Privacy Policy

Version 2.0
Effective: December 16, 2013

Introduction

1. All banks in Canada are subject to *Personal Information Protection and Electronic Documents Act* (PIPEDA). This Act supports and promotes electronic commerce by protecting personal information that is collected, used, or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions.
In this context, the term "*Personal Information*" means information about an identifiable individual; however, it does not include the name, title, business address, or telephone number of an employee of an organization.
PIPEDA has two parts. The first part of the Act, *Protection of Personal Information in the Private Sector*, establishes rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.
The second part of the Act, *Electronic Documents*, provides for the use of electronic alternatives in the manner provided for in this Part where federal laws contemplate the use of paper to record or communicate information or transactions.
The *Office of the Privacy Commissioner of Canada (OPC)* has also issued several guidelines and interpretation bulletins that convey OPC's expectations of banks regarding compliance with PIPEDA.
This Privacy Policy (the "Policy") defines the enterprise-wide approach adopted by the SBI Canada Bank, hereinafter referred to as "SBIC" and the "Bank", for complying with PIPEDA as well as guidelines and interpretation bulletins issued by the OPC.

Scope of this Policy

2. This Policy applies to all directors, senior management, and employees of the Bank.
3. This Policy shall be read in conjunction with the other compliance-related policies and procedures issued by the Bank, especially the *Legislative Compliance Management Policy* and related procedures.
4. The Bank defines compliance with the policies and procedures of the Bank as well as the legal and regulatory requirements applicable to the Bank as a responsibility of every employee of the Bank.
5. A breach of this Policy by an officer or employee of the Bank may result in disciplinary action, which could lead to dismissal.
6. This Policy is subject to annual review and approval by the Board.

Protection of Personal Information

7. PIPEDA applies to the Bank in respect of the following types of personal information:
a. Personal Information that the Bank collects, uses, or discloses in the course of commercial activities; or
b. Personal Information about employees of the Bank that the Bank collects, uses or discloses in connection with its operations.
8. The Bank is required to comply with the following ten Privacy Principles as set out in

Schedule 1 of PIPEDA.
Principle 1. Accountability
Principle 2. Identifying Purposes
Principle 3. Consent
Principle 4. Limiting Collection
Principle 5. Limiting Use, Disclosure, and Retention
Principle 6. Accuracy
Principle 7. Safeguard
Principle 8. Openness
Principle 9. Individual Access
Principle 10. Challenging Compliance
9. SBIC shall also take appropriate steps in the event of a privacy breach. This includes taking measures to contain the breach; evaluating the risks associated with the breach; notifying the affected parties, if required; and implementing preventative solutions.

Privacy Process at SBIC

Accountability

10. SBIC is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The Bank shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

The Privacy Officer is responsible for establishing and managing compliance with the Privacy requirements applicable to the Bank. The contact details of the Privacy Officer made available on the website of the Bank and provided to clients upon request.
12. The role and responsibilities of the Privacy Officer are defined in the mandate of the Privacy Officer. The mandate is approved by the Audit Committee of the Board.
13. The Bank, with the authorization of Audit Committee of the Board, may delegate other individuals to act on behalf of Privacy Officer.
14. Each employee of the Bank is responsible for complying with this Policy and protecting the personal information under his/her control.
15. The Bank will provide training to all staff members and senior management to ensure compliance with the Privacy requirements. The training can be provided through in-person training sessions or through the computer-based training system used by the Bank.

Identifying Purposes

16. The Bank identifies the purpose for collecting personal information at or before the time of collection.
17. The purpose of obtaining clients' personal information shall be defined in the respective "Approach Paper" or product program. In this regard, the Bank has issued a Product Development Policy. This policy defines the process used by the Bank for introducing new products and services and making changes to its existing products and services.
18. If it is not feasible to provide written notice in advance, the individual can be notified orally.

In such cases, prior approval from the Privacy Officer of the Bank shall be obtained by the respective business function head.
19. The personal information collected by the Bank shall only be used for the identified purposes.
20. If personal information that has been collected is to be used for a purpose not previously identified, the Bank shall identify the new purpose prior to using the information.

Consent

21. The Bank notifies and seeks consent from the individual about whom the personal information is collected at or before the time of collection, except where it is inappropriate.
22. The Bank prefers to notify and clients about the purpose of collecting, using, and disclosing personal information and seeking consent from the clients in writing. In this regard, an application form is deemed to provide notice of the purpose.
23. The Bank shall use only standard forms for collecting personal information required providing products and services to clients. This approach will provide All client forms and applications used by the Bank shall be pre-approved by the Privacy Officer of the Bank. 24. The Bank may seek consent orally when information is collected over the phone, provided that the information is required to provide services or products required by the client.
25. If the Bank wishes to collect personal information of clients for marketing and research purposes or for any other specific purpose, prior approval from the Privacy Officer of the Bank shall be obtained by the respective business function head.
26. In accordance with PIPEDA - Schedule 1, the Bank can collect, use, or disclose personal information without the knowledge and consent of the individual only under circumstances where seeking consent may be impossible, inappropriate, or might defeat the purpose of collecting the information. This includes circumstances where seeking consent is impossible or impractical due to legal, medical, or security reasons; when information is being collected for the detection and prevention of fraud or for law enforcement; and when the individual is a minor, seriously ill, or mentally incapacitated.
27. If personal information that has been collected earlier is to be used for a purpose not previously identified, the Bank shall seek consent form the individual prior to using the information for the new purpose. This does not apply if the new purpose is required by law.
28. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. See sections 1.1 through 1.8 for currently identified purposes.
29. SBIC will not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified and legitimate purposes.
30. The Bank will not obtain consent through deception.
31. The Bank will allow its clients to withdraw their consent subject to legal or contractual restrictions and reasonable notice. If a client withdraws his/her consent, the Bank will inform the client about the implication of such withdrawal.

