

Credit Union Code for the Protection of Personal Information

Version 3.1: March, 2000

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.

The credit union is a member-owned and controlled financial institution and, as such, has an inherent responsibility to be open and accessible while, at the same time, demonstrating the greatest respect for protection of the member's personal privacy.

Credit unions that also serve non-members shall ensure the same standards of protection are applied to these individuals as to members.

In adopting this Credit Union Code for the Protection of Personal Information, what has been accepted practice becomes a documented commitment to the member.

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 an individual 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 the information is collected.

3. **Consent**

The knowledge and consent of the member are required for the collection, use, or disclosure of personal information, except where inappropriate.

Credit Union Code for the Protection of Personal Information

Version 3.1: March, 2000

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 by law. Personal information shall be retained only as long as necessary for the fulfilment 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 to members specific, understandable information about its policies and practices relating to the management of personal information.

9. **Individual Access**

Upon request, a member shall be informed of the existence, use, and disclosure of their personal information, and shall be given access to that information. A member is entitled to question the accuracy and completeness of the information and have it amended as appropriate.

10. **Compliance**

A member shall be able to question compliance with the above principles to the designated individual accountable for the credit union's compliance. The credit union shall have policies and procedures to respond to the member's questions

Credit Union Code for the Protection of Personal Information

Version 3.1: March, 2000

and concerns.

Definitions

The following definitions apply in this Code.

"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. Express consent is given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of the credit union seeking consent. Implied consent arises where consent may reasonably be inferred from the action or inaction of the member.

"Designated Individual"

The person within the credit union who is responsible for collecting, using, disclosing and protecting the members' personal information and the credit union's day-to-day compliance with the Code.

"Disclosure"

Making personal information available to others outside the credit union.

"Member"

The person who is a member and owner of the credit union.

"Organization"

A term used in the Code that includes organizations, partnerships, associations, businesses, charitable organizations, clubs, government bodies, institutions, professional practices and unions.

"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 or telephone number of an employee of an organization.

"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 the member.

"Use"

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

Principles

Credit Union Code for the Protection of Personal Information

Version 3.1: March, 2000

1.0 Principle 1 - Accountability

The credit union is responsible for personal information under its control and shall designate an individual 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 Board of Directors, who delegate day-to-day accountability to a designated individual. Other individuals within the credit union may be accountable for the day-to-day collection and processing of personal information, or to act on behalf of the designated individual.

1.2 The credit union shall identify internally and to its members the designated individual who is responsible for the day-to-day compliance with the principles.

1.3 The credit union is responsible for personal information in its possession. The credit union shall use contractual or other means to provide a comparable level of protection while the information is being processed by a Third Party.

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 staff to understand and follow the credit union's policies and procedures
- d. annual review of the effectiveness of the polices and procedures to ensure compliance with the Code and consideration of revision as deemed appropriate.

2.0 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 prior to the information being collected.

2.2 The credit union shall make reasonable efforts to ensure that the member is aware of the purposes for which personal information is collected, including use by Third Parties.

2.3 Identifying the purposes for which personal information is being collected at or before the time of collection also defines the information needed to fulfil these

Credit Union Code for the Protection of Personal Information

Version 3.1: March, 2000

purposes. The credit union shall collect personal information for the following purposes:

- to aid in understanding the member's needs
- to determine the suitability of the products or services for the member or the eligibility of the member for products and services
- to set up, offer and manage products and services that meet the member's needs
- to provide ongoing service
- to meet legal and regulatory requirements.

2.4 The identified purposes should be specified to the member 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, the consent of the member is required before information can be used for that purpose

3.0 Principle 3 - Consent

The knowledge and consent of the member are required for the collection, use, or disclosure of personal information, except in specific circumstances as described below.

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

- Where clearly in the interests of the individual and consent cannot be obtained in a timely way;
- To avoid compromising information availability or accuracy and if reasonable to investigate a breach of an agreement or a contravention of the laws of Canada or a province;
- Where the information is generally considered to be in the public domain;
- To act in respect of an emergency that threatens the life, health or security on an individual;
- To investigate an offence under the laws of Canada, 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.

Credit Union Code for the Protection of Personal Information

Version 3.1: March, 2000

3.1 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 the credit union wants to use information for a purpose not previously identified).

The credit union may be required to collect, use, or disclose personal information without the member's consent for certain purposes, including the collection of overdue accounts, legal or security reasons.

3.2 The principle requires "knowledge and consent". The credit union shall make a reasonable effort to ensure that the member 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 the member 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 product or service, require a member to consent to the collection, use, or disclosure of information beyond that required to fulfil explicitly specified and legitimate purposes

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 income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context.

3.5 In obtaining consent, the reasonable expectations of the member are also relevant.

For example, as an owner of the credit union, a member should reasonably expect the credit union to periodically supply information on credit union developments, products and services. A member who requests debit card service should reasonably expect that the credit union, in addition to using the member's name and address for statement mailing purposes, would also contact the member to renew the card. Similarly, consent will not be obtained when personal information is supplied to agents of the credit union to carry out processing functions, such as data processing or the printing of cheques. In this case, the credit union can assume that the member's request constitutes consent for specific purposes.

On the other hand, a member would not reasonably expect that personal information given to a credit union would be given to a company selling insurance products, unless consent was obtained.

