THE CREDIT UNION CODE FOR THE PROTECTION OF PERSONAL INFORMATION

Introduction

Canada is part of a global economy based on the creation, processing, and exchange of information. The technology underlying the information economy provides a number of benefits that improve the quality of our lives. This technology also gives rise to concerns about the protection of privacy rights and the individual's right to control the use and exchange of personal information.

Credit unions and their Central institutions are member-owned and controlled financial institutions and, as such, have an inherent responsibility to be open and accessible while, at the same time, demonstrating the greatest respect for protection of personal privacy.

In adopting the Credit Union Code for the Protection of Personal Information (the “Code”), what has long been accepted practice for years now becomes a documented commitment to privacy.

List of Principles

Ten interrelated principles form the basis of the Credit Union Code for the Protection of Personal Information ("the Code"). Each principle must be read in conjunction with the accompanying commentary.

1 Accountability
The credit union is responsible for personal information under its control and shall designate a Privacy Officer who is accountable for the credit union’s compliance with the principles of the Code.

2 Identifying Purposes
The purposes for which personal information is collected shall be identified by the credit union at or before the time such information is collected.

3 Consent
The knowledge and consent of individuals is required for the collection, use, or disclosure of personal information, except in specific circumstances as described within this Code.

4 Limiting Collection
The collection of personal information shall be limited to that which is necessary for the purposes identified by the credit union. Information shall be collected by fair and lawful means.

5 Limiting Use, Disclosure, and Retention
Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required or permitted by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

6 Accuracy
Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7 Safeguards
Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8 Openness
The credit union shall make readily available specific, understandable information about its policies and practices relating to the management of personal information.

9 Individual Access
Upon request, individuals shall be informed of the existence, use, and disclosure of their personal information, and shall be given access to that information. Individuals are entitled to question the accuracy and completeness of the information and have it amended as appropriate.

10 Compliance
Individuals shall be able to direct questions concerning the credit union's compliance with the above principles to the Privacy Officer. The credit union shall have policies and procedures to respond to the questions and concerns.

Definitions

The following definitions apply in this Code:

Agent
An organization contracted by the credit union to provide services such as the processing of personal information on its behalf. Where personal information is transferred to agents for processing, the credit union will employ adequate safeguards to protect the information.

Collection
The act of gathering, acquiring, or obtaining personal information from any source, including Third Parties, by any means.

Consent
Voluntary agreement with what is being done or proposed. Consent can be either express or implied and can be provided directly by the individual or by an authorized representative. Express consent is given explicitly, either orally, electronically or in writing. Express consent is unequivocal and does not require any inference on the part of the credit union. Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual.

Disclosure
Making personal information available to third parties outside the credit union, including related organizations.

Individual
The term "individual" includes members and non-members.

Credit Union Model Privacy Code

Organization
A term used in the Code that includes business corporations, partnerships, professional practices, persons, government bodies, institutions, associations, charitable organizations, clubs, unions, or any other form of organization.

Personal information
Any information that is about or can be linked to an identifiable individual, but does not include the name, title or business address, telephone number, fax number or email address of an employee of an organization.

Privacy Breach
The loss of, unauthorized access to or unauthorized disclosure of personal information.

Privacy Officer
The person within the credit union who is responsible for overseeing the collection, use, disclosure and protection of personal information, and the credit union's day-to-day compliance with the Code.

Subsidiary
A company or organization wholly-owned or controlled by the credit union.

Third Party
Any person or organization other than the credit union or its employees or agents.

Use
Refers to the treatment and handling of personal information within the credit union.

1 *Principle 1* -- Accountability

The credit union is responsible for personal information under its control and shall designate a Privacy Officer who is accountable for the credit union's compliance with the principles of the Code.

1.1 Ultimate accountability for the credit union's compliance with the principles rests with the credit union's Board of Directors, which delegates day-to-day accountability to a Privacy Officer. Other individuals within the credit union may be accountable for the collection and processing of personal information, or to act on behalf of the Privacy Officer.

1.2 The credit union shall inform its employees and other individuals, upon request, of the name or title of the Privacy Officer who is responsible for the day-to-day compliance with the principles of the Code.

1.3 The credit union is responsible for personal information under its control, including information that has been transferred to an agent for processing. The credit union shall use contractual or other means to provide a comparable level of protection while the information is being processed by an agent.

