Highlights from:

Evaluation of Operations Related to the Canadian Code of Practice for Consumer Debit Card Services

Submitted to:

The Electronic Funds Transfer Working Group

By

EKOS Research Associates Inc.

October 31, 2002

Highlights prepared by:

Office of Consumer Affairs, Industry Canada

255 Albert Street, 10th Floor East, Ottawa, ON K1A 0H2
Mailing Address: 235 Queen Street, Ottawa, ON K1A 0H5

TABLE OF CONTENTS

1 INTRODUCTION

The Canadian Code of Practice for Consumer Debit Card Services is a voluntary code of practice for Canadian industry and consumers involved in issuing and using debit cards and personal identification numbers (PINs). The Code was developed in consultation with a variety of key stakeholders, including consumer organizations, financial institutions, retailers, and federal and provincial governments, in order to ensure that the range of issues and concerns pertaining to both industry practice and consumer and industry responsibilities were readily addressed. The Code applies to limited types of services that use debit cards and PINs to have access to point-of-service terminals including automated banking machines (ABM), and point-of-sale (POS) terminals. While the Code is designed to help protect industries and consumers, it does so in addition to other forms of protection provided by existing laws and standards.

1.1 Evaluation Objectives and Issues

The purpose of the evaluation was to provide feedback and analysis on the nature and extent of operational adherence to the Canadian Code of Practice for Consumer Debit Card Services. The specific objectives of the evaluation were to explore operational adherence to, and cardholder and card issuer awareness of, various components using multiple lines of evidence. The specific components of the Code that were evaluated are PIN security and liability for loss; transactions; and dispute resolution.

1.2 Evaluation Methodology

The approach to the evaluation of the Code involved six methodological components: a review of card issuer documentation, spot checks of card issuers, spot checks of point-of-service terminals, a telephone survey of cardholders, a review of complaint data, and key informant telephone interviews with merchants. Each of these data-collection activities is described in turn below.

a) *Review of Card Issuer Documentation*

The objective of this component of the evaluation was to review documentation from 10 financial institutions. The list of financial institutions selected to participate in the review was developed in consultation with the client and included most major financial institutions currently operating in Canada, including: CIBC; TD/Canada Trust; Royal Bank; Bank of Montreal; Scotiabank; Laurentian Bank; National Bank; President's Choice; Caisses Populaire Desjardins (with documentation from two member caisses); and Credit Union Central of Canada (with documentation from two member credit unions).

b) *Spot Checks of Card Issuers*

The major objective of this line of evidence was to gather and then compare the nature of the information provided in the products and practices issued by selected branches of the same 10 financial institutions identified for the documentation review. In an effort to get a representative sample reflecting each of the financial institutions from varying regions across the country, the spot checks were conducted in five cities (i.e., Victoria, Saskatoon, Ottawa, Montreal and Fredericton) representing five different regions throughout Canada (i.e., BC, the Prairies, Ontario, Quebec and the Maritimes).

Two presenting situations were employed when conducting independent spot checks: a) **unprompted —** the researcher posed as an applicant for an account with a debit card and did not prompt the customer service representative for further information beyond what was offered; and b) **prompted —** the researcher posed as an applicant for an

account with a debit card and prompted the customer service representative for further information. A total of 40 spots checks were conducted. All spot checks involved the acquisition of both verbal and written information (i.e., cardholder agreement and other literature) for comparison with components of the Code.

c) *Point-of-Service Spot Checks*

Point-of-service terminals are electronic terminals that incorporate a card reader and PIN pad and are used to make debit card transactions, including automated bank machines, and point-of-sale (POS) terminals. As part of this evaluation, a total of 80 point-of-service terminal spot checks conducted in the same cities in which the spot checks of card issuers were carried out. Although the number of spot checks conducted is not sufficient to generalize to all merchants, it nonetheless provided sufficient feedback to identify issues that may need to be considered.

Point-of-service terminals were classified into one of five categories according to the type of environment within which the transaction occurs. These categories were:

- ***lane environments***: point-of-service terminals where the cardholder typically purchases multiple items and must pass through a "lane" at one of several purchase counters grouped together in one area of the store, usually just before the exit. This point-of-service terminal is used almost exclusively to pay for purchases and other services, such as customer enquiries and assistance, are accessed elsewhere in the store.
- ***cash wrap***: typically includes specialty retailers or traditional department stores where the customer selects their merchandise and goes to one of a number of purchase counters located throughout the store where their purchase can be "wrapped". Other services, such as enquiries and personalized assistance, can also be obtained from these locations at this type of merchant.
- ***small format:*** includes merchants where the merchandise tends to be displayed in a relatively small space and in close proximity to the point-of-sale. Examples of the type of point-of-service terminal include gas stations and corner stores.
- ***Automated Banking Machines (ABMs)***; and
- ***dining and entertainment.***

d) *Survey of Cardholders*

The initial survey objective was to complete a total of 1,000 interviews with cardholders from across Canada. Following the survey pretest, however, it was discovered that the instrument was longer than anticipated. Furthermore, while it was assumed that a majority of Canadian households has at least one adult who holds a debit card (we had assumed a figure of 85 per cent), the true incidence of cardholders may have been somewhat lower. As a result of both of these factors, the total number of interviews conducted for the survey was revised to 809 in order to accommodate the survey within the existing budget.

Following a brief statement identifying the project sponsor and explaining the purpose of the survey, respondents were asked an initial screening question to determine if there was a cardholder within their household. If so, the interview proceeded, provided that the cardholder agreed to participate in the survey. EKOS designed the survey questionnaire in consultation with the client to address the evaluation issues. More specifically, the instrument was designed to gather information on:

- cardholder awareness of the importance of ensuring the security of their card and PIN;
- cardholder awareness of the criteria for the selection of a PIN;
- cardholder awareness of their responsibilities and liabilities with respect to the loss of their debit card;
- cardholder perceptions of the degree of privacy at both point-of-service terminals and point-of-sale terminals when cardholders enter their PIN;
- cardholder background characteristics (e.g., frequency and patterns of debit card use, age, gender, income, province); and
- cardholder experiences with debit card problems and the complaint process.

e) *Review of Complaint Data*

The main objective of the review of complaint data was to find out about the nature of complaints registered by cardholders. The nature and range of complaints explored pertained to the following issues:

- ***Transaction errors or problems***, such as ABMs dispensing an incorrect amount, bill payments not received/received late, ABM deposit errors/discrepancy, cardholders/retailers processing transactions for the wrong amount, transaction amounts posted differing from the amount on the transaction record, transactions posted to the wrong account, and duplicate transactions; and
- ***Unauthorized or fraudulent transactions*****,** such as cardholders not remembering doing the transaction, empty ABM deposit envelopes, worthless items on ABM deposits, unauthorized ABM withdrawals, and unauthorized debit transactions

A covering letter and data collection template were distributed to each of the major financial institutions identified for the documentation review asking them to provide aggregate data concerning the number and nature of complaints received by their call centres over a one-year period (i.e., November 1, 1999 and October 31, 2000), as well as any actions they may have taken in response to the complaint. A separate covering letter and data collection template were used to gather data concerning complaints received by the Canadian Banking Ombudsmen, consumer organizations and the Office of the Superintendent of Financial Institutions (OSFI) over the same period of time. The data collection template for these institutions asked additional questions about the nature of the complaints and was completed individually for each file received from these latter sources.

Very few financial institutions were able to provide the call centre complaint data as requested and the quality and thoroughness of the information varied a great deal for those institutions that were able to submit this information. A total of four institutions (of 10 invited to participate) were able to submit complaint data and only two of these institutions were able to provide aggregate complaint data at the level of detail requested (although the data from all four institutions is presented in Chapter 4). Similarly, only two of the five "other" institutions (i.e., OSFI, Canadian Banking Ombudsmen, consumer organizations) invited to take part were able to submit data regarding the complaints their organization had received during the time period under review. The primary discrepancies in the nature of information received from financial institutions through this exercise are as follows:

- One institution was only able to provide overall totals for complaints received during the time period under review (not broken down by type of complaint);
- One institution submitted hard copies of complaints received by the institution's ombudsman, since call centre data was not available; and
- The data collection template requested aggregate information on complaints received by the call centre between November 1999 and September 2001, however, the timeframes for the receipt of complaint data tended to vary from institution to institution.

