PRIVACY CODE
FOR THE PROTECTION
OF PERSONAL INFORMATION

2011

PRIVACY CODE
FOR THE PROTECTION OF PERSONAL INFORMATION

PREAMBLE

The Bank and companies part of its group, including B2B Trust, have always thrived to preserve the accuracy, confidentiality, safety and privacy of its clients' business. True to this tradition, a Privacy Code for the Protection of Personal Information (the "Code") which sets out the goals and practices with respect to client privacy has been adopted. This Code is based on the *Model code for the Protection of Personal Information* published by the Canadian Standards Association (CAN/CSA-Q830-96) as well as on the principles set out in the *Personal Information Protection and Electronic Documents Act*, which became effective on January 1, 2001. The Code adopted by the Laurentian Bank Group (the "Group") regulates the collection, preservation, use and communication of personal information while preserving individuals' right to privacy. This Code governs the relations between the members of the Group and the clients whose personal information is held by such members.

The members of the Group referred to in this Code includes: Laurentian Bank of Canada, Laurentian Trust of Canada Inc., B2B Trust, LBC Trust, Laurentian Bank Securities Inc. and LBC Financial Services Inc. (hereinafter referred to collectively as "Members of the Group", "the Group" and individually as "a Member").

PRIVACY CODE
FOR THE PROTECTION OF PERSONAL INFORMATION

1. DEFINITIONS

Client: Person who uses or intends to use a product or service provided by one of the Members.

Collection of information: Act of collecting, receiving or recording personal information from any source and by any means.

Commissioner: The Privacy Commissioner appointed in accordance with Clause 53 of the *Personal Information Protection Act*.

Consent: Free assent. The consent may be expressed or implied; it may also be given by an authorized personal representative. The client may give his express consent orally, in writing or by electronic means. Express consent is unambiguous and is not influenced by the Member to which such consent is given.

Court: The Trial Division of the Federal Court.

Disclosure: Act of making personal information accessible to a third party.

Record: A record includes any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film microform, sound recording, videotape, machine readable record, and any other documentary material, regardless of physical form or characteristics, and any copy of it.

Direct marketing: Promotions aimed at clients whose personal information reveals that they may be interested in a specific product. Direct marketing includes telemarketing and centralized mailing activities but excludes statements sent on a regular basis, inserts included with statements, messages from automatic teller machines, announcements on electronic bulletin boards and actions directed at individuals or relating to customized management of a client's business.

Organization: Includes associations, partnerships, persons and labour organizations.

Personal information: Information about an identifiable individual, regardless of the format in which the information is consigned (eg: paper, email, database) including, but not limited to, his name, personal address, age, sex, identification numbers, income, employment, assets, liabilities, capital sources, repayment experience, personal references and medical records, credit and payment history, except for the name, title and work phone number of employees of an organization. Information such as identification of individuals to whom a Member has provided information and whether or not credit has been granted to these individuals may also constitute personal information.

Personal information of a medical nature: Any information concerning a living or deceased individual:

a) relating to physical or mental health;
b) relating to health services administered to such individual;

c) relating to the donation of body parts or bodily substances by such person, or to results of tests or examinations performed on such person's body parts or bodily substances;
d) obtained in connection with the delivery of health services to such person;
e) accidentally obtained while providing health services to such person.

Third party: A private individual or organization other than the Group.

Use: Management of personal information by or inside the Group.

2. SCOPE OF THE PRIVACY CODE FOR THE PROTECTION OF PERSONNAL INFORMATION

The Code only applies to personal information. It does not apply to information regarding businesses, nor to information about commercial accounts belonging to individuals involved in an organized economic activity, of a business nature or not, consisting in the production, management or the disposal of commodities, or in the delivery of services.

3. PRINCIPLES OF PRIVACY

The ten principles of privacy are:

1. Accountability of the Members
2. Identifying information collection purposes
3. Client's consent
4. Limitations regarding collection of personal information
5. Limitations regarding use, disclosure and retention of personal information
6. Updating personal information
7. Safeguards
8. Client access to standards and procedures
9. Client access to personal information regarding them
10. Settlement of complaints and processing of inquiries

Principle 1 - Accountability of Member

Each Member is accountable for the personal information in its possession, including information that has been disclosed to a third party for processing. It must set standards and procedures for this purpose and make one or more individuals accountable for ensuring compliance with the Code.