1.4 The credit union shall implement policies and procedures to give effect to the principles, including:

(a) procedures to protect personal information;

(b) procedures to receive and respond to concerns and inquiries;
(c) training for staff to understand and follow the credit union's policies and procedures; and
(d) developing information to explain the organization's policies and procedures.

2 *Principle 2:* -- Identifying Purposes

The purposes for which personal information is collected shall be identified by the credit union when or before the information is collected.

2.1 The credit union shall document the purposes for which personal information is collected in order to comply with the Openness principle (section 4.8) and the Individual Access principle (section 4.9)

2.2 The credit union shall make reasonable efforts to ensure that individuals are aware of the purposes for which personal information is collected, including any disclosures to Third Parties.

2.3 Identifying the purposes for which personal information is being collected at or before the time of collection also helps define the information needed. The credit union shall collect personal information for the following purposes:

- understanding individuals' needs;
- determining the suitability of the products or services for the individual or the eligibility of the individual for products and services;
- developing, offering and managing products, services and courses and other learning opportunities that meet the individual's needs;
- providing ongoing service;
- detecting and preventing fraud, money laundering or other criminal activity, and to help safeguard the financial interests of the credit union and its members;
- meeting legal and regulatory requirements; and
- meeting personnel requirements.

2.4 The identified purposes should be specified to the individual from whom the personal information is being collected. This can be done orally, electronically or in writing. An application form with the purposes highlighted, for example, may give notice of the purposes.

2.5 When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, or is subject to a legal exception to consent, the consent of the individual is required before information can be used for that purpose.

3 *Principle 3:* -- Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except in specific circumstances as described within this Code.

Note:
In certain circumstances personal information may be collected, used, or disclosed without the knowledge or consent of the individual. Examples of such circumstances include:

- Where clearly in the interests of the individual and consent cannot be obtained in a timely way;
- To act in respect of an emergency that threatens the life, health or security of an individual;
- To avoid compromising information availability or accuracy and if reasonable to investigate a breach of an agreement, a contravention of the laws of Canada or a province; or a threat to Canada's security;
- To comply with a subpoena, warrant or court order, or rules of court relating to the production of records, or otherwise as required by law;
- For the purposes of administering any law of Canada or a province;
- To collect an overdue account or debt owed by an individual to the credit union;
- Where the information is considered by law to be publicly available;

3.1 Subject to the note above, consent is required for the collection of personal information and the subsequent use or disclosure of this information. In certain circumstances, consent may be sought after the information has been collected but before use (for example, when existing information is to be used for a purpose not previously identified).

3.2 The principle requires "knowledge and consent." The credit union shall make a reasonable effort to ensure the individual is aware of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that individuals can reasonably understand how the information will be used or disclosed.

3.3 The credit union shall not, as a condition of the supply of a legitimate product or service, require an individual to consent to the collection, use, or disclosure of personal information beyond what is necessary to provide the product or service.

3.4 In determining the form of consent to use, the credit union shall take into account the sensitivity of the information. Although some information (for example, medical and financial records) is almost always considered to be sensitive, any information can be sensitive, depending on the context.

3.5 In obtaining consent, an individual's reasonable expectations are also relevant. For example, an individual should reasonably expect the credit union to periodically supply information on credit union developments, products and services, and to provide ongoing services without a requirement for further consent. In this case, the credit union can assume that the existence of a relationship constitutes consent for reasonably associated purposes.

On the other hand, an individual would not reasonably expect that personal information given to the credit union would be given to a Third Party company selling insurance products, unless specific consent was obtained. Consent will not be obtained through deception.

3.6 The way in which the credit union seeks consent may vary, depending on the circumstances and the type of information collected. The credit union will seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive.

Consent can be obtained in many ways. For example:

(a) in writing, such as when completing and signing an application;
(b) through inaction, such as failing to check a box indicating that they do not wish their names and addresses to be used for optional purposes;
(c) orally, such as when information is collected over the telephone or in person;
(d) at the time they use a product or service; and
(e) through an authorized representative (such as a legal guardian or a person having power of attorney).