To accommodate these various discrepancies in the data, raw totals of complaints received were summarised in a single table to provide an overall picture of the nature of debit card complaints. Complaints received from one financial institution's banking ombudsman were reviewed individually and categorised to be included with the aggregate complaint data (in Section 4.3, Table 4.5), while overall numbers of complaints received from another institution were included in the table as "non-classified" complaints.

f) *Key Informant Interviews with Merchants*

Twenty-one key informant interviews with merchants were conducted. The list of potential merchants to be interviewed was developed using a combination of the Canada Survey Sampler, as well as the Canada 411 search engine, and was stratified according to region, the size of the operation (i.e., chain or independent) and the type of merchant (i.e., lane environment, cash wrap, small format or other). Two types of potential respondent were interviewed for this component of the evaluation. Four interviews were conducted with "experts" who had primary responsibility for the design and placement of point-of-service terminals within retail outlets and 17 interviews were conducted with an owner or manager. The interviews were conducted over the telephone by EKOS researchers in Ottawa.

2 ISSUING DEBIT CARDS AND PINS

2.1 Documented Adherence to the Code

Financial institutions invited to participate in the evaluation were asked to submit copies of all relevant documentation that contain any reference to the institution's policies and practices with respect to PIN security, liability for loss and dispute resolution and complaint processes. Among the 10 participating institutions, the vast majority included the customer copies of their cardholder agreements[1] (90 per cent), followed by other documents such as VHS tapes and customer pamphlets (80 per cent), employee training manuals (70 per cent), cardholder literature (70 per cent) and operational policies (30 per cent).

Table 2.1 presents overall ratings of the degree to which the documentation adheres to the Code in terms of practices pertaining to the issuance of debit cards, as well as separate ratings for the documentation provided to cardholders and internal documentation.

Overall, we observe that financial institutions generally adhere to the Code in most regards with respect to the issuance of debit cards. The highest rates of adherence are observed in terms of the degree to which the documentation advises cardholders of how to avoid unauthorized use of the card (100 per cent), followed by the extent to which the documentation ensures that the PIN is disclosed only to the cardholder or selected only by the cardholder (100 per cent), informs the applicant of the cardholder's responsibility for card security (100 per cent), and informs the applicant of how to contact the card issuer (95 per cent). Slightly lower overall levels of adherence are observed for the degree to which the documentation informs the applicant of the purpose and functions of the card (89 per cent), the possible consequences of a breach of responsibility for card security (68 per cent), and the

[1] The cardholder agreement for the remaining institution was reproduced in other supporting documents.

potential extent of losses that could occur due to unauthorized use of the card (63 per cent). The lowest level of compliance was found for the degree to which documentation outlines the cardholder's ability to choose which eligible accounts the card will access (37 per cent). It should be noted, however, that this information tends to be imparted during the process of opening accounts, as presented in Section 2.2 (Table 2.2).

TABLE 2.1 of EKOS Evaluation
Distribution of Rated Adherence of Documentation to the Code - Issuing Debit Cards

Documentation Provided to Cardholders (n=10)						Internal Documentation (n=9)						Overall % in compliance**
1*	2	3	4	9	% in compliance**	1	2	3	4	9	% in compliance**	
"It is the responsibility of the card issuer to … "												
Advise the cardholder of how to avoid unauthorized use of the card												
0	0	9	1	0	**100%**	0	0	7	2	0	**100%**	**100%**
Ensure that the PIN is disclosed only to the cardholder, or selected only by the cardholder												
0	0	10	0	0	**100%**	0	0	9	0	0	**100%**	**100%**
Inform the applicant of the cardholder's responsibility for card security												
0	0	10	0	0	**100%**	0	0	7	2	0	**100%**	**100%**
Inform the applicant of how to contact the card issuer in the event of a problem												
0	0	10	0	0	**100%**	1	0	8	0	0	**89%**	**95%**
Inform the applicant of the purpose and functions of the card												
1	0	8	1	0	**90%**	1	0	8	0	0	**89%**	**89%**
Inform the applicant of the possible consequences of a breach of responsibility for card security												
0	3	7	0	0	**70%**	1	2	6	0	0	**67%**	**68%**
Advise the cardholder of the potential extent of losses that could occur due to unauthorized use of the card												
0	4	6	0	0	**60%**	1	2	4	2	0	**67%**	**63%**
Enable the applicant to choose which eligible accounts the card will access***												
4	4	2	0	0	**20%**	0	4	4	1	0	**56%**	**37%**

* 1=no reference to clause, 2=contradicts code or insufficient information provided, 3=meets code, 4=exceeds code, 9= refers to documents or information alluded to but not provided
** Presents the proportion of cases that received a rating of 3 or 4
*** Although not always documented, this information was communicated in the vast majority of card issuer spot checks (Table 2.2, below).

2.2 Observed Adherence to the Code

In this section, we present evidence from the spot checks of card issuers pertaining to the degree to which the card issuers adhered to recommended procedures outlined in the Code for the issuance of debit cards and PINs. Recall that each spot check received three different ratings based on the degree to which the relevant information was imparted verbally, through the cardholder agreement or through other supporting literature.

As described in Section 1.2b (above), two scenarios were used to open accounts with debit card access: a prompted scenario where the researcher asked follow-up questions designed to elicit feedback from the customer service representative to address those aspects of the Code that were not already covered verbally; and an unprompted scenario where no follow-up questions were asked. Table 2.2 presents overall ratings of the degree to which procedural information relating to the issuance of debit cards was communicated to the researchers (either verbally or in writing), as well as the distribution of ratings according to which scenario was used. For most types of information pertaining to general procedural information when issuing debit cards, we observe that a high proportion of financial institutions visited through the spot checks complied with the Code (i.e., rating of 3 or 4 on a 4-point scale). Financial institutions were most likely to comply with the Code in terms of ensuring that the card and PIN were or would be delivered to the intended cardholder (95 per cent) and informing the applicant of any fees associated with holding and using the PIN (95 per cent), followed by ensuring that the PIN was disclosed only to the cardholder, or selected only by the cardholder (93 per cent) and commencing debit card service only on receipt of a signed request from the applicant (93 per cent). Financial institutions were least likely to comply with the Code in terms of providing the cardholder with a copy of the cardholder agreement (78 per cent) and informing the applicant of the purpose and functions of the PIN (65 per cent).

TABLE 2.2 of EKOS Evaluation
Communication of Procedural Information When Issuing Debit Cards

Prompted Scenario (n=20)						Unprompted Scenario (n=20)						Overall % in compliance**
1*	2	3	4	9	% In compliance**	1	2	3	4	9	% In compliance**	
"To what extent did the institution personnel inform the applicant … of each of the following standards related to the issuance of debit cards? "												
Ensure that the card and PIN [were or would be] delivered to the intended cardholder												
0	0	11	9	0	**100%**	1	1	12	6	0	**90%**	**95%**
Inform the applicant of any fees associated with holding and using the PIN												
0	1	14	5	0	**95%**	0	1	14	5	0	**95%**	**95%**
Ensure that the PIN was disclosed only to the cardholder, or selected only by the cardholder												
0	0	11	9	0	**100%**	2	1	13	4	0	**85%**	**93%**
Commence debit card service only on receipt of a signed request from the applicant												
1	0	16	3	0	**95%**	2	0	16	2	0	**90%**	**93%**
Enable the applicant to choose which eligible accounts the card will access												
1	0	15	4	0	**95%**	3	0	11	6	0	**85%**	**90%**
Inform the applicant of how to contact the card/PIN issuer in the event of a problem***												
0	0	15	5	0	**100%**	0	4	14	2	0	**80%**	**90%**
Inform the applicant of the purpose and functions of the card												
0	1	17	2	0	**95%**	2	2	14	2	0	**80%**	**88%**
Provide the cardholder with a copy of the cardholder agreement												
3	0	13	4	0	**85%**	6	0	11	3	0	**70%**	**78%**
Inform the applicant of the purpose and functions of the PIN												
1	4	12	3	0	**75%**	6	3	10	1	0	**55%**	**65%**

* 1=no reference to clause, 2=contradicts code or insufficient information provided, 3=meets code, 4=exceeds code, 9= refers to documents or information alluded to but not provided
** Presents the proportion of cases that received a rating of 3 or 4
*** Originally coded as two separate questions.

