Consumers and Debit Cards

Canadian Code of Practice for Consumer Debit Card Services

Prepared by the Electronic Funds Transfer Working Group

May 1992
Revised 1996
Revised 2002

2004 REVISION*

* **Note: The highlighted sections of the 2004 revised Code come into force on September 30, 2005.**

Table of Contents

1. About This Code

1. This voluntary code of practice has been developed through consultation with the Electronic Funds Transfer Working Group – which is made up of representatives from consumer organizations, financial institutions, retailers, and federal and provincial governments.

2. The code was developed in 1992 and was revised in 1996. In January 2002, a guide to the interpretation of Section 5, Liability for Loss, was agreed to by the Electronic Funds Transfer Working Group and has been added as Appendix A to this document. The guide provides additional interpretation for financial institution staff and consumers on the question of liability for losses, which is covered in Section 5 of the code. The code was further revised in 2004 to clarify the procedures for addressing unauthorized transactions and other transaction problems.

3. Organizations endorsing the code will maintain or exceed the level of consumer protection it establishes. The code does not preclude the protection given by existing laws and standards.

4. The code outlines industry practices and consumer and industry responsibilities, which will help to protect consumers in their use of debit card services in Canada. It applies only to services that use debit cards and personal identification numbers (PIN) to access point-of-service terminals, such as automated banking machines (ABM), point-of-sale (POS) terminals and debit card terminals in the home. The code does not cover transactions that take place outside Canada, or that transfer funds into or out of Canada; other arrangements apply to these transactions. Card issuers will also do their best to protect consumers in such transactions and to resolve any problems that may occur.

5. The code will be reviewed regularly to ensure its relevance to current technology and business practices, and its effectiveness in promoting consumer protection in electronic funds transfers.

6. Debit cards provide consumers with a convenient alternative method of making payments. The use of debit cards is not intended to limit consumers' choice among payment methods at the point of sale, such as cash, cheque or credit card.

7. Definitions for a number of terms used in the code are found in Section 9.

2. Issuing Debit Cards and Personal Identification Numbers (PIN)

1. A debit card and its associated PIN may be issued by two separate organizations. For example, it may be that a retailer or other organization issues the card and the financial institution issues the PIN. For this reason, the responsibilities of the PIN issuer and card issuer are described separately below.

When debit cards and/or PINs are issued,

2. It is the responsibility of the PIN issuer to:

a) commence the debit card service only on receipt of a signed request from an applicant;

b) enable the applicant to choose which eligible accounts the card will access. Access to the accounts will include access to all the accounts' features selected by the applicant, such as overdraft protection;

c) inform the applicant of:

- any fees associated with holding and using the PIN;
- the purpose and functions of the PIN;
- the cardholder's responsibility for PIN security, and the possible consequences of a breach of that responsibility; and
- how to contact the PIN issuer in the event of a problem.

d) ensure that the PIN is disclosed only to the cardholder, or selected only by the cardholder; and

e) advise the cardholder:

- of how to avoid unauthorized use of the card and PIN, including typical PIN combinations to avoid for security reasons when cardholders select their own PIN; and
- of the potential extent of losses that could occur due to unauthorized use of the card and PIN.

3. It is the responsibility of the card issuer to

a) inform the applicant of:

- any fees associated with holding and using the debit card;
- the purpose and functions of the card;
- the cardholder's responsibility for card security, and the possible consequences of a breach of that responsibility; and
- how to contact the card issuer in the event of a problem;

b) ensure that the card is delivered to the intended cardholder;

c) provide the cardholder with a copy of the cardholder agreement; and

d) advise the cardholder:

- of how to avoid unauthorized use of the card; and
- of the potential extent of losses that could occur due to unauthorized use of the card.

3. Debit Cardholder Agreements

1. Cardholder agreements will be written in plain language.

2. A copy of the cardholder agreement(s) will be provided to the cardholder or applicant for a debit card

a) when a card is issued or a PIN is initially issued or selected; or
b) when requested.

3. The following general headings or equivalent wording will be used in cardholder agreements: Definitions; Dispute Resolution; Liability; Lost or Stolen Card; PIN Confidentiality; Service Charges; and Termination of This Agreement.

