relate to voluntary supply of SINs.

PRIVATE SECTOR ORGANIZATIONS & THE SOCIAL INSURANCE NUMBER

1. Notice of the purpose for collection

- An organization:
 - must notify individuals, orally or in writing, of the purpose for collecting the SIN at the time of collection,
 - must clearly specify whether it is requesting the SIN for income-reporting purposes, other legally required purposes, or for identification purposes,
 - that asks for the SIN for income-reporting or other legally-required purposes must clearly indicate that it is required by law to collect the SIN and specify these purposes,
 - that asks for the SIN for identification or credit check purposes only must clearly indicate that the SIN is optional,

- that is legally required to collect the SIN but intends to use it for other purposes such as identification, credit checks or debt collection must, at the time of collection, clearly specify this.

2. **Consent of the individual**

- An organization that collects the SIN for purposes other than those legally required must get the individual's consent in writing or verbally.
- An organization that collects the SIN for purposes that are reasonable and have been clearly communicated to the individual at the time of collection can treat the individual's provision of the SIN as consent.
- PIPA allows collection, use and disclosure of personal information reasonably required to establish, manage or terminate an employment relationship and employee consent to collection, use or disclosure of the SIN is not required in such cases. Employers should, however, only collect, use and disclose employee SINs where they are legally required to do so. It is not reasonable to collect and use SINs for employee identification purposes without employee consent. Organizations should be asking employees to consent to collection and use of their SINs for identification purposes.
- PIPA prevents an organization from requiring an individual to give personal information as a condition of supplying a product or service unless the personal information is necessary to supply the product or service. A SIN is "necessary" only where the SIN is legally required. If an organization is asking for the SIN for identification purposes only, it must not in any way suggest to the individual that the SIN is required as a condition of supplying a product or service.
- In transactions where it is reasonable for an organization to ask a customer for proof of identity, the organization must make it clear to the customer that any request for the SIN is optional and that the customer is not required to provide it. An organization may ask for the SIN as one option among others, but should never purport to require it.
- When a financial institution or other organization that is giving credit to an individual needs to confirm the individual's identity to obtain a credit check, the organization may ask for the SIN as one identification option, but it should not be required as a condition for granting credit.
- Where the SIN is for identification purposes, an organization must provide a convenient mechanism for the individual to withdraw consent at any time after providing the SIN. The mechanism should be clear, inexpensive, easy to execute and effective at once.

3. **Use and disclosure of the SIN only for notified and agreed-to purposes**

- PIPA prohibits an organization that has collected an individual's SIN from using or disclosing the SIN for purposes other than the purpose to which the individual consented.

- An organization must not use the SIN for any purpose not previously identified without first specifying the new purpose and obtaining the individual's consent to the new use. In other words, if the organization originally specified only income-reporting as the purpose for collecting the SIN, it must seek the individual's consent before using the SIN for other purposes.

4. **Security measures to protect SINs**

- Organizations covered by PIPA are required to make reasonable security arrangements to protect individuals' personal information from unauthorized collection, access, use, disclosure, copying, modification, disposal or destruction. Personal information includes the SIN, which can be very valuable for identity thieves, fraud artists and others.
- Any organization that collects SINs should take reasonable steps to ensure they are protected from theft or loss and to ensure that, when they are disposed of, they are disposed of securely. SINs should be kept under lock and key in paper form and be encrypted or at least password protected, in a segregated place, where they are kept in electronic form.
- Organizations should limit access to SINs to only those employees who absolutely must have access to them to do their work. These employees should be required to sign confidentiality agreements and should be aware of possible disciplinary consequences for their misuse of another individual's SIN.

This publication is jointly produced by the Offices of the Information and Privacy Commissioners of British Columbia and Alberta.

This document has drawn on *Best Practices for the Use of Social Insurance Numbers in the Private Sector*, published by the Office of the Privacy Commissioner of Canada, which regulates the privacy practices of federal government institutions and certain private sector organizations: http://www.privcom.gc.ca/fs-fi/02_05_d_21_e.asp.

This document is also based on findings in Investigation Report P2004-IR-001, issued by the Alberta OIPC regarding private sector use of the SIN for credit check purposes: <http://www.oipc.ab.ca/ims/client/upload/P2004-IR-001.pdf>.

This document is for general information only. It is not intended to be, and cannot be relied upon as legal advice or other advice. Its contents do not fetter, bind, or constitute a decision or finding by the Office of the Information and Privacy Commissioner (OIPC) of BC or of Alberta with respect to any matter, including any complaint, investigation or other matter, respecting which each OIPC will keep an open mind. Responsibility for compliance with the law (and any applicable professional or trade standards or requirements) remains with each organization.