It is important to note that for all but one clause of the Code reviewed here (i.e., informing the applicant of any fees associated with holding and using the PIN), financial institutions were more likely to be in compliance with the Code during the prompted scenario than the unprompted scenario, suggesting that financial institutions do not necessarily volunteer all of the pertinent general procedural information pertaining to the issuance of debit cards.

Another noteworthy finding related to the different levels of adherence observed for the prompted and unprompted spot checks concerns the degree to which researchers were provided with copies of the cardholder agreement. Overall, cardholder agreements were provided in approximately three-quarters (78 per cent) of the spot checks conducted, and were more likely to have been distributed during the prompted spot checks (85 per cent) than the unprompted spot checks (70 per cent).

Finally, while only 37 per cent of documentation informed cardholders that they could choose which eligible accounts their debit card could access (Table 2.1), it should be noted that the compliance rate was much higher for the mystery shopping exercise (i.e., the spot checks of card issuers). In both prompted and unprompted scenarios, a large majority of the financial institutions visited informed the researchers that they could choose which eligible accounts the debit card could access (95 and 85 per cent, respectively).

The spot checks of card issuers also collected information on the degree to which financial institutions adhered to the Code with respect to clauses dealing with general security issues when issuing debit cards (Table 2.3). Financial institutions were most likely to comply with the Code in terms of informing applicants of their responsibility for PIN security (85 per cent), of the cardholder's responsibility for card security (78 per cent) and of how to avoid unauthorized use of the card/PIN and outlining unacceptable PIN combinations (75 per cent). Moderately lower rates of adherence were found for the degree to which applicants were informed of the possible consequences of a breach of their responsibility for PIN security (63 per cent), the possible consequences of a breach of their responsibility for card security (60 per cent), and the potential extent of losses that could occur due to unauthorized use of the card and PIN (53 per cent).

It is not surprising that similar overall rates of adherence were found for the latter three clauses of the Code if we consider that they address similar security issues, namely the potential consequences of unauthorised debit card use. The fact that these three items received lower ratings suggests that cardholders are not always receiving information that could prove to be a useful incentive for ensuring card and PIN security. It is also apparent that levels of compliance for the prompted scenario are higher than those for the unprompted

scenario for all security issues pertaining to the issuance of debit cards, once again suggesting that this information is not always being volunteered to cardholders.

TABLE 2.3 of EKOS Evaluation
Communication of Security Information When Issuing of Debit Cards

Prompted Scenario (n=20)						Unprompted Scenario (n=20)						Overall % in compliance**
1*	2	3	4	9	% in compliance**	1	2	3	4	9	% in compliance**	
"To what extent did the institution personnel inform the applicant … of each of the following standards related to the issuance of debit cards? "												
Inform the applicant of the cardholder's responsibility for PIN security												
0	0	17	3	0	**100%**	4	2	13	1	0	**70%**	**85%**
Inform the applicant of the cardholder's responsibility for card security												
0	2	14	4	0	**90%**	4	3	12	1	0	**65%**	**78%**
Advise the cardholder of how to avoid unauthorized use of the card/PIN and outline unacceptable PIN combinations												
0	1	15	4	0	**95%**	4	5	10	1	0	**55%**	**75%**
Inform the applicant of the possible consequences of a breach of their responsibility for PIN security												
0	5	14	1	0	**75%**	5	5	9	1	0	**50%**	**63%**
Inform the applicant of the possible consequences of a breach of their responsibility for card security												
1	4	13	2	0	**75%**	7	4	8	1	0	**45%**	**60%**
Advise the cardholder of the potential extent of losses that could occur due to unauthorized use of the card and PIN												
0	6	12	2	0	**70%**	6	7	6	1	0	**35%**	**53%**

* 1=no reference to clause, 2=contradicts code or insufficient information provided, 3=meets code, 4=exceeds code, 9= refers to documents or information alluded to but not provided
** Presents the proportion of cases that received a rating of 3 or 4

2.3 Consumer Use of Secure PINs

While the documentation review and spot checks of card issuers attempted to examine the extent to which efforts are made to impart relevant information to cardholders, the survey of cardholders collected evidence of the degree to which this information is applied. Four in ten respondents indicate that their PIN is a random number, either one that they had chosen themselves (27 per cent) or that was generated by their financial institution (14 per cent). About one-third of respondents report using personal information as the basis for their PIN – including 23 per cent who use personal information such as a birth date or phone number and another 10 per cent whose PIN is based on a combination of familiar numbers (e.g., age and address). Thirteen per cent transformed a word or name into a number and six per cent use

an easy combination of numbers to remember (e.g., 1234, 2222). These results show that overall, roughly one-quarter of the cardholders surveyed (23 per cent) report using a PIN that is based on some easily guessed or obtained number (i.e., personal information).

In terms of sub-group differences:

- youth are more likely to use a name or word transformed into a number for their PIN, while older cardholders (age 60 and over) are more likely to use a random number; and
- those who never use their debit card for ABM withdrawals are more likely to use a PIN based on personal information than those who are more frequent users of debit cards.

2.4 FI Advice on the Selection of PINs

Since one of the major aspects of PIN security concerns the degree to which cardholders are well informed of the proper criteria to be used for the choice of PIN, documentation was also reviewed to determine the overall number and nature of the criteria outlined in the documentation[2]. Both cardholder and internal documents on average provide five examples of types of information that should not be used to choose a PIN. The most common examples provided for unsafe PINs are birth dates (100 per cent), telephone numbers (89 per cent) and addresses (63 per cent). Other examples that were listed somewhat less frequently include various other familiar numbers (e.g., SIN, license, sequential numbers) (42 per cent), the cardholder's or a relative's name (26 per cent) and a PIN or number for another account (16 per cent).

[2] It should be noted that documentation was also rated according to a number of other criteria (e.g., extent to which the information emphasizes the importance of ensuring card/PIN security, the clarity of language, format of materials for ease of use). It was decided, however, that ratings of these characteristics of the documentation were insufficiently reliable (given their subjective nature and the absence of operational definitions for the criteria) to allow for an accurate assessment of the documentation on this basis.

3 PIN SECURITY AND LIABILITY FOR LOSS

3.1 Documented Adherence to the Code

The documentation received from financial institutions was also rated according to the degree to which it addressed liability for loss issues outlined in the Code. As shown in Table 3.1, overall rates of adherence to the Code in terms of the degree to which documentation communicated information concerning liability for loss issues tend to be somewhat lower than those observed for issues relating to issuing debit cards. Documentation was most likely to comply with the Code in terms of specifying that cardholders are responsible for all authorized use of valid cards (95 per cent), and that cardholders are not liable for losses resulting from technical problems, card issuer errors, and other system malfunctions (89 per cent). The lowest rates of compliance were observed for the extent to which the documentation specifies that cardholders are not liable for losses resulting from circumstances beyond their control (53 per cent), a cardholder contributes to unauthorized use by voluntarily disclosing the PIN (53 per cent), when cardholders contribute to unauthorized use (other than use resulting from circumstances beyond the cardholder control), the cardholder will be liable (53 per cent), and a cardholder contributes to unauthorized use by failing to notify the issuer that the card has been lost, stolen or misused, or that the PIN may have become known to someone other than the cardholder (42 per cent).

It should be noted that three of the four clauses yielding the lowest levels of compliance with the Code are clauses that define those instances in which cardholders contribute to unauthorised use, suggesting one area in which cardholders may not be adequately informed of their responsibilities with respect to debit cards and PINs. A comparison of compliance rates for cardholder and internal documentation reveals that for most clauses of the Code dealing with liability for loss, similar levels of compliance were observed.