1.1 The senior management of every Member is ultimately accountable for protecting personal information regarding its clients. However, it may assign the daily administration of compliance monitoring mechanisms to one or more individuals who roles should be specifically outlined in the Member's procedures.

1.2 Each Member shall designate, internally as well as to its clients, the individual or individuals responsible for protecting personal information and monitoring compliance.

1.3 Each Member is responsible for personal information disclosed to a third party for processing purposes. Such personal information must be protected through a contract or agreement with the proposed third party.

1.4 To comply with the principles of the Code, every Member shall:

- establish procedures to protect the confidentiality of personal information;
- establish procedures to receive and address clients' complaints and inquiries;
- inform its clients and their staff about such procedures;
- train its own staff to understand and enforce such established procedures.

Each Member shall enforce compliance with the privacy principles through periodic surveys of risks or through compliance monitoring mechanisms. They shall report to the Board of Directors or one of its committees regarding compliance with the Code, as required.

Principle 2 - Identifying information collection purposes

Each Member must identify the purposes for which information is collected, at or before the time such information is collected.

2.1 When a client asks for a product or service, the Member must ensure that the client knows:

- why the Member needs the personal information which it is requesting from the client;
- for which other purposes the information could be used subject to the client's consent;
- that the Client is free to refuse to allow the Member to use his personal information for these other purposes.

There may also be other situations where Members might not explain such other purposes or might not seek the client's consent. Refer to paragraphs 3.4 and 5.1 regarding these situations.

2.2 Members shall only collect personal information in order to:

- understand the client's needs;
- determine the suitability and accessibility of products and services for the client;
- determine and manage products and services which meet the client's needs;
- offer products and services which satisfy such needs;
- provide current services;
- comply with laws and regulations.

2.3 Members shall specify the purpose of the information in writing, orally (either in person or by telephone) or by whatever means it usually communicates with the client. They shall use words which are easily understandable by the client.

If the information request is made by phone, they will tell the client, aside from such request, how they intend to use the information provided.

2.4 Member employees who collect personal information from clients should be able to explain to them the purpose for which the information is being collected. A client should be able to obtain an explanation as to why such information is needed when he phones the Member, visits one of its branches or writes to Customer Service. The Member may also seek personal information from external sources such as other lenders, credit bureaus, employers and from other sources of income, financial institutions and references.

2.5 The Member shall endeavour to explain to the client the purposes for which the collection of personal information may seem less obvious. The purpose of basic information such as the client's name, address, etc. is fairly straightforward, while other information will require clarification. For example, it would be appropriate to explain to the client that:

- references are needed to verify the accuracy of information recorded on a request form;
- the social insurance number is needed because the *Income Tax Act* requires it for the customer's income tax return;
- credit history is made available to credit bureaus, credit product insurers and other lenders in order to maintain the integrity of the credit granting process;
- information is required to open an account when purchasing securities;
- Information is required to determine client's needs.

Principle 3 - Client's consent

Each Member shall make reasonable efforts to ensure that the client understands the circumstances in which the personal information will be used or disclosed. The Member shall obtain the client's consent before or at the time of collecting, using or disclosing personal information regarding the client. Consent shall not be obtained through deceptive means.

The client's consent may be expressed or implied; it may also be given by an authorized representative, such as pursuant to a valid general power of attorney arrangement. The client may withdraw his consent at any time, subject to specified restrictions.

However, the Member may collect, use or disclose personal information without the client's consent for legal or security reasons or, in certain cases, in order to process such information.

3.1 The Member shall ensure, to the best of its abilities, that the client understands in which circumstances the personal information will be used or disclosed. It shall obtain the client's consent before or at the time of collecting, using or disclosing personal information regarding the client.

Generally, the Member will seek the client's consent while collecting the information. However, new uses may be found at a later time, in which case consent should be sought after the fact.

3.2 The Member must not rely on false pretences to secure the client's consent. It must explain to the client how it intends to use the personal information before asking for his consent.

3.3 The client may give his consent orally, in writing or through electronic means. Consent may be implied in the client's action or inaction. Consent may also be given by an authorized personal representative. Express consent remains the preferred form of consent.