3.7 Consent may be withdrawn at any time, subject to legal or contractual restrictions, provided that:

(a) reasonable notice of withdrawal of consent is given to the credit union;
(b) consent does not relate to a credit product requiring the collection and reporting of information after credit has been granted; and
(c) the withdrawal of consent is in writing and includes understanding by the individual that the credit union may subsequently not be able to provide the individual with a related product, service or information of value.

The credit union shall inform the individual of the implications of consent withdrawal.

4 *Principle 4:* -- Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the credit union. Information shall be collected by fair and lawful means.

4.1 The credit union shall not collect personal information indiscriminately. It shall specify both the amount and the type of information collected, limited to that which is necessary to fulfill the purposes identified, in accordance with the credit union's policies and procedures.

4.2 The credit union shall collect personal information by fair and lawful means, and not by misleading or deceiving individuals about the purpose for which information is being collected.

5 *Principle 5:* -- Limiting Use, Disclosure and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

5.1 When the credit union uses personal information for a new purpose, the purpose shall be documented.

5.2 The credit union shall protect the interests of individuals by taking reasonable steps to ensure that:

(a) Demands or requests for personal information by government agencies under a statutory authority comply with the laws under which they were issued;
(b) only the personal information that is legally required to respond to a legitimate demand or request by a government agency is disclosed and nothing more; and
(c) personal information disclosed to unrelated Third Party suppliers is strictly limited to programs endorsed by the credit union or Canadian Credit Union System.

The credit union will make reasonable efforts to notify the individual that an order has been received, if not contrary to the security of the credit union and if the law allows it. Notification may be by telephone, or by letter to the individual's usual address.

5.3 The credit union shall maintain guidelines and procedures with respect to the retention of personal information. These guidelines include minimum and maximum retention periods. 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. The credit union may be subject to legislative requirements with respect to retention of records.

5.4 Subject to any requirement to retain records, personal information that is no longer required to fulfill the identified purposes shall be destroyed, erased, or made anonymous. The credit union shall develop guidelines and implement procedures to govern the destruction of personal information.

6 *Principle 6:* -- Accuracy

Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

6.1 The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the uses of the information, taking into account the interests of the individual. The credit union relies on the individual to keep certain personal information, such as address information accurate, complete and up-to-date. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

6.2 The credit union shall not routinely update personal information, unless such a process is necessary to fulfill the purposes for which the information was collected.

6.3 Personal information that is used on an ongoing basis, including information that is disclosed to Third Parties, will generally be accurate and up-to-date unless limits to the requirement for accuracy are clearly set out.

7 *Principle 7:* -- Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. The credit union will apply the same standard of care as it applies to safeguard its own confidential information of a similar nature.

7.1 The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, use, copying, modification, disclosure or disposal. The credit union shall protect personal information regardless of the format in which it is held.

7.2 The nature of the safeguards will vary depending on the sensitivity, amount, distribution and format of the information, and the method of storage. More sensitive information will be safeguarded by a higher level of protection.

7.3 The methods of protection will include:

(a) physical measures, for example, locked filing cabinets and restricted access to offices;
(b) organizational measures, for example, controlling entry to data centers and limiting access to information to a "need-to-know" basis;
(c) technological measures, for example, the use of passwords and encryption; and
(d) investigative measures, in cases where the credit union has reasonable grounds to believe that personal information is being inappropriately collected, used or disclosed.

7.4 The credit union shall periodically remind employees, officers and directors of the importance of maintaining the confidentiality of personal information. Employees, officers and directors are individually required to act in accordance with the company's Business Ethics policy as a condition of employment, which includes a commitment to keep individuals' personal information in strict confidence.

7.5 Agents shall be required to safeguard personal information transferred to them in a manner consistent with the policies of the credit union.

7.6 Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information.

8 *Principle 8:* - Openness

The credit union shall make readily available to individuals specific, understandable information about its policies and procedures relating to the management of personal information.

8.1 The credit union shall be open about privacy policies and procedures with respect to the management of personal information and shall make them readily available in a form that is generally understandable.

8.2 The information made available shall include:

(a) the name or title, and the address of the Privacy Officer who is accountable for compliance with the credit union's policies and procedures and to whom inquiries or complaints can be directed;
(b) the means of gaining access to personal information held by the credit union;
(c) a description of the type of personal information held by the credit union, including a general account of its uses;
(d) a copy of any brochures or other information that explains the credit union's policies, procedures, standards or codes; and
(e) the types of personal information made available to related organizations, such as subsidiaries or other suppliers of services.