TABLE 3.1 of EKOS Evaluation
Adherence of Documentation to the Code - Liability for Loss

Cardholder Documentation Ratings (n=10)						Internal Documentation Ratings (n=9)						Overall % in compliance**
1*	2	3	4	9	% in compliance**	1	2	3	4	9	% in compliance**	
"Did the institution's documentation specify that … "												
Cardholders are responsible for all authorized use of valid cards.												
0	1	9	0	0	**90%**	0	0	9	0	0	**100%**	**95%**
Cardholders are not liable for losses resulting from technical problems, card issuer errors, and other system malfunctions.												
1	0	9	0	0	**90%**	1	0	7	0	1	**88%**	**89%**
Cardholder liability for losses will not exceed the established debit card transaction withdrawal limits, including instances where an account has a line of credit or overdraft protection, is linked with other accounts, or a transaction is made on the basis of a fraudulent deposit.												
1	1	8	0	0	**80%**	1	0	8	0	0	**89%**	**84%**
Cardholder liability for loss could include losses for overdraft, other accounts linked to the debit card, such as a line of credit, and fraudulent deposits.												
2	0	8	0	0	**80%**	2	0	7	0	0	**78%**	**79%**
Cardholders are not liable for losses resulting from unauthorized use of a card and PIN where the issuer is responsible for preventing such use												
0	2	8	0	0	**80%**	1	2	4	2	0	**67%**	**74%**
Cardholders are not liable for losses resulting from unauthorized use, where the cardholder has unintentionally contributed to such use, provided the cardholder co-operates in any subsequent investigation.												
2	1	7	0	0	**70%**	2	0	7	0	0	**78%**	**74%**
Cardholders are responsible if they make entry errors at point-of-service terminals, or if they make fraudulent or worthless deposits.												
1	3	6	0	0	**60%**	1	2	6	0	0	**67%**	**63%**
Cardholders are not liable for losses resulting from circumstances beyond their control												
1	4	5	0	0	**50%**	2	2	5	0	0	**56%**	**53%**
A cardholder contributes to unauthorized use by 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.												
0	6	4	0	0	**40%**	1	2	5	1	0	**67%**	**53%**
When a cardholder contributes to unauthorized use (other than use resulting from circumstances beyond the cardholder's control), the cardholder will be liable for the resulting loss.												
0	6	4	0	0	**40%**	1	2	5	1	0	**67%**	**53%**
A cardholder contributes to unauthorized use by 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.												
0	6	3	1	0	**40%**	1	4	3	1	0	**44%**	**42%**

* 1=no reference to clause, 2=contradicts code or insufficient information provided, 3=meets code, 4=exceeds code, 9= refers to documents or information alluded to but not provided

** Presents the proportion of cases that received a rating of 3 or 4

3.2 Observed Adherence to the Code

Overall ratings of the degree to which liability for loss issues were communicated (either verbally or through written documents) to researchers during the spot checks of card issuers are based on the highest of the three ratings (one for each of verbal, cardholder and other literature) provided for each issue. Table 3.2 shows the highest rates of compliance were observed for the degree to which institution personnel informed the applicants that cardholders are responsible for all authorized use of valid cards (83 per cent), that cardholders liability for losses will not exceed the established debit card transaction withdrawal limits (75 per cent), and that cardholders are not liable for losses resulting from unauthorized use of a card and PIN where the issuer is responsible for preventing such use (68 per cent). The financial institutions visited were least likely to comply with the Code in terms of informing the applicant that cardholders are not liable for losses resulting from circumstances beyond their control (45 per cent), when a cardholder contributes to unauthorized use, the cardholder will be liable for the resulting loss (45 per cent), and that cardholders are responsible if they make entry errors at point-of-service terminals, or if they make fraudulent or worthless deposits (40 per cent).

Once again, it is important to note that compliance was observed for all clauses of the Code dealing with liability for loss during a majority of the prompted scenario spot checks, but that much lower proportions of institutions informed applicants of these issues during the unprompted scenarios. These findings suggest that while staff may be informed of these issues, they tend not to share the information unless a specific enquiry is made.

TABLE 3.2 of EKOS Evaluation
Communication of Information Pertaining to PIN Security and Liability for Loss
During the Card Issuer Spot Checks

Prompted Scenario (n=20)						Unprompted Scenario (n=20)						Overall % in compliance**
1*	2	3	4	9	% in compliance**	1	2	3	4	9	% in compliance**	
"To what extent did the institution personnel inform the applicant … of each of the following standards pertaining to liability for loss?"												
Cardholders are responsible for all authorized use of valid cards.												
0	2	16	2	0	**90%**	5	0	14	1	0	**75%**	**83%**
Cardholder liability for losses will not exceed the established debit card transaction withdrawal limits, including instances where 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												
2	1	16	1	0	**85%**	7	0	13	0	0	**65%**	**75%**
Cardholders are not liable for losses resulting from unauthorized use of a card and PIN where the issuer is responsible for preventing such use												
1	2	16	1	0	**85%**	6	4	10	0	0	**50%**	**68%**
Cardholders are not liable for losses resulting from unauthorized use, where the cardholder has unintentionally contributed to such use, provided the cardholder co-operates in any subsequent investigation.												
2	3	15	0	0	**75%**	8	2	9	1	0	**50%**	**63%**
A cardholder contributes to unauthorized use by 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.												
0	2	16	2	0	**90%**	7	7	5	1	0	**30%**	**60%**
Cardholders are not liable for losses resulting from technical problems, card issuer errors, and other system malfunctions.												
3	3	13	1	0	**70%**	8	2	10	0	0	**50%**	**60%**
A cardholder contributes to unauthorized use by 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.												
0	6	12	2	0	**70%**	5	7	8	0	0	**40%**	**55%**
Cardholders are not liable for losses resulting from circumstances beyond their control.												
1	6	12	1	0	**65%**	8	7	5	0	0	**25%**	**45%**
When a cardholder contributes to unauthorized use (other than use resulting from circumstances beyond the cardholder's control), the cardholder will be liable for the resulting loss.												
0	8	11	1	0	**60%**	7	7	5	1	0	**30%**	**45%**
Cardholders are responsible if they make entry errors at point-of-service terminals, or if they make fraudulent or worthless deposits.												
1	9	9	1	0	**50%**	7	7	6	0	0	**30%**	**40%**

* 1=no reference to clause, 2=contradicts code or insufficient information provided, 3=meets code, 4=exceeds code, 9= refers to documents or information alluded to but not provided
** Presents the proportion of cases that received a rating of 3 or 4

3.3 Consumer Awareness of Responsibilities

Respondents to the survey of cardholders were asked about the steps a cardholder should take to protect the security of their PIN. It should be mentioned that respondents were asked this question in a free recall fashion (i.e., they were not read a list and asked whether they agreed with each of a number of possible courses of action), thus these results represent respondents' unaided recall. Four in ten (42 per cent) respondents mentioned shielding entry of their PIN number when using a PIN pad. More than one-third of respondents (39 per cent) noted that a PIN should never be revealed to someone else and just under one-third mentioned security steps related to maintaining a separation between the PIN and the debit card (27 per cent indicating a PIN should never be written down unless it is disguised and another four per cent mentioned that the PIN and card should not be kept together). Roughly one in four respondents (23 per cent) noted the PIN combination itself as important in protecting security and four per cent mentioned changing the PIN number periodically. Differences by sub-groups include:

- women are more likely to mention avoiding writing their PIN down while men more often noted shielding entry of their PIN when using a PIN pad;
- likelihood of mentioning not using an obvious PIN combination decreases with age, and older cardholders were more likely to mention not writing one's PIN down unless it is disguised; and
- those with lower levels of education and income are more likely to mention not revealing your PIN as a step to take to protect PIN security.