4. Cardholders will be informed

a) as soon as the terms and conditions of a cardholder agreement change; and
b) of where to obtain a copy of the changes or the revised agreement.

4. Debit Card Transactions

1. Transaction records, together with periodic statements or passbook entries, will contain enough information to enable cardholders to check account entries. The information may be in the form of abbreviations or codes, as long as the meanings of the codes are clearly set out in the document in which the codes are used.

a) Transaction Record

When a debit card transaction takes place, the cardholder will be offered a paper or electronic transaction record containing the following information:

- transaction amount;
- transaction date;
- transaction time, if possible. If the transaction time does not appear on the transaction record, information on the transaction time will be available from the card issuer;
- transaction type (e.g. deposit, withdrawal, purchase or refund);
- type of account being credited or debited;
- card number (full or abbreviated);
- transaction number; and
- identity of the card acceptor: the trade name and local address of the merchant involved in the transaction, as generally known to the public; and,
- the identity of the terminal, including, specifically, the name under which the machine operates. When the location of the machine is identified on the transaction record by a number only, the card issuer will provide the street address on request.

If a transaction record cannot be provided, for example, when the machine runs out of transaction slips, the cardholder will be offered the choice of whether or not to proceed with the debit card transaction.

b) Periodic Statements

For an account other than a passbook account, the cardholder will be provided with periodic statements containing the following information about all debit card transactions occurring since the previous statement:

- transaction amount;
- transaction date;
- transaction type (e.g. deposit, withdrawal, purchase or refund);
- transaction number where possible; and
- where possible, the identity of the card acceptor: the trade name and local address of the merchant involved in the transaction, as generally known to the public; and
- the identity of the terminal, including, specifically, the name under which the machine operates.

c) Passbook Accounts

For a passbook account, the following debit card transaction information will be printed in the passbook when it is presented for update:

- transaction amount;
- transaction date; and
- transaction type (e.g. deposit, withdrawal, purchase or refund).

2. Transaction Security

a) Point-of-service terminals will give access to information on a cardholder's account(s) only when used with that cardholder's card and PIN.

b) When point-of-service terminals in a public place are installed or replaced, the terminals and their immediate surroundings will allow sufficient privacy to enable a cardholder to enter a PIN with minimum risk of the PIN being revealed to others.

5. Liability for Loss

The interpretation guide for this section is in Appendix A.

1. Cardholders are responsible for all authorized use of valid cards.

2. Cardholders are responsible if they make entry errors at point-of-service terminals, or if they make fraudulent or worthless deposits.

3. Cardholders are not liable for losses resulting from circumstances beyond their control. Such circumstances include, but are not limited to:

a) technical problems, card issuer errors, and other system malfunctions;

b) unauthorized use of a card and PIN where the issuer is responsible for preventing such use, for example after:

- the card has been reported lost or stolen;
- the card is cancelled or expired; or
- the cardholder has reported that the PIN may be known to someone other than the cardholder; and

c) unauthorized use, where the cardholder has unintentionally contributed to such use, provided the cardholder co-operates in any subsequent investigation.

4. In all other cases, when a cardholder contributes to unauthorized use, the cardholder will be liable for the resulting loss. This loss will not exceed the established debit card transaction withdrawal limits. However, in some circumstances, the loss may exceed the actual funds in an account. This may occur, for example,

- if an account has a line of credit or overdraft protection or is linked with another account or other accounts; or
- if a debit card transaction is made on the basis of a fraudulent deposit at an ABM.

5. A cardholder contributes to unauthorized use by

a) voluntarily disclosing the PIN, including writing the PIN on the card, or keeping a poorly disguised written record of the PIN in proximity with the card;

b) failing to notify the issuer, within a reasonable time, that the card has been lost, stolen or misused, or that the PIN may have become known to someone other than the cardholder.

6. Procedures for Addressing Unauthorized Transactions and other Transaction problems

1. In the event of a problem with a debit card transaction, a cardholder should first attempt to resolve the problem with the PIN issuer.
(Note: Section 6.1 was section 6.2 in the previous version of the Code — Revised 2002 version.)