The client may give his express consent:

- orally; i.e. when providing information by telephone;
- in writing, i.e. when completing and signing a service request;
- electronically, i.e. when applying for a service on his computer.

The client may give his implied consent:

- by using a Member product or service;
- by not replying to a Member's offer to remove his personal information from a direct marketing listing. If so, the Member is entitled to presume that the client allows it to use such personal information.

The client may also give his consent through an authorized representative such as a legal guardian or a person having a general power of attorney. This type of consent may prove necessary when the Member is unable to obtain the consent of a client who is underage, seriously ill or mentally incapacitated.

In order to decide which type of consent is appropriate, the Member must take into account the type of personal information required, the purposes for which it is required and the nature of its relationship with the client.

3.4 The Member may collect, use or disclose personal information without the knowledge and consent of the client when, for legal or security reason or in certain situations, for processing reasons, it is unable to obtain such consent.

For example:

- The Member is not required to seek the client's consent when it collects, uses or discloses personal information for:
  - fraud detection and suppression;
  - debt collection;
  - law enforcement.
- The client's consent is not required when transferring personal information to the Member's representatives who need it for the performance of duties such as data processing, cheque printing or credit card processing.
- When obtaining a customer listing from another organization, the Member shall assume that the other organization has obtained its clients' consent before disclosing the information.

3.5 Subject to legal or contractual restrictions, the Client may refuse to give his consent to a Member or withdraw his consent at any time, provided that:

- he gives the Member reasonable notice;
- the consent does not apply to credit products for which the Member has to collect and disclose information after credit has been granted. This action is aimed at preserving the integrity of the credit system.

The client who intends to refuse or withdraw his consent must be advised by the Member about the implications of his action. For example, a client who refuses or withdraws his consent may be denied access to certain products, services or to important information.

However, the Member cannot, without just cause, refuse to provide products, services or information to a client who has refused or withdrawn his consent.

For example, if a client does not authorize a Member to obtain a credit report, the Member may not be able to grant him a loan because it has to exercise care regarding credit and comply with the standards of the Canada Deposit Insurance Corporation and other applicable regulations.

3.6 The Member may ask the client for his social insurance number (SIN) in order to obtain information about him from a credit rating agency. If so, it must:

- explain the reason to the client;
- inform the client that he is not obliged to give his SIN to the Member;
- ask the client's consent for using and disclosing his SIN, if it has been given. The Member cannot deny credit to a client solely because he refuses to give his SIN.

Principle 4 - Limitations regarding collection of personal information

Each Member must comply with the limitations regarding the amount and the type of information collected. Information shall be collected by fair and lawful means, and solely for the purposes specified to the client.

4.1 The Member shall collect only the amount and type of information required to fulfill the purposes documented and specified to the client.

4.2 Although personal information is mainly obtained from the clients themselves, it may also be collected from third parties such as credit bureaus, employers and other lenders.

Principle 5 - Limitations regarding use, disclosure and retention of personal information

Members shall not use or disclose personal information for purposes other than those for which it was collected, unless the client allows them to use or disclose such information for other purposes.

In certain exceptional circumstances, Members have the public duty or the right to disclose personal information without the client's consent, in order to protect their own interests or public interest.

Personal information shall only be retained as long as required for the fulfillment of its identified purposes.

5.1 Each Member may disclose personal information without the client's consent if required by law, i.e. when such information is transferred:

- to the Member's solicitor;
- to the Attorney General;

- to an investigative body, a government institution or subdivision thereof if there are reasonable grounds to believe that the information is related to a breach of an agreement or to a violation of federal, provincial or foreign laws which has already been committed or is about to be committed;
- to a government institution or division thereof having requested the information and demonstrated its legal right to obtain such information if the information is believed to be relevant to national security, to the defence of Canada or to the administration of international affairs and if the information transfer is requested for the enforcement of federal, provincial or foreign laws or for the administration of federal or provincial laws;
- to a person having the power to summon or to issue a warrant or a court order or to an organization having the power to compel people to produce information (Ex: Canada Customs and Revenue Agency or another agency) upon receipt of a proper request;
- to a person hired for recovering a debt or investigating a fraud;
- in emergency situations where the life, health or safety of a person could be affected.