Reflecting the findings above, 92 per cent of respondents completely disagreed with the statement "A written copy of my PIN is best kept close to my debit card to ensure that I can always find it when using my debit card". Women, English-speaking respondents and those with a university education were more likely to disagree with this statement. Those in the lowest income category (earning less than $20,000) were less likely to disagree with this statement.

The vast majority of cardholders are aware of their responsibilities to report losses quickly when a debit card is lost or stolen. Virtually all cardholders (98 per cent)

indicate that they would report a lost or stolen card to the card issuer as soon as they became aware of it.

3.4 Consumer Awareness of Liability for Loss

The survey of cardholders indicates that consumers' level of awareness of liability for loss is mixed. On the one hand, consumers are conscious of their responsibilities for PIN secrecy and the link between this responsibility and liability for loss. Eight in ten respondents disagree that that they "would not be responsible for loss if they revealed their PIN and someone used their card without their consent" (lower among youth, women and those with lower levels of education and income). Put another way, 80 per cent of respondents understand that they would be liable for any losses if they revealed their PIN and someone used their card without their consent, while 16 per cent were unaware of their liability in this instance.

On the other hand, the PIN combination itself was less closely tied to liability for loss. Twenty-one per cent agree that they would not be reimbursed for money taken if their PIN was based on a number found in another document and someone else used their card. Over half of respondents (57 per cent), however, disagree with this statement (higher among older age cardholders), suggesting that a large proportion of the respondents surveyed do not appreciate their liability for losses that could result from their choice of PIN.

Four in ten cardholders agree that, if found responsible, they could be liable for money taken from an overdraft or a line of credit (women and those with higher levels of income were more likely to agree). One-third of respondents overall, however, disagree with this statement, once again indicating that a large number of cardholders are unaware of the limits to their liability.

3.5 Perceptions of Security

One half of survey respondents (49 per cent) indicate they are very comfortable (responded with a six or seven on a seven-point scale) and 44 per cent are

moderately comfortable (responded with a three, four or five on a seven-point scale) with the privacy and security of banking transactions (e.g., withdrawal of money) using their debit card. A small minority, six per cent, indicate that they are not comfortable with the level of privacy and security afforded these transactions (responded with a one or two on a seven-point scale).

Cardholders indicate a lesser degree of comfort with their ability to enter their PIN without others seeing it when carrying out POS transactions. Twenty-eight per cent indicate they are very comfortable and just over one-half (54 per cent) are moderately comfortable that they can enter their PIN without others seeing it when conducting these transactions. Fifteen per cent report only a small level of comfort (responded with a one or two on a seven-point scale) when entering their PIN during POS transactions.

When asked whether they had concerns with a lack of privacy when entering their PIN at various different types of outlets, about one-third of respondents indicate that they do not have any.

Among those who express privacy concerns, these concerns are more likely to be related to transactions at commercial outlets rather than at ATMs/ABMs. Four in ten respondents indicate they have concerns about lack of privacy at stores featuring a lane environment (e.g., grocery stores, liquor stores, discount stores). One-third of cardholders have privacy concerns in outlets where customers pay for items at counters located throughout the store (such as department stores) and the same proportion are concerned about privacy at smaller commercial outlets (e.g., gas stations and corner stores). Privacy concerns at ATMs/ABMs outside of financial institutions were noted by 28 per cent, and 27 per cent mentioned entertainment outlets (such as movie theatres, restaurants or bars). Of least concern (mentioned by 16 per cent of respondents) are ATMs/ABMs at financial institutions.

The types of privacy concerns mentioned by surveyed cardholders focus on a lack of shielding of the PIN pad (41 per cent) (higher among the most frequent debit card users). One-third are concerned about their inability to screen the PIN pad with their body and a similar proportion have concerns about the proximity of other customers (higher among the oldest age category and among less frequent debit card users at point-of-service). One-quarter of respondents mentioned too little shielding around the ABM as the source of their privacy

concerns. Other issues (mentioned by fewer than ten per cent) included: inability to move the PIN pad on a cord or to swivel the PIN pad, proximity of staff and proximity of security cameras in the store.

3.6 Point-of-service Security

a) *Interviews with Merchants*

A series of key informant interviews were conducted with merchants to solicit their perspectives concerning the degree to which their point-of-service terminals provide sufficient security for debit card users. Merchants interviewed as part of the evaluation were most likely to represent a chain of stores (16 *versus* 5 independent merchants).

Of those respondents who indicated that their PIN pads are leased, just more than half stated that they had an agreement or contract with the financial institution specifying the manner in which the debit card services are to be delivered, while the remaining respondents were unaware of whether such an agreement existed. When respondents were asked whether they were aware of the requirement that retailers install PIN pads such that they provide sufficient privacy to allow customers to enter their PIN with a minimum risk of it being observed by others, roughly half (including all of the experts) indicated that they were aware of this requirement. Once again, this suggests that merchants may not always be fully aware of their responsibilities concerning the security of the POS terminals.

Overall, the PIN pads employed by the merchants interviewed for the study appear to have most of the characteristics associated with providing a secure environment. All but one of the merchants indicated that their PIN pad was on a cord and only two of these respondents felt that the cord was not long enough for customers to move the PIN pad to within a hand's width of their chest. One-quarter of the merchants indicated that their PIN pad had both a cord and a shield. Of the two respondents who used fixed PIN pads, both had shields, although only one swivelled. None of the merchants we spoke to reported that their PIN pads lacked both a cord and a shield.

Only three merchants interviewed for the evaluation (all of whom were experts) indicated that their organization has ever experienced difficulties in providing privacy. Two indicated that these difficulties concerned malfunctioning PIN pads, while the third mentioned that some older customers had requested that the cashiers enter their PINs for them. To overcome this problem, this respondent indicated that staff had been instructed never to involve themselves in the customers' transactions (i.e., do not swipe cards, enter PINs or otherwise handle the PIN pad during the transaction). When asked if they believe the PIN pads in their stores allow customers to enter their PINs with minimum risk of the being observed by others, only three merchants mentioned that they did not feel this was the case.

Roughly half of the merchants interviewed reported that some form of staff training is provided to ensure the secure operation of their PIN pads. This training most often involves showing the employees how to use the PIN pads or training on security issues as part of their general instruction. Finally, merchants were asked to provide suggestions about how to improve the security of their PIN pads. While most respondents did not provide a suggestion, others offered that technical or physical changes to the pads might enhance security, such as more shielding, the use of longer PINs, and screens which cannot be seen unless the customer stares directly at it. Other suggestions include more staff training and for customers to use cash if they have concerns about the security of using debit cards for point-of-service transactions.

b) *Point-of-Service Spot Checks*

The results in relation to the point-of-service checks were examined separately for point-of-sale terminals and ATM/ABM machines.

Visits to determine the characteristics of point-of-sale terminals revealed that a higher proportion of the PIN pads examined as part of the evaluation were on a cord (90 *versus* 10 per cent fixed PIN pads).

Of those PIN pads that were on a cord, over three-quarters (77 per cent) had cords which were long enough to come within a hands width of the researchers chest, although only 22 per cent had shields. For fixed PIN pads at point-of-sale terminals, we observe that 71 per cent swivel and over three-quarters provide shielding (86 per cent).

To assess the effectiveness of these security features, researchers were also asked to record whether staff or other customers were able to view entry of the PIN without making any meaningful effort to do so. The results show that for 14 per cent of spot checks at point-of-sale terminals, members of the staff were able to view entry of the researchers' PIN, while for 35 per cent of spot checks the other customers were able to do so.

During the spot checks, researchers were also asked to record those characteristics of the point-of-sale terminals that reduced or increased the risk of the PIN being revealed to others. Those characteristics most often associated with reduced risk of exposing the PIN were the ability for the customer to screen the PIN pad with their body (85 per cent), the ability to move the PIN pad on a cord (83 per cent), and the inability of other customers to get close enough to observe the cardholder's PIN (43 per cent). Characteristics most likely to be associated with an increased risk of the PIN being revealed to others were too little shielding provided for the PIN pad (43 per cent) and the ability/inability to swivel the PIN pad (36 per cent).