2. In the event of a problem with a debit card terminal in the home, a cardholder may also contact the card acceptor, who will trace the source of the problem and advise the cardholder of the appropriate party to contact to resolve the problem.
(Note: Section 6.2 was section 6.3 in the previous version of the Code — Revised 2002 version.)

3. In the event of a problem with merchandise or retail service that is paid for through a debit card transaction, a cardholder should resolve the problem with the retailer concerned.
(Note: Section 6.3 was section 6.4 in the previous version of the Code — Revised 2002 version.)

4. PIN issuers will have clear, timely procedures for dealing with debit card transaction problems, which will include:
(Note: This part of Section 6.4 was section 6.1 in the previous version of the Code — Revised 2002 version.)

- procedures to investigate the reported transaction problem; and
- provisions for review of problems at a senior level within their organizations.
  (Note: New Section, which becomes effective on September 30, 2005.)

5. When a cardholder contacts the PIN issuer regarding an unauthorized transaction, the PIN issuer will inform the cardholder of the following:

- that the PIN issuer will investigate the transaction(s) in question;
- that a determination regarding any reimbursement will stem from the investigation;
- that the PIN issuer will respond to the cardholder's report of an unauthorized transaction as soon as possible, but in no later than 10 business days; and
- that, during the course of the investigation, the PIN issuer may require a signed written statement, or where appropriate, a signed written affidavit from the cardholder, which may result in a temporary suspension of the 10 day time limit, until the requested information is received.
  (Note: New Section, which becomes effective on September 30, 2005.)

6. In the event that the results of an investigation determines that not all the funds will be reimbursed to the cardholder, the PIN issuer is responsible for showing that, on the balance of probabilities, the cardholder contributed to the unauthorized use of the card, subject to section 5 of this Code.
(Note: New Section, which becomes effective on September 30, 2005.)

7. In the event that the PIN issuer requests that a cardholder provide a signed, written statement or where appropriate, a signed written affidavit with regard to the reported unauthorized transaction during the course of an investigation, the investigation time limits (10 days) may be temporarily suspended until such a statement or affidavit is received.
(Note: New Section, which becomes effective on September 30, 2005.)

7. Resolving Disputes

1. The PIN issuer will provide information, in writing on how the dispute-resolution process works if :

a) a problem with a debit card transaction cannot be settled when the cardholder first complains; or,
b) subject to section 6(5), the cardholder contacts the PIN issuer claiming that she or he has not received a response to a claim of an unauthorized transaction.

(Note: Section 7.1 is new and becomes effective on September 30, 2005.)

2. A cardholder whose problem cannot be settled by the PIN issuer will be informed of the reasons for the issuer's position on the matter. The issuer will then advise the cardholder of the appropriate party to contact regarding the dispute.
(Note: Section 7.2 was section 6.6 in the previous version of the Code — Revised 2002 version.)

3. During the dispute-resolution process, cardholders will not be unreasonably restricted from the use of funds that are the subject of the dispute.
(Note: Section 7.3 was section 6.7 in the previous version of the Code — Revised 2002 version.)

8. Organizations That Endorse the Code

1. The following organizations endorse the Code:

- Canadian Bankers Association
- Canadian Federation of Independent Business
- Credit Union Central of Canada
- Consumers' Association of Canada
- La Fédération des caisses Desjardins du Québec
- Retail Council of Canada

2. In addition, the following organizations support the Code:

- Canadian Payments Association

(Note: This section has been amended in the 2004 revision.)

9. Terms Used in This Code

1. Automated Banking Machine (ABM. Also known as Automated Teller Machine — ATM): an electronic terminal used by consumers to access financial services provided by the financial institution(s) that hold(s) their account(s).

2. Card Acceptor: the financial institution, retailer or other service provider that owns or operates a point-of-service terminal that accepts the use of a debit card.

3. Cardholder: the person to whom a valid debit card is issued.

4. Card Issuer: the organization that issues a valid debit card.

5. Debit Card: a card with electronically readable data that is used, in conjunction with a PIN, to confirm the identity of the cardholder and authorize debit card transactions.