5.2 Under these circumstances, each Member shall protect its client's interests by:

- ensuring that the orders and requests comply with the law which governs them;
- disclosing only the personal information required by law;
- refusing requests for personal information not submitted in due form by governmental or judicial authorities.

Each Member may let the client know that an order has been received, if permitted or required by applicable law. It can do so by telephone or by mail, at the client's usual address.

5.3 Each Member may wish to use personal information (except information taken from medical records) in order to promote his products and services to his customer base, either directly or through its subsidiaries or affiliated companies. If so, it shall seek the client's consent before using personal information for this purpose.

When a client provides personal information in order to obtain a product or service, each Member must:

- inform the client that this personal information may be used by a Member or an affiliated company to sell him other products and services;
- specify the type of Member or affiliated company which might promote its products and services in this way;
- ask the client for his consent after advising him that he is free to give it or not.

When a new type of Member or affiliated company distributes promotional information on its products and services, the subsidiary or affiliated company must:

- explain to the client how it intends to use his personal information; and
- give the client the possibility to withdraw his consent regarding the ulterior use of his personal information.

5.4 Each Member shall only take personal information from medical records for specific purposes and shall not disclose such information to its subsidiaries or affiliated companies, or conversely. For example, it may not use personal information taken from the medical records of a subsidiary's client to assess a loan application.

5.5 Each Members' standards and procedures shall specify the personal information minimum and maximum retention periods. Some retention periods may be subject to legislative requirements. Personal information that has been used by a Member to make a decision about a client shall be retained long enough to allow the client access to such information after the decision has been made.

5.6 Personal information that is no longer required to fulfil the identified purposes or to comply with legislative requirements shall be destroyed, erased or made anonymous.

Each Member has standards and procedures specifying how to dispose of personal information in order to prevent unauthorized individuals and organizations from gaining access to such information.

Principle 6 - Updating personal information

Each Member shall maintain its personal information in order for it to be as accurate, complete, up-to-date and relevant as necessary to serve its identified purposes.

A client may challenge the accuracy and completeness of his personal information and have it amended as appropriate.

6.1 Each Member shall make reasonable efforts to minimize the risk of making decisions regarding clients based on inaccurate, incomplete or outdated information.

6.2 Each Member shall only update personal information if this is necessary to fulfil the purposes for which the information was collected.

6.3 Each Member shall make reasonable efforts to ensure that personal information used on an ongoing basis, including information disclosed to third parties for processing purposes, is accurate and up-to-date, unless limits to the requirement for accuracy have been clearly set out by the Member.

6.4 Each Member must also rely on clients to ensure that personal information (such as clients' names, addresses and phone numbers) is accurate, complete and up-to-date. If notified by a client that his personal information is inaccurate, incomplete, outdated or irrelevant, each Member shall revise the information accordingly. If required, it will disclose the revised personal information to third parties in order for them to update their files.

6.5 The client may object to the refusal by a Member to update his personal information. If so, the Member should take note of this objection and, if necessary, report it to third parties who also hold personal information about the client.

Principle 7 - Safeguards

Each Member shall set security safeguards which take into account the actual risk to the information security.

7.1 The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification.

7.2 The nature of the safeguards is based on the personal information sensitivity, amount and format as well as on its distribution range and its method of storage. The most sensitive personal information should warrant the highest safeguards.

7.3 Each Member shall use the following safeguards to protect personal information:

- physical safeguards such as locking filing cabinets and restricting access to offices;
- administrative safeguards such as restricting access to data processing centres and to relevant information;
- electronic safeguards such as passwords and encryption codes.

7.4 Each Member shall regularly inform its employees of its standards and procedures for protecting clients' personal information and shall stress the importance of complying with these standards and procedures. Compliance with such standards and procedures is a condition of employment.

7.5 Each Member may disclose personal information to third parties for cheque printing, data processing or debt collecting purposes, or for the delivery of other goods and services. The third party shall be required to protect all personal information according to each Member's security measures and to the relevant provisions of the regulations.