When asked in another question about any other relevant features that enhanced the privacy and security of the point-of-sale terminals, researchers pointed to the additional space around the terminal (21 per cent). Among the other relevant features of the point-of-sale terminals which were felt to decrease privacy and security, researchers were more likely to make note of a lack of space around the terminal (25 per cent), other features such as security cameras or very large PIN pads (17 per cent), and the fact that the merchant swiped the researchers debit card (17 per cent).

The characteristics of ATMs/ABMs that were most often associated with reduced risk of exposing the PIN were the inability of other customers to get close enough to observe the cardholder's PIN (63 per cent), the ability for the customer to screen the PIN pad with their body (50 per cent), and sufficient shielding around the ABM (38 per cent). Characteristics most likely to be associated with an increased risk of the PIN being revealed to others were too little shielding (50 per cent) and the ability for customers to get close enough to observe the cardholder's PIN (38 per cent).

4 DISPUTE RESOLUTION

4.1 Documented Adherence to the Code

The third general issue area examined through the review of cardholder documents involved the degree to which the financial institution's documentation addressed issues pertaining to dispute resolution. Those components of the Code dealing with dispute resolution with which the documentation was most likely to comply include the degree to which the documentation informed the reader that a cardholder should first attempt to resolve the problem with the card issuer in the event of a problem with a debit card transaction (100 per cent), that card issuers will have clear, timely procedures for dealing with debit card transaction problems, which provide for review of problems at a senior level within their organizations (100 per cent) and that a cardholder should resolve the problem with the retailer in the event of a problem with merchandise or retail service (89 per cent). Compliance with the Code was least likely to be observed for those clauses which indicate that the institution should inform the reader that during the dispute-resolution process, cardholders will not be unreasonably restricted from the use of funds which are the subject of the dispute (47 per cent) and that card issuers will provide information on how the dispute resolution process works and how long each stage will take under normal circumstances (42 per cent).

Few differences were observed between cardholder and internal documents in terms of compliance levels for issues pertaining to dispute resolution. Nonetheless, documents used internally by staff tended to yield higher rates of adherence to the Code in terms of informing the cardholder of the existence of the Canadian Code of Practice for Consumer Debit Card Services (78 *versus* 60 per cent for cardholder documents) and that a cardholder whose problem cannot be settled by the card issuer will be informed of the reasons for the issuer's position on the matter and advise the cardholder of the appropriate party to contact regarding the dispute (67 *versus* 30 per cent for cardholder documents).

TABLE 4.1 of EKOS Evaluation
Adherence of Documents to the Code - Dispute Resolution

Cardholder Documentation Ratings (n=10)						Internal Documentation Ratings (n=9)						Overall % in compliance**
1*	2	3	4	9	% in compliance**	1	2	3	4	9	% in compliance**	
To what degree is the documentation consistent with … each of the following dispute resolution issues?												
In the event of a problem with a debit card transaction, a cardholder should first attempt to resolve the problem with the card issuer.												
0	0	10	0	0	**100%**	0	0	9	0	0	**100%**	**100%**
Card issuers will have clear, timely procedures for dealing with debit card transaction problems, which provide for review of problems at a senior level within their organizations.												
0	0	10	0	0	**100%**	0	0	7	2	0	**100%**	**100%**
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.												
1	0	9	0	0	**90%**	1	0	8	0	0	**89%**	**89%**
The cardholder is informed of the existence of the Canadian Code of Practice for Consumer Debit Card Services												
3	1	6	0	0	**60%**	2	0	5	2	0	**78%**	**68%**
A cardholder whose problem cannot be settled by the card 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.												
0	7	3	0	0	**30%**	0	3	5	1	0	**67%**	**47%**
During the dispute-resolution process, cardholders will not be unreasonably restricted from the use of funds which are the subject of the dispute.												
5	0	5	0	0	**50%**	4	1	4	0	0	**44%**	**47%**
If a problem with a debit card transaction cannot be settled when the cardholder first complains, the card issuer will provide information on how the dispute-resolution process works and on how long each stage will take under normal circumstances.												
0	6	3	1	0	**40%**	0	5	2	2	0	**44%**	**42%**

* 1=no reference to clause, 2=contradicts code or insufficient information provided, 3=meets code, 4=exceeds code, 9=refers to documents or information alluded to but not provided
** Presents the proportion of cases that received a rating of 3 or 4

4.2 Observed Adherence to the Code

When evidence gathered through the spot checks was examined to determine the degree to which financial institutions are adhering to the Code, it was found that lower levels of adherence, relative to what the institutions have documented, were observed for all components of the Code dealing with dispute resolution, although the same general patterns were observed in terms of those areas of highest and lowest adherence (Table 4.2). The highest overall compliance rates were observed for the degree to which the researchers were informed that cardholders should first attempt to resolve the problem with the card issuer in the event of a problem with a debit card transaction (65 per cent), that cardholders should resolve the problem with the retailer concerned in the event of a problem with merchandise or retail service (63 per cent) and that card issuers will have clear, timely procedures for dealing with debit card transaction problems, which provide for review of problems at a senior level within their organizations (45 per cent). Researchers were least likely to be informed that if a problem with a debit card transaction cannot be settled when the cardholder first complains, the card issuer will provide information on how the dispute-resolution process works and on how long each stage will take under normal circumstances (28 per cent), that during the dispute-resolution process, cardholders will not be unreasonably restricted from the use of funds which are the subject of the dispute (25 per cent), and that a cardholder whose problem cannot be settled by the card issuer will be informed of the reasons for the issuer's position on the matter and of the appropriate party to contact regarding the dispute (20 per cent). Once again, observed adherence was higher during the prompted scenarios for most issues pertaining to dispute resolution.

TABLE 4.2 of EKOS Evaluation
Overall Adherence to the Code During Spot Checks – Dispute Resolution

Prompted Scenario (n=20)						Unprompted Scenario (n=20)						Overall
1*	2	3	4	9	% in compliance**	1	2	3	4	9	% in compliance**	% in compliance**
"To what extent did the institution personnel inform the applicant … of each of the following standards pertaining to dispute resolution?"												
In the event of a problem with a debit card transaction, a cardholder should first attempt to resolve the problem with the card issuer.												
4	1	14	1	0	**75%**	6	3	9	2	0	**55%**	**65%**
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.												
5	1	14	0	0	**70%**	9	0	11	0	0	**55%**	**63%**
Card issuers will have clear, timely procedures for dealing with debit card transaction problems, which provide for review of problems at a senior level within their organizations.												
6	4	9	1	0	**50%**	10	2	7	1	0	**40%**	**45%**
If a problem with a debit card transaction cannot be settled when the cardholder first complains, the card issuer will provide information on how the dispute-resolution process works and on how long each stage will take under normal circumstances.												
9	5	6	0	0	**30%**	12	3	5	0	0	**25%**	**28%**
During the dispute-resolution process, cardholders will not be unreasonably restricted from the use of funds which are the subject of the dispute.												
12	1	7	0	0	**35%**	17	0	3	0	0	**15%**	**25%**
A cardholder whose problem cannot be settled by the card 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.												
12	4	4	0	0	**20%**	11	5	3	1	0	**20%**	**20%**

* 1=no reference to clause, 2=contradicts code or insufficient information provided, 3=meets code, 4=exceeds code, 9=refers to documents or information alluded to but not provided
** Presents the proportion of cases that received a rating of 3 or 4

4.3 Cardholder Complaints

In this section we review the call centre complaint data provided by the financial institutions that participated in the evaluation, as well as complaints received by the Office of the Superintendent of Financial Institutions (OSFI) and the Canadian Banking Ombudsman (CBO) over a one-year period. Most financial institutions and consumer associations were unable to provide the data requested for this phase of the research because these organizations do not collect and store information on complaints in a manner that would allow them to retrieve this information or to distinguish debit card and other complaints. Furthermore, the data that were received was generally not provided in the detail requested. For instance, while researchers had requested that complaints involving transaction errors or problems be broken down into more detailed categories, some financial institutions were only able to supply overall numbers of complaints that fall into this broader category. As such, it is important to point out that the complaint data presented in this section provides only a rough overview of the types of complaints received by financial institutions and other organizations and should not be viewed as a comprehensive profile of consumer complaints as they pertain to debit cards.