6. Debit Card Service: a service that enables a cardholder to undertake financial transactions at point-of-service terminals.

7. Debit Card Terminal in the Home: an in-home electronic terminal used by cardholders to make debit card transactions.

8. Debit Card Transactions: deposits, withdrawals, payments, or other funds transfers made at point-of-service terminals using a debit card.

9. Electronic Funds Transfer: transfers of funds using electronically transmitted instructions. Examples include

- payment for goods or services at a point-of-sale terminal;
- deposits, withdrawals and transfers of funds between a cardholder's accounts, made at an ABM; and
- payments and transfers of funds made at a debit card terminal in the home.

10. Personal Identification Number (PIN): a secret code intended for the sole use of a cardholder. The PIN is used in conjunction with a debit card to confirm the identity of the cardholder and to authorize debit card transactions.

11. PIN Issuer: a financial institution that issues PINs for use with debit cards.

12. Point-of-sale Terminal: an electronic terminal used by cardholders to pay for goods or services at a retail or service outlet.

13. Point-of-service Terminal: an electronic terminal, incorporating a card reader and PIN pad, used to make debit card transactions. Automated banking machines, point-of-sale terminals and terminals in the home are examples of point-of-service terminals.

The plain language definitions given above are based in part on the technical definitions used by the Canadian Payments Association (CPA) in its Rule E1, “Clearing and Settlement of Shared Electronic Point-of-Service Payment Items.” The CPA is an organization that governs how payments, including both paper payments (such as cheques) and electronic payments (such as ABM and EFT/POS), are cleared and settled between financial institutions. Copies of Rule E1 may be obtained from their website at www.cdnpay.ca or by writing to:

Canadian Payments Association
50 O’Connor Street, Suite 1212
Ottawa, Ontario
K1P 6L2

APPENDIX A
Guide to the Interpretation of Section 5: Liability for Loss

Note: For the purposes of this interpretation, a loss is defined as an amount withdrawn from an account without the authority of the cardholder, including related service and interest charges.

Clause 1. Cardholders are responsible for all authorized use of valid cards.

Interpretation

1. An authorized transaction is one in which the card and PIN are used to carry out the transaction and in which the cardholder has not been the victim of trickery, force, intimidation or theft.

Clause 2. Cardholders are responsible if they make entry errors at point-of service terminals, or if they make fraudulent or worthless deposits.

Interpretation

1. In situations in which a cardholder is responsible, the entry error will be corrected by the card issuer, but the cardholder may still be liable for consequential costs such as service, NSF and/or interest charges.

2. At ABMs, cardholders are responsible if they accidentally enter the same transaction twice, enter an amount greater or less than the actual deposit, or forget to include the deposit. For example, if a cardholder deposits $1000.00 but incorrectly enters an amount of $100.00, which subsequently results in the card issuer returning a cardholder's cheque NSF prior to the card issuer verifying funds, the cardholder may be liable for NSF charges.

3. If a cardholder makes an error because the ABM instruction/message has not been written in clear and understandable language, then the cardholder is not responsible and thus would not be debited for related service or interest charges.

4. At point-of-sale terminals, the card acceptor and the cardholder have a shared responsibility to ensure that the transaction is processed for the correct amount. In the event that there is an error, it is the responsibility of the merchant to assist the cardholder in correction of the error.

Clause 3. Cardholders are not liable for losses resulting from circumstances beyond their control. Such circumstances include, but are not limited to

a) technical problems, card issuer errors and other system malfunctions;

b) unauthorized use of a card and PIN where the issuer is responsible for preventing such use, for example after

- **the card has been reported lost or stolen;**
- **the card is cancelled or expired; or**
- **the cardholder has reported that the PIN may be known to someone other than the cardholder; and**

c) unauthorized use, where the cardholder has unintentionally contributed to such use, provided the cardholder co-operates in any subsequent investigation.