7.6 Each Member may disclose personal information to firms such as credit rating agencies and money lenders, subject to a client's consent. It shall protect the confidentiality of personal information through procedures or agreements. It will also rely on the legislation governing the safeguarding of credit information to ensure that credit rating agencies are protecting the personal information in their possession.

7.7 As mentioned in paragraph 5.6, each Member must use care in the disposal or destruction of personal information in order to prevent unauthorized individuals from gaining access to such information.

Principle 8 - Client access to standards and procedures

Each Member shall be open about the standards and procedures it uses with respect to the management of personal information. Such standards and procedures shall be accessible to clients and easy to understand.

8.1 Each Member shall make available to its clients the standards and procedures it uses with respect to the management of personal information, by making available copies of its Code.

8.2 The Code shall be readily accessible and easily understandable. As well, each Member must provide brochures or other documents which discloses to clients:

- the title and work address of the person responsible for protecting clients' personal information and the identity of the person to whom complaints and inquiries can be forwarded;
- how to gain access to personal information held by each Member;
- the type of personal information held by each Member as well as the purpose of such information;
- what personal information is disclosed within the Group and made available to affiliated companies.

8.3 Each Member may disclose information on how it manages personal information in a variety of ways, depending on the nature of services provided to clients and on the sensitivity of the personal information in its possession. For example, it may make brochures available in its branches, mail information to its clients, set up a toll-free line or provide direct electronic access.

Principle 9 - Client access to their own personal information

Each Member must advise its clients, upon request, of the existence, use and disclosure of personal information about them.

Upon request, clients must be provided access to personal information held by a Member regarding them. However, in certain situations, this access can be denied, in which case the reasons for denying access should be provided to the client.

9.1 The client is entitled to know, upon request, which personal information each Member is holding about him. The Code states that the client is entitled to access the personal information about him and to know to which third parties this information has been disclosed.

9.2 Each Member shall set up mechanisms in order to comply with clients' requests to gain access to their personal information and shall inform clients of the existence of such mechanisms. Clients must specify the type of personal information which each Member may hold .

9.3 Each Member shall specify where the personal information was collected, as well as how, when and to whom it was disclosed. It shall take such information from its records and provide it to the client in an easily understandable format, explaining abbreviations and codes, if any. It shall provide relevant information to the client within a reasonable time and at minimal or no cost.

9.4 In certain situations, a Member may not be able to provide access to the personal information it holds about a client. Such situations should be limited to a minimum and be clearly identified in the standards and procedures. For example, some personal information may:

- be too costly to extract;
- contain references to other individuals;
- be subject to solicitor-client or litigation privilege;

- contain “proprietary information”; for example, each Member might use a rating system or make a recommendation which it wants to remain confidential;
- not be allowed to be disclosed for legal reasons; for example in certain provinces, banks are not allowed to make available to clients the information provided by credit rating agencies.

9.5 A Member is not required to record in the client’s file the situations where personal information is made available to third parties in connection with ongoing activities, such as:

- the printing of cheques and other account services;
- the production of statements for Revenue Canada (T5 and others);
- the updating of information with credit rating agencies;
- communication with third parties regarding NSF cheques.

9.6 When refusing to make personal information available to a client who has requested access to his information, each Member shall specify the reason for its refusal. The client may then decide to challenge this decision. See Principle 10.

9.7 A client may question the cost of disclosing the personal information, if such cost seems unreasonable.

Principle 10 - Limitations regarding use, disclosure and retention of personal information

A client may claim that a Member is not complying with the Code. The Member has in place standards and procedures for receiving, investigating and answering complaints and inquiries.

10.1 Each Member shall establish standard and procedures for receiving, reviewing and answering complaints and inquiries from clients regarding confidentiality. It shall inform clients of the existence of such mechanisms, which should be easy to understand and simple to use. These procedures shall identify the relevant complaint resolution mechanism and the person whom the client should contact.

10.2 Each Member shall investigate all complaints. If a complaint is found to be justified, the Member shall seek to resolve it and, if necessary, amend its standards and procedures in order to prevent the problem from recurring.

10.3 If a client is not satisfied with the way his complaint has been handled, he may appeal to the banking ombudsman, the Privacy Commissioner or the Information Access Commission (Quebec). The brochure entitled *Achieving customer satisfaction* will provide the client with the appropriate procedures to follow.