Table 4.5 presents an aggregation of all complaint data received by the four financial institutions that participated in this phase of the research. These data show that 83 per cent of the complaints received by the call centres (see rows c and f) involve transaction errors or problems (82.4 per cent *versus* 17.3 per cent for unauthorized or fraudulent transactions). Among the complaints categorised as transaction errors, financial institutions were unable to classify the complaint into one of the sub-categories 75 per cent of the time. Of those complaints concerning transaction errors that were classified, the financial institutions report that most involved complaints about the ABM dispensing an incorrect amount (9.8 per cent), followed by ABM deposit errors/discrepancies (9.0 per cent) or bill payments which were not received or received late (4.9 per cent). While no information was provided concerning how most of these specific complaints were resolved, the most likely resolution for transaction errors or problems was that the client was reimbursed (11.2 per cent). Clients were found to be responsible for the loss for 3.2 per cent of these cases and only two complaints were pending resolution.

Those complaints involving unauthorised or fraudulent transactions that the financial institutions were able to classify were most likely to involve unauthorized ABM cash

withdrawal (35 per cent), followed by worthless items on the ABM deposit (26.3 per cent), empty ABM deposit envelopes (16.3 per cent), the client not remembering having done the transaction (15 per cent), and an unauthorized debit transaction at a point-of-service terminals (6.3 per cent). Clients were only slightly more likely to be reimbursed (37.5 per cent) than to be found responsible (32.5 per cent) for these transactions. Relatively small numbers of these complaints were still pending resolution (2.5 per cent) or had been referred to the Canadian Banking Ombudsman (1.3 per cent). It is also important to note that a higher rate of resolution appear to have been observed for unauthorised or fraudulent transactions relative to transaction errors or problems, however, the incomplete nature of the data received means this observation should be treated with caution.

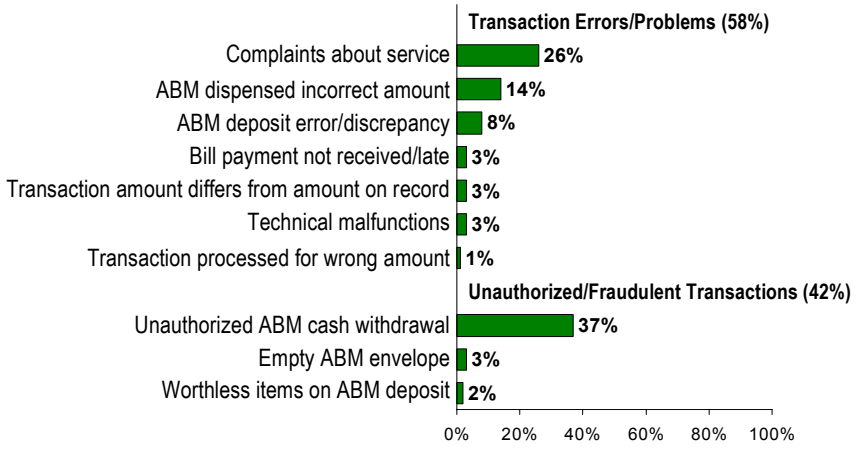
TABLE 4.5 of EKOS Evaluation
Distribution of Call Centre Complaints Over a One-Year Period

Type of Complaint	Total Complaints	Resolution of Compliant			
		Client Reimbursed	Client Responsible for loss	Pending Resolution	Referred to CBO
Transaction Error/Problem					
ABM dispensed incorrect amount	**40 (9.8%)***	28	2	--	--
ABM deposit error/discrepancy	**37 (9.0%)**	7	7	1	--
Bill payment not received/received late	**20 (4.9%)**	5	3	--	--
Transaction amount posted differs from amount on transaction record	**2 (0.5%)**	1	--	--	--
Duplicate transaction	**2 (0.5%)**	1	--	--	--
Cardholder/retailer processed transaction for wrong amount	**1 (0.2%)**	--	1	1	--
Transaction posted to wrong account	**--**	--	--	--	--
Other	**307 (75.1%)**	4	--	--	--
a) Total Transaction Errors/Problems Classified	**409**	**46 (11.2%)****	**13 (3.2%)**	**2 (0.5%)**	**--**
b) Total Transaction Errors/Problems Not Classified***	138	--	--	--	--
c) Total Transaction Errors/Problems	**547 (82.4%)******	--	--	--	--
Unauthorized/Fraudulent Transactions					
Unauthorized ABM cash withdrawal	**28 (35.0%)***	10	2	2	1
Worthless items on ABM deposit	**21 (26.3%)**	5	16	--	--
Empty ABM deposit envelope	**13 (16.3%)**	8	4	--	--
Do not remember doing transaction	**12 (15.0%)**	6	3	--	--
Unauthorized debit transaction at point-of-service terminal	**5 (6.3%)**	1	1	--	--
Other	**1 (1.3%)**	--	--	--	--
d) Total Unauthorised/Fraudulent Transactions Classified	**80**	**30 (37.5%)****	**26 (32.5%)**	**2 (2.5%)**	**1 (1.3%)**
e) Total Unauthorised/Fraudulent Transactions Not Classified***	35	--	--	--	--
f) Total Unauthorised/Fraudulent Transactions	**115 (17.3%)******	--	--	--	--
g) TOTAL COMPLAINTS	**664**	**--**	**--**	**--**	**--**

* Percentages reflect the total number of complaints in the small sub-categories, divided by the total number of complaints that the financial institutions were able classify into one or another of the two broad sub-categories (labelled as rows “a)” and “d)”).
** Reflects the proportion of complaints resolved out of the total number of complaints which the financial institutions were able to classify (i.e., total columns for row “a)” or row “d)”). Note that information concerning the resolution of the complaint was provided for only a small proportion of classified complaints.
*** Represents complaint data from one financial institution which was not classified into the appropriate sub-categories
**** Percentages reflect total number of complaints in the two primary categories (i.e., row “c” of transaction errors/problems or row “f” of unauthorized/fraudulent transactions) divided by overall total number of complaints presented in row g.

A similar distribution is observed for complaints received from the OSFI and the Canadian Banking Ombudsman. Once again, most of these complaints involved transaction errors or problems (58 per cent), although the higher proportion of unauthorised or fraudulent transactions received by these institutions (42 *versus* 17.3 per cent of call centre complaints) indicates that these more serious complaints are more likely to be addressed outside of the financial institutions themselves. The most common type of complaint concerning transaction errors or problems received by these institutions involved general complaints about service, such as accessibility, denominations dispensed and lighting (26 per cent), followed by ABMs dispensing an incorrect amount (14 per cent) and ABM deposit errors or discrepancies (eight per cent). The types of complaints involving unauthorised or fraudulent transactions that were received by the OSFI and Canadian Banking Ombudsman included unauthorised ABM cash withdrawals (37 per cent), empty ABM envelopes (three per cent) and worthless items on an ABM deposit (two per cent).

EXHIBIT 4.1
Distribution Of Complaints Received by the OSFI and the Canadian Banking Ombudsmen Over a One-Year Period



EKOS Research Associates Inc.