Interpretation

1. The cardholder is not liable for losses relating to transactions:

a) resulting from a technical failure of the system or equipment when a transaction has been accepted at a terminal in accordance with the cardholder's instructions;

b) that are caused by the fraudulent or negligent conduct of any of the following: employees or agents of the card issuer; companies involved in networking arrangements; merchants who are linked to the electronic fund transfer system, or their agents or employees;

c) that are caused by the card acceptor or card issuer incorrectly debiting the account more than once for the same transaction;

d) relating to cards that are forged, faulty, expired or cancelled;

e) occurring before it has been ascertained that the cardholder has received the card and PIN. Neither the card issuer nor the PIN issuer, whether or not they are the same body, can rely solely on records of delivery to the cardholder's address by mail or courier as proof that the PIN was received by the cardholder;

f) occurring after the cardholder has notified the card issuer that the card has been misused; lost or stolen; or that PIN security has been breached;

g) where the cardholder has been the victim of fraud, theft, or has been coerced by trickery, force or intimidation, provided that the cardholder reports the incident promptly and co-operates fully in any subsequent investigation; or

h) resulting from the PIN issuer failing to fulfill their obligations under Section 2, Clause 2(e) of the code.

Clause 4. In all other cases, when a cardholder contributes to unauthorized use, the cardholder will be liable for the resulting loss. This loss will not exceed the established debit card transaction withdrawal limits.
However, in some circumstances, the loss may exceed the actual funds in an account. This may occur, for example,

- **if an account has a line of credit or overdraft protection or is linked with another account or other accounts;**
- **if a debit card transaction is made on the basis of a fraudulent deposit at an ABM.**

Interpretation

1. Most card issuers set daily limits for cash withdrawals at ABMs and separate daily limits for purchases at point-of-sale terminals. For example, the following daily transaction limits could apply:

Cash at ABMs up to $1000.00
Purchases at point-of-sale terminals up to $2000.00
Total limit up to $3000.00

Note: limits vary depending on the institution and the cardholder's agreement.

In the above example, even if there is only $2000.00 in the account, daily withdrawals totaling $3000.00 could still be made, if:

a) the account has overdraft protection
b) the account is linked to a line of credit or other accounts; or
c) a fraudulent cheque or empty envelope is deposited.

Clause 5. A cardholder contributes to unauthorized use by:

a) voluntarily disclosing the PIN, including writing the PIN on the card, or keeping a poorly disguised written record of the PIN in proximity with the card;
b) failing to notify the issuer, within a reasonable time, that the card has been lost, stolen or misused, or that the PIN may have become known to someone other than the cardholder.

Interpretation

1. Cardholders are not considered to have disclosed the PIN "voluntarily" if the PIN is obtained by coercion, trickery, force or intimidation.
This includes situations where the customer's PIN is observed at point-of-sale terminals.

2. The fact that a cardholder uses the same PIN for more than one card does not constitute contribution to unauthorized use.

3. For the cardholder to be liable, a voluntary disclosure of the PIN must contribute to the loss.

4. Cardholders are considered to have disclosed the PIN voluntarily if they use a PIN combination selected from the cardholder's name, telephone number, date of birth, address, or social insurance number.

5. A PIN is poorly disguised when:

a) it is written on the card; or
b) a record of the PIN is kept without making a reasonable attempt to hide or disguise the code, and could be lost or stolen simultaneously with the card. For example, if it is kept in the same receptacle which itself can be lost or stolen (e.g. a wallet, purse, briefcase or suitcase), or it is kept in the same location so that the card and PIN record can be easily associated

6. The reasonableness of an attempt to disguise a PIN should be assessed from the point of view of the reasonable cardholder, not from the point of view of the thief or the card issuer's official who through experience have become familiar with many types of disguises and their strengths and weaknesses.

7. A PIN is reasonably disguised if it is concealed within a record, for example, by re-arranging the numerals, substituting other numerals or symbols, or if it is made to appear as another type of number by surrounding it with other numerals or symbols.

8. Notification of the issuer within a **reasonable time***:*

a) The card issuer should be notified of lost, stolen, or misused cards and/or disclosure of the PIN as soon as the cardholder becomes aware of the loss or disclosure.