

This Privacy Statement provides an overview of the Privacy Management Program (PMP) implemented by SBI Canada Bank, (hereinafter referred to as “SBIC”, the “Bank”, “we” and “us”) for complying with the *Personal Information Protection and Electronic Documents Act (PIPEDA)* as well as guidelines and interpretation bulletins issued by the Office of the Privacy Commissioner (OPC).

Table of Contents

Privacy Management Program at SBIC	1
What is Personal Information?	1
Identifying Purposes	2
Your consent is important!	2
How do we limit collection of personal information?	3
How do we limit the use of personal information?	3
How do we limit the retention of personal information?	3
Do we disclose personal information to External Parties?	3
• Service Providers	3
• Production Orders and Requests for Information	4
How do we ensure that the Personal Information held by us is accurate?	4
How do we protect your Personal Information?	4
Accessing your Personal Information held by SBIC	5
• Request for information	5
• Timeframe	5
• Cost	5
• Alternative Format	5
• Refusal to provide access	5
Do you have any questions?	6

Privacy Management Program at SBIC

The PMP implemented by SBIC includes a privacy policy, detailed procedures, physical and electronic access controls, staff training, and periodic assessment of the effectiveness of and ongoing compliance with the PMP. Each employee of the Bank is responsible for complying with the Privacy Policy and associated procedures and for protecting the personal information under their control. The Bank provides training on privacy requirements to all staff members and senior management on periodic basis.

What is Personal Information?

The term “Personal Information” can be defined as a set or combination of information that can be used to identify an individual. The Personal Information of clients collected, used, or disclosed by SBIC includes the following:

- Name
- Age / Date of birth
- Principal Occupation / Nature of Business
- Address
- Identification Documents (IDs)

- Reports provided by service providers such as credit reports and reports used for verifying the identity of clients
- Loan records and debt-related information. For example, mortgage applications, residential property appraisal documents including the selling/purchase price of an individual's home, etc.
- Video surveillance that captures an individual's physical image or movement while visiting a branch or automated teller machine (ATM) of SBIC
- Internet Protocol (IP) address, customers' online and mobile banking profile details, login ID, and transactions' information for billing purposes

In addition to the above,

- our digital platforms, such as our internet banking platform, our mobile apps, and third party solutions provided through them, might use cookies to identify users and their preferences for developing a personal customized experience for them, and
- we might also become aware of or come into possession of certain information about our clients. For example, checks deposited by clients bear certain details of the issuer and wire transfers received by us include details of the sender/remitter.

Identifying Purposes

To ensure that the purpose of collecting any Personal Information is identified at the time of or before collection, SBIC uses standard forms for collecting personal information. Each form includes the name of a specific product or service or a unique name that identifies the purpose of collecting the details required in the form. For example, Personal Account Opening Form, Application Form for Money Transfer, etc. All forms used by the Bank are approved by the Privacy Officer of the Bank who ensures that only such details are collected that are relevant to providing the product or service.

Your consent is important!

SBIC notifies and seeks consent from the individual about whom the personal information is collected at or before the time of collection, except under certain circumstances as exempted under PIPEDA. As mentioned earlier, SBIC uses standard forms that identify the purpose of collection. By completing these forms and providing them to the Bank, the clients provide their consent for collection, use, and disclosure of their information in accordance with the applicable terms and conditions. SBIC might seek consent orally when information is collected over the phone or electronically when information is collected through phone banking. The Bank might also use innovative processes that can be used to obtain the consent at the time of disclosure. If personal information that has been collected earlier is to be used for a purpose not previously identified, the Bank seeks consent from the individual prior to using the information for the new purpose. This does not apply if the new purpose is required by law.

By completing an application for a product or service, the customers consent to the following:

- collection of their Personal Information by the Bank directly from them or from a service provider, including credit bureaus; and
- use and disclosure of their Personal Information by the Bank to, amongst other purposes, identify them, protect them and the Bank from error and fraud, understand their financial needs and eligibility for products and services, recommend particular products and services that meet their financial needs - unless the Customer has "opted out" of such use, provide ongoing service, and for Bank's compliance with legal and regulatory requirements.