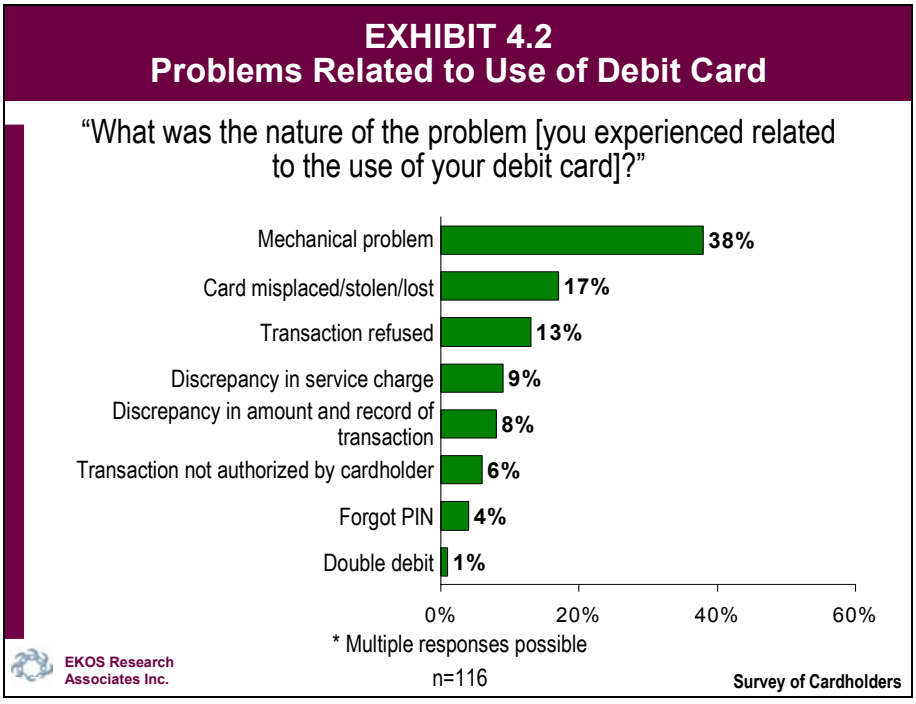
n=107

Review of Complaint Data

In terms of the amount of money involved in the complaints received from the OSFI and CBO, this information was available for only 27 of the 107 complaint files reviewed. The average amount of money involved in these disputes was $3,931, with a minimum value of $20 and a maximum value of $30,000.

a) *Cardholder Experiences with Debit Card Problems and the Complaint Process*

According to surveyed cardholders, 13 per cent had experienced problems related to the use of their debit card in the last year that led them to discuss the problem with a financial institution (higher among those who use their debit card more frequently). The most frequently mentioned problems were mechanical in nature (card did not work, system down, no transaction record, insufficient funds dispersed, etc.) (38 per cent). Related to this, another 13 per cent had their transaction refused by the financial institution (e.g., insufficient funds, did not accept card, invalid PIN, PIN entry error). A lost or stolen card was mentioned by 17 per cent. Nine and eight per cent of respondents respectively noted a discrepancy in service charges or a discrepancy between the amount withdrawn and the record of transaction. An unauthorized transaction was reported by six per cent. Four per cent indicated that in the last year they had forgotten their PIN and one per cent noted a double debit.



Cardholders were most likely to resolve their debit card problem with their financial institution branch (82 per cent). Another 10 per cent discussed the issue with the head

office and five per cent used the institution's service centre or 1-800 number (the latter was higher among youth). A minority (four per cent) went to an outside agency – the Ombudsman or consumer association. Four per cent did not discuss the problem with any financial institution or other agency.

When asked about the steps the cardholder went through to resolve the problem, the most frequently mentioned steps simply involved contacting the financial institution (49 per cent went to or phoned the institution, 13 per cent spoke with a teller, 11 per cent spoke to someone at the customer service or toll free line, three per cent spoke with a manager). Four per cent spoke to a retailer and two per cent filed a complaint with the financial institution. About four in ten (43 per cent) cardholders who had a problem received a new debit card.

The majority of cardholders (78 per cent) indicated that the problem they experienced had been resolved to their satisfaction. Of those who were not satisfied, the most frequently mentioned reason was that the problem continued (50 per cent). Other responses included: institution did not act on the complaint (22 per cent); still in the process of resolving the problem (19 per cent); and respondent did not agree with the service charge (19 per cent).

5 SUMMARY OF FINDINGS

The main findings of the evaluation are as follows:

a) *Adherence to the Canadian Code of Practice*

- There is room for improvement for all financial institutions that participated in the evaluation as no one financial institution fully adhered to all aspects of the Code.
- In their documentation, financial institutions generally adhere to those clauses of the Code that address practices related to issuing debit cards and PINs, with average documented rates of adherence of 81 per cent (Table 2.1). Lower average rates of documented adherence were observed for the information relating to dispute resolution (71 per cent -Table 4.1) and liability for loss (67 per cent -Table 3.1).
- During spot checks conducted to determine the degree to which the staff of financial institutions provided information (either verbally or in writing) to cardholders, card issuers demonstrated an observed adherence rate of 87 per cent for the provision of procedural information related to issuance of the debit card (Table 2.2). The observed average rate of adherence concerning the provision of information on general security issues was 69 per cent (Table 2.3), for liability for loss the observed rate of adherence was 59 per cent (Table 3.2), and for dispute resolution the observed rate of adherence was 41 per cent (Table 4.2).
- Cardholder agreements tend to be the primary means employed by financial institutions to communicate information outlined in the Code to the cardholder. Other literature (i.e., other than cardholder agreements) and verbal communication tend not to address most aspects of the Code. While this information may not be volunteered by client service representatives, it is nonetheless available, as demonstrated by consistently higher levels of adherence to the Code when researchers prompted staff for information beyond what was already offered.
- While cardholder agreements are an important means of communicating pertinent information to cardholders, a number of financial institutions do not consistently provide cardholders with a copy of the cardholder agreement (i.e., cardholder agreements were not received for 22 per cent of the card issuer spot checks), nor do they offer this information verbally when a cardholder opens an account.
- Cardholder agreements are often not in conformity with Code provisions with respect to cardholder liability for loss and in particular, that cardholders are not responsible for losses beyond their control.

b) *Cardholder Complaints*

- Survey findings suggest that roughly one-in-ten cardholders (13 per cent) experienced problems with the use of their debit card over the last year.
- More than three-quarters (78 per cent) of survey respondents who filed a complaint in the last year were satisfied with its resolution.
- The majority of complaints received by financial institutions appear to involve transaction errors or problems, while 17 per cent of complaints received involve unauthorised or fraudulent transactions.
- Of those transaction errors or problems that were resolved, it was more likely for the client to be reimbursed than to be held liable for the loss. For complaints involving unauthorised or fraudulent transactions, the allocation of responsibility tended to be shared between the client and financial institution.
- The higher proportion of complaints involving unauthorised or fraudulent transactions reported by other organizations (e.g., the OSFI and the Banking Ombudsman) relative to those received by financial institution call centres suggests that this type of complaint is more likely to be referred to the OSFI and/or the Canadian Banking Ombudsman.
- Financial institutions and consumer associations did not organize their complaint data in a uniform fashion with the result that it was difficult to summarize and analyze their data in this report.

c) *Consumer Awareness of Responsibility/Liability*

- Survey findings suggest that roughly seven in ten cardholders select appropriate PINs (i.e., that are not based on personal information such as name, address or phone number) and that 80 per cent of respondents understand that they would be liable for losses if they revealed their PIN to someone.
- Survey findings further suggest that only 21 per cent of respondents understand that they could be liable for losses if their PIN was based on a number found in another document while only 44 per cent of respondents understand that they could be liable for money taken from an overdraft or a line of credit if found responsible for the loss.

d) *Security of Point-of-Service Terminals*

- Most cardholders are moderately to very comfortable with the privacy and security of banking (i.e., withdrawal of money at ABMs/ATMs) and point-of-sale (POS) transactions. Nonetheless, two-thirds of surveyed cardholders expressed concerns over a lack of privacy

when entering their PIN at point-of-service terminals. Researchers conducting point-of-service spot checks indicated that for 14 per cent of spot checks, retail staff were able to view entry of the researchers' PIN, and for 35 per cent of spot checks, other customers were able to view entry of the researchers' PIN.

- Interviews with merchants reveal that roughly one-half of those who lease their PIN pads (n=16) are aware of the requirement that retailers install PIN pads such that they provide sufficient privacy to allow customers to enter their PIN with a minimum of risk of others observing entry of the PIN. Roughly one-half of merchants interviewed indicated that some form of staff training is provided to ensure the secure operation of their PIN pads. A small proportion (14 per cent) of merchants indicated that they have experienced difficulties in providing privacy.