Consent will not be obtained through deception.

Credit Union Code for the Protection of Personal Information

Version 3.1: March, 2000

3.6 The way in which a credit union seeks consent may vary, depending on the circumstances and the type of information collected. A 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.

Members can give consent:

- 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 given to other organizations
- c. orally, such as when information is collected over the telephone or in person
- d. at the time they use a product or service
- e. through an authorized representative (such as a legal guardian or a person having power of attorney).

3.7 A member may withdraw consent at any time, subject to legal or contractual restrictions, provided that:

- a. reasonable notice of withdrawal of consent is give 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 member that withdrawal of consent could mean that the credit union cannot provide the member with a related product, service or information of value.

The credit union shall inform the member of the implication of such withdrawal.

4.0 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. The credit union shall specify both the amount and the type of information collected, limited to that which is necessary to fulfil 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 members about the purpose for which information is being collected

Credit Union Code for the Protection of Personal Information

Version 3.1: March, 2000

5.0 Principle 5 - 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 member or as required by law. Personal information shall be retained only as long as necessary for the fulfilment 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 may disclose personal information without consent to protect the interests of the credit union or when required by law, for example, when requested:

- a. by subpoena or search warrant;
- b. by other court and government orders;
- c. by demands from other parties who have a legal right to personal information;
- d. by a person acting in a confidential or professional relationship with the credit union, such as an auditor or a solicitor.

5.3 The credit union shall protect the interests of its members by taking reasonable steps to ensure that:

- a. orders or demands comply with the laws under which they were issued
- b. only the personal information that is legally required is disclosed and nothing more
- c. casual requests for personal information are denied
- d. personal information disclosed to unrelated Third Party suppliers of non-financial services is strictly limited to programs endorsed by the credit union.

The credit union will make reasonable effort to notify the member 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 member's usual address.

5.4 The member's health records at the credit union may be used for credit application and related insurance purposes. The member's health records shall not be collected from, or disclosed to, any other organization.

5.5 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 a member shall be retained long enough to allow the member access to the information after the decision has been made. The credit union may be subject to legislative

Credit Union Code for the Protection of Personal Information

Version 3.1: March, 2000

requirements with respect to retention of records.

5.6 Subject to any requirement to retain records, personal information that is no longer required to fulfil 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.

6.0 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 use of the information, taking into account the interests of the member. The credit union relies on the member to keep certain personal information accurate, complete and current, such as name and address. 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 member.

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

6.3 Personal information that is used on an on-going 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.

7.0 Principle 7 - Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. The credit union will take the same standard of care as it takes 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, disclosure, copying, use, or modification. 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:

Credit Union Code for the Protection of Personal Information

Version 3.1: March, 2000

- a. physical measures, for example, locked filing cabinets and restricted access to offices
- b. organizational measures, for example, controlling entry to data centres and limiting access to information to a "need-to-know" basis
- c. technological measures, for example, the use of passwords and encryption.
- 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, directors and officers of the importance of maintaining the confidentiality of personal information. Employees and directors are individually required to sign an oath of ethical conduct annually, including commitment to keep member's personal information in strict confidence.

7.5 Third Parties shall be required to safeguard personal information disclosed to them in a manner consistent with the policies of the credit union. Examples include cheque printing, data processing, credit collection, credit bureaus and card production.

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

8.0 Principle 8 - Openness

The credit union shall make readily available to members specific, understandable information about its policies and practices 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 designated individual who is accountable for compliance with the credit union's policies and procedures and to whom complaints or inquiries can be forwarded
- 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 use
- d. a copy of any brochures or other information that explains the credit union's policies, procedures, standards or codes
- e. the types of personal information made available to related organizations, such

Credit Union Code for the Protection of Personal Information

Version 3.1: March, 2000

as subsidiaries or other suppliers.

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 its members, provide on-line access, or establish a toll-free telephone number.

9.0 Principle 9 - Individual Access

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

Note: In certain situations, a credit union may not be able to provide access to all the personal information it holds about a member. 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 administration of any law, the protection of national security, the defence 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

Credit Union Code for the Protection of Personal Information

Version 3.1: March, 2000

process.

9.1 Upon request, the credit union shall inform a member of the existence, use, disclosure, and source of personal information about the member held by the credit union, and shall allow the member access to this information. However, the credit union may choose to make sensitive medical information available through a medical practitioner.

9.2 In some cases, the credit union may not be able to provide all of the personal information that it holds. The credit union will limit these cases and make them specific in its policies and procedures. For example, some personal information may not be provided, or not provided in full, because it may contain the credit union's own "proprietary information", such as personal information used in making an evaluation regarding eligibility for services.

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

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

9.5 The credit union shall respond to a member's request within a reasonable time and at no cost, or reasonable cost, to the member. 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.

9.6 When a member 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.

9.7 When a challenge is not resolved to the satisfaction of the member, 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 Code for the Protection of Personal Information

Version 3.1: March, 2000

10.0 Principle 10 - Compliance

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

10.1 The designated individual accountable for the credit union's compliance shall be known to staff and identified to the member 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 Members 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 designated individual in the credit union, it may be taken to the credit union Board of Directors. If not resolved there, procedures shall be in place to refer it to the Credit Union Central, 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.