In accordance with PIPEDA, the Bank might collect use, or disclose Personal Information without the knowledge and consent of an individual under certain circumstances. This includes circumstances where seeking consent is impossible or impractical due to legal, medical, or security reasons; where information is being collected and or disclosed for the detection and prevention of fraud or for law enforcement; or when the individual is a minor, seriously ill, or mentally incapacitated. In such events, the Bank takes

reasonable measures to ensure that the collection, use, or disclosure is made in accordance with the exceptions provided in PIPEDA. In this context, reasonable measures include but are not limited to conducting and documenting a review of the exceptions provided under PIPEDA, referring the matter to the Privacy Officer of the Bank, or referring the matter to an external consultant.

The Bank allows its clients to withdraw their consent subject to legal or contractual restrictions and reasonable notice. If a client withdraws his/her consent, the Bank informs them about the implication of such withdrawal. Rest assured that SBIC does not obtain consent through deception or collect personal information through unfair, unlawful, or unethical means.

How do we limit collection of personal information?

We only collect personal information that is essentially required. In this context, essentially required information refers to the set of information that is required by the Bank to provide the product or service required by the clients, perform its functions, or comply with the applicable legislative and regulatory requirements. As mentioned earlier, all forms used by the Bank are approved by the Privacy Officer of the Bank who ensures that only such details are collected that are relevant to providing the product or service.

How do we limit the use of personal information?

In accordance with PIPEDA and guidance issued by OPC, SBIC collects, uses, or discloses personal information only for purposes that a reasonable person would consider as appropriate under the circumstances. The personal information collected by us is used only for the identified purposes. If personal information that has been collected is to be used for a purpose not previously identified, we identify the new purpose prior to using the information.

Profiling or categorization might lead to unfair, unethical, or discriminatory treatment contrary to human rights law. SBIC does not engage in any exercise that might create or increase the risk of unfair, unethical, or discriminatory practices.

How do we limit the retention of personal information?

We retain personal information in accordance with the various legislative and regulatory requirements that apply to all banks in Canada and only as long as necessary for the fulfillment of the identified purposes. For example, Personal Information that has been used to make a decision about an individual is required to be retained long enough to allow the individual to access to the information after the decision was made. The Bank retains personal information that is or was the subject of an Access Request as long as necessary for the individual making the request to exhaust any recourse provided by law. Personal Information that is no longer required to fulfill the identified purposes is destroyed, erased, or made anonymous by the Bank in accordance with the applicable legislative and regulatory requirements pertaining to record keeping as well as the Record Management Policy and other policies and procedures implemented by the Bank.

Do we disclose personal information to External Parties?

- **Service Providers**

In order to provide you with world class banking services, SBIC uses certain services provided by State Bank of India (the parent bank) and/or external service providers, operating within and outside Canada. Therefore, the Bank transfers certain personal information of clients to the parent bank and external service providers. This includes, but is not limited to, personal information such as name, date of birth, address, identification document details, transactions information, information related to money transfers, and credit history. The information that is transferred by the Bank to the parent bank or any other service provider is only used for the purpose for which it was originally collected. The personal information transferred to another jurisdiction might be accessed by the courts as well as law enforcement and national security authorities of that jurisdiction.

The Bank uses service level agreements (SLA) to ensure that a comparable level of protection is provided when Personal Information is transferred by the Bank. The SLAs are developed in accordance with PIPEDA as well as guidelines issued by the OPC and *Office of the Superintendent of Financial Institutions* (OSFI). This includes measures to be taken by both parties during the process of transferring/sharing of the information, on an ongoing basis during the term of the agreement, and upon termination of the agreement.

SBIC might also receive information from the parent bank or external service providers as part of the services provided by them.

- **Production Orders and Requests for Information**

From time to time, SBIC might be served with production orders or requests for information from law enforcement or other government agencies such as the Canada Revenue Agency (CRA). Before providing the requested information in any such event, the Bank ensures that the disclosure is made in accordance with PIPEDA and is limited to the information requested in the production order or request for information. Before disclosing the requested information, the Bank satisfies itself with the genuineness of the production order or the lawful authority of a request for information made by an individual representing a law enforcement agency, any other government institution, or part of a government institution.

How do we ensure that the Personal Information held by us is accurate?

We make reasonable efforts to ensure that personal information collected, used, or disclosed by us is accurate, complete, and current. In this context, making reasonable efforts include obtaining the information from the individual. We do not routinely update personal information unless we are required to do so to fulfill the purposes for which the information was collected or it is required by law. To ensure accuracy of information, the Bank might also take measures to validate the information provided by client by verifying it with the information under its control or with the information that is publicly and /or commercially available.