8.3 The credit union may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, the credit union may choose to make brochures available in its place of business, mail information to individuals, provide on-line access, or establish a toll-free telephone number.

9 *Principle 9:* - Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of their personal information, and shall be given access to that information. An individual is entitled to challenge the accuracy and completeness of the information and have it amended as appropriate.

Note:

In certain situations, the credit union may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement will be limited and specific. The reasons for denying access include the following:

- providing access would likely reveal personal information about a Third Party unless such information can be severed from the record or the Third Party consents to the disclosure, or the information is needed due to a threat to life, health or security;

- the personal information has been requested by a government institution for the purposes of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out any investigation related to the enforcement of any law, the protection of national security, the defense of Canada or the conduct of international affairs;

- the information is protected by solicitor-client privilege;

- providing access would reveal confidential commercial information, provided this information cannot be severed from the file containing other information requested by the individual;

- providing access could reasonably be expected to threaten the life or security of another individual, provided this information cannot be severed from the file containing other information requested by the individual;

- the information was collected without the knowledge or consent of the individual for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province;

- the information was generated in the course of a formal dispute resolution process.

9.1 Upon request, the credit union shall inform an individual of the existence, use, disclosure, and source of personal information about the individual held by the credit union, and shall allow the individual access to this information.

9.2 For the credit union to provide an account of the existence, use, and disclosure of personal information held by the credit union, the individual may be asked to provide sufficient information to aid in the search. The additional information provided shall only be used for this purpose.

9.3 In providing an account of Third Parties to which it has, or may have, disclosed personal information about an individual, the credit union will be as specific as possible, including a list of Third Parties.

9.4 The credit union shall respond to an individual's request within a reasonable time and at no cost, or reasonable cost, to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the credit union uses abbreviations or codes to record information, an explanation will be provided.

9.5 When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the credit union shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to Third Parties having access to the information in question.

9.6 When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the credit union. When appropriate, the existence of the unresolved challenge shall be transmitted to Third Parties having access to the information in question.

Credit Union Model Privacy Code

10 *Principle 10:* - Compliance

An individual shall be able to question compliance with the above principles to the Privacy Officer accountable for the credit union's compliance. The credit union shall have policies and procedures to respond to the individual's questions and concerns.

10.1 The name or title of the Privacy Officer shall be known to staff. Information on how to contact the Privacy Officer shall be identified to other individuals periodically.

10.2 The credit union shall maintain procedures to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures will be easily accessible and simple to use.

10.3 Individuals who make inquiries or lodge complaints shall be informed by the credit union of the existence of relevant complaint procedures. If a complaint is not satisfactorily resolved with the Privacy Officer in the credit union, it may be taken to the credit union's Board of Directors. If not resolved there, procedures shall be in place to refer it to a regulator, or to an independent mediator or arbitrator, as may be appropriate.

10.4 The credit union shall investigate all complaints. If a complaint is found to be justified, the credit union shall take appropriate measures, including revision of the personal information and, if necessary, amending the credit union's policies and practices.

11 Privacy Breach Notification and Reporting

The credit union shall comply with the data breach notification and reporting requirements of PIPEDA. The credit union has established a Breach Response Plan (attached).

11.1 The Breach Response Plan includes four stages. Depending on the magnitude of the event and how the investigation evolves, some of these steps may occur simultaneously:

1) Privacy breach containment and preliminary assessment;
2) Evaluation of risks associated with the breach;
3) Communication and notification; and
4) Prevention of future breaches.

11.2 Immediate action to the situation is required to contain the privacy breach and minimize potential damages.

11.3 An assessment of the incident will be conducted to determine if an actual privacy breach occurred and its scope.

11.4 Privacy breaches that pose real risk of significant harm to affected individuals will be reported to the Privacy Commissioner of Canada with notification made to the affected individuals.

11.5 Reports to the Privacy Commissioner will include all information as prescribed within PIPEDA.

11.6 Reports will be retained on all privacy breaches to comply with record keeping responsibilities.

11.7 Privacy breaches will be reported to the Board.

How to contact the Privacy Officer

Access requests, inquiries or complaints should be addressed in writing to:

Privacy Officer
[Name and address of the credit union]