Limited Collection

32. The Bank shall 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, and comply with the applicable requirements.
33. The details of personal information that is required to provide any product or service shall be provided in the respective Approach Paper.
34. SBIC will collect personal information by fair and lawful means.

Limiting Use, Disclosure, and Retention

35. The Bank will not use or disclose personal information for purposes other than those for which it was collected, except with the consent of the individual or as required by law.
36. The Bank shall retain personal information only as long as necessary for the fulfillment of the identified purposes. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made.
37. Personal information that is no longer required to fulfill the identified purposes will be destroyed, erased, or made anonymous. This shall be applied in compliance with the legislative requirements pertaining to record keeping as well as policies and procedures issued by the Bank.
38. The Bank shares certain client details with the Parent Bank and external service providers for the purpose of processing client transactions and/or complying with the applicable legislative and regulatory requirements.

Accuracy

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

Safeguards

42. The Bank is responsible for implementing security safeguards to protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification.
43. The Bank collects and maintains personal information in paper as well as electronic/digital format and has implemented various security safeguards to protect it.
44. The Bank has implemented physical measures to restrict access to its offices and physical records maintained at various locations. In this regards, access cards are required to access various areas of the Bank and physical records are maintained in locked filing cabinets.

45. All staff members are responsible for safeguarding the access cards and key(s) provided to them by the Bank, protecting them from theft or loss, and promptly reporting any lost or

stolen key or card to their immediate supervisor as well as to the persons responsible for issuing access cards and keys.
46. The Bank provides certain information or provides access to certain information to all staff members of the Bank to enable them to perform their day-to-day activities. This includes personal information of clients and other staff members as well as information about the processes used by the Bank. The Bank requires all staff members to sign a confidentially agreement at the time of their employment. All staff members shall treat the information provided to them by the Bank as confidential and share it only with other staff members of the Bank on a need-to-know basis.
47. All staff members of the Bank are required to ensure that physical records under their custody are duly protected. Sensitive information shall not be left unattended during the day and shall be locked in filing cabinets at the end of each day.
48. The Bank has implemented technological controls to protect the digital information collected by it. These controls are defined in the *Information Technology and Information Security Policy* of the Bank. All staff members of the Bank are required to comply with the *Information Technology and Information Security Policy* of the Bank and ensure that computer terminals and laptops provided to them by the Bank are secured with passwords and digital records under their custody is duly protected.
49. The Bank will use contractual or other means to provide a comparable level of protection while personal information is being processed by a third party.

Openness

50. The Bank will make readily available to individuals its policies and practices specific information about its policies and practices relating to the management of personal information. The Bank is required to provide this information in a form that is generally understandable.
51. The Privacy Officer of the Bank may issue a privacy statement in a simple and clear language for the purpose of providing a generic overview of the privacy process adopted by the Bank to the clients. This statement shall include the following details:
a. The title and the office address of the Privacy Officer of the Bank who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;
b. The means of gaining access to personal information held by the Bank;
c. A description of the type of personal information held by the Bank, including a general account of its use;
d. A copy of any brochures or other information that explain the organization's policies, standards, or codes; and

e. Type of personal information that is generally disclosed by the Bank to affiliated entities and service providers for the purpose of providing services to clients.
52. The Privacy Officer will address specific requests about the privacy related processes adopted by the Bank on a case-by-case basis.

Individual Access

53. The Bank will inform an individual, upon request, of the existence, use, and disclosure of his or her personal information and will provide access to that information.

54. The Bank will respond to an individual's request within thirty days after the receipt of the request at minimal or no cost to the individual. The requested information will be provided or made available in a form that is generally understandable.
55. In accordance with PIPEDA, the Bank 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. The Bank 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.
56. If the Bank extends the time limit for responding to a request, the Bank 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.
57. The Bank shall respond to requests involving information provided by the Bank to a government institution or a part of a government institution in accordance with § 9. (2.1) of PIPEDA.
58. The Bank may respond to an individual's request at a cost to the individual only if the Bank has informed the individual of the approximate cost and the individual has advised the Bank that the request is not being withdrawn.
59. 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 under this Part. The Bank does not readily maintain information in alternative format.
60. 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.

61. An individual can challenge the accuracy and completeness of the information provided to him/her by the Bank and have it amended as appropriate.
62. 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.

Challenging Compliance

63. Any individual can challenge Bank's compliance with PIPEDA by writing to the Privacy Officer of the Bank. The Bank has issued a Compliant Resolution Brochure that provides the contact details of the Privacy Officer of the Bank as well as the contact details of the OPC.
64. The Privacy Officer of the Bank can be contacted by mail or email at the following addresses:
Privacy Officer

SBI Canada Bank
Suite 106, 77 City Centre Drive
Mississauga, ON L5B 1M5
Fax: 905-896-6545
Privacy.Officer@sbicanada.com

65. The Privacy Officer shall investigate all complaints. If a complaint is found to be justified, the Privacy Officer shall make recommendations to the concerned function of the Bank to take measures, as deemed appropriate by the Privacy Officer and P&CEO of the Bank.