An individual can challenge the accuracy and completeness of the information provided to him/her by the Bank and have it amended as appropriate. The Bank will take appropriate measures if an individual successfully demonstrates the inaccuracy or incompleteness of Personal Information held by the Bank. Depending upon the nature of the information challenged, the Bank will amend, make correction, delete, or add information in its records. If required, the amended information will be provided to affiliated entities and service providers having access to the same information.

How do we protect your Personal Information?

A privacy breach is defined as an unauthorized access to or collection, use, or disclosure of personal information. A privacy breach might lead to various consequences that might cause a significant harm to the individual. In accordance with the Digital Privacy Act, the term "Significant Harm" include bodily harm, humiliation, damage to reputation or relationship, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record, and damage to or loss of property.

SBIC has implemented various safeguards to protect the personal information collected, used, or disclosed by it against loss and unauthorized access, disclosure, copying, use, or modification. For example, access cards are required to access various areas of the Bank, technological controls are in place to protect the digital information, physical records are maintained in locked filing cabinets, and all staff members are required to sign a confidentially agreement at the time of their employment. However, if the Bank determines at any point in time that the Personal Information collected, used, or disclosed by it might have been subject to a privacy breach and that the breach might result in Significant Harm to its clients, SBIC would immediately notify OPC and the concerned individuals.

Accessing your Personal Information held by SBIC

- **Request for information**

We will inform any individual, upon receiving a written request, of the existence, use, and disclosure of his or her personal information and will provide access to that information. This includes providing information about the use that has been made or is being made of the client's information and list of third parties to which it has been disclosed. In accordance with PIPEDA, the Bank will not give an individual access to personal information if doing so would likely reveal personal information about a third party, unless the information about the third party is severable.

- **Timeframe**

We will respond to an individual's written request within thirty days after the receipt of the request. The requested information will be provided or made available in a form that is generally understandable. In accordance with PIPEDA, we may extend the time limit for a maximum of thirty days if meeting the time limit would unreasonably interfere with the activities of the Bank or the time required to undertake any consultations necessary to respond to the request would make the time limit impracticable to meet. We may also extend the limit for the period that is necessary in order to be able to convert the personal information into an alternative format. If we extend the time limit for responding to a request, we shall, no later than thirty days after the date of the request, send a notice of extension to the individual, advising them of the new time limit, the reasons for extending the time limit and of their right to make a complaint to the OPC in respect of the extension.

- **Cost**

Access to your personal information would be usually provided at no cost. We would respond to an individual's request at a cost to the individual only if we have informed the individual of the approximate cost and the individual has advised the Bank that the request is not being withdrawn.

- **Alternative Format**

The Bank will give access to personal information in an alternative format to an individual with a sensory disability who has a right of access to personal information and who requests that it be transmitted in the alternative format if its conversion into that format is reasonable and necessary in order for the individual to be able to exercise rights defined in PIPEDA. The Bank does not readily maintain information in alternative format.

- **Refusal to provide access**

The Bank is not required to give access to personal information in the following circumstances:

- a. Providing access to requested information would reveal confidential commercial information,
- b. Providing access to requested information would reasonably be expected to threaten the life or security of another individual,
- c. The information was collected under a provision provided in PIPEDA that allows collection without knowledge or consent of the individual, or
- d. The information was generated in the course of a formal dispute resolution process.

If the information mentioned above is severable from the record containing other information for which access is requested, the Bank will give access after severing the information. The exceptions mentioned above do not apply if the individual needs the information because the individual's life, health, or security is threatened.

If the Bank is not able to provide access to all the Personal Information it holds about an individual, due to an exception as defined in PIPEDA, the reasons for denying access shall be provided to the individual.

Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

Do you have any questions?

SBIC has assigned a Privacy Officer who addresses privacy-related complaints. If you have any questions about SBIC's PMP, want to access your personal information maintained by SBIC, or have a concern about collection, use, or disclosure of your Person Information, the Privacy Officer of the Bank can be contacted by mail or email at the following addresses:

Privacy Officer
SBI Canada Bank
220 Bay Street, 10th Floor
Toronto, ON. M5J 2W4
Facsimile: 416-504-2040
Email: Privacy.Officer@sbicanada.com

The Privacy Officer investigates all privacy-related complaints. If a complaint is found to be justified, the Privacy Officer makes recommendations to the concerned function of the Bank to take measures, as deemed appropriate by the Privacy Officer and P&CEO of the Bank.