MeRC

McMaster eBusiness Research Centre

MEASURING IDENTITY THEFT IN CANADA: 2008 CONSUMER SURVEY

By

Susan Sproule and Norm Archer

Sproule@mcmaster.ca
archer@mcmaster.ca

McMaster eBusiness Research Centre (MeRC)
DeGroote School of Business

MeRC Working Paper No. 23

July 2008

MEASURING IDENTITY THEFT IN CANADA: 2008 CONSUMER SURVEY

By

Susan Sproule and Norm Archer

MeRC Working Paper #23

July 2008

DeGroote School of Business

McMaster University

Hamilton, Ontario, L8S 4M4

Canada

sprouls@mcmaster.ca

archer@mcmaster.ca

TABLE OF CONTENTS

1.0 EXECUTIVE SUMMARY

This paper reports the results of a 2008 survey of Canadian consumers conducted by the McMaster eBusiness Research Centre (MeRC) on behalf of the Ontario Research Network on Electronic Commerce (ORNEC). The survey was designed to determine the nature and extent of identity theft and fraud in Canada. It also examines the concerns of Canadian consumers and their behaviour related to the prevention and detection of identity theft and fraud. The survey was conducted using an Internet panel, with 3017 valid responses.

This was the second of two consumer surveys conducted by MeRC for ORNEC. The first survey was conducted in late 2006 and collected information about a large number of historical cases of identity theft and fraud.[1] The survey described in this paper was conducted in early 2008 and focuses on cases that occurred in the most recent year.

According to the results of this survey, 6.5% of Canadian adults, or almost 1.7 million people, were the victim of some kind of identity fraud in the last year. These victims spent over 20 million hours and more than $150 million to resolve problems associated with these frauds.

More than half of these frauds involved nothing more than unauthorized purchases made with credit cards. Consumers rarely pay the costs of such frauds. If we eliminate credit card fraud from the incidence rate and costs quoted above, the number of victims is reduced to 700,000 but they still spend 12 million hours and more than $110 million dollars of their own money to resolve these other problems.

Most victims (57%) did not know how their personal information was accessed, but when they did know, the identity fraud was most often associated with a business transaction conducted either in person (25% of these cases) or online (15% of these cases). The proportion of online transaction fraud has increased from 5% of cases historically. Debit card skimming operations made up another 13% of the cases where the method of access was known. Recent US studies have found a significant increase in telephone scams and frauds, but our data does not reflect this increase.

While earlier studies have found that 25% of all cases of identity fraud were committed by someone known to the victim, this survey found that to be the case in only 7% of the total number of cases.

Very few of the cases of identity fraud were reported to the police (13%), credit reporting agencies (6%) or PhoneBusters - the RCMP/OPP fraud reporting agency (0.5%).

In addition to the victims of fraud reported above, another 2.7% of the sample indicated that their personal data had been accessed by unauthorized people as part of a data breach

[1] Results from this survey can be found in MeRC Working paper #21.

or fraud operation in the last year. This represents another 700,000 Canadian adults who are at risk for identity fraud.

One third of Canadian consumers report that their level of concern about identity fraud is higher than it was a year ago. The level of concern increases with age. Past victims of **credit card fraud** are less concerned than past victims of other kinds of identity frauds - and are even less concerned than those who have never been a victim. We believe that this is because credit card fraud detection and resolution processes are mature and sophisticated. As far as the consumer is concerned the problem is easily and quickly resolved at little to no personal cost. This is not the case for many other identity frauds. This result suggests that it is important to isolate credit card fraud and discuss it separately from other identity frauds.

Canadian consumers protect their personal information from physical theft in the following ways:

- 79% shred financial documents or other important documents all of the time or most of the time
- 59% use a locked mailbox all of the time or most of the time
- 57% keep sensitive information in a secure location, such as a locked box or drawer, all of the time or most of the time
- 50% have eliminated or reduced the number of identity documents that they carry with them
- 30% have either stopped receiving mailed account statements or reduced the number of mailed statements that they receive

Canadian consumers take the following measures to keep their personal information from prying eyes or unauthorized access:

- 92% never or rarely give information over the phone to people claiming to do surveys or offer promotional goods or services
- 88% make sure that no one is watching, all of the time or most of the time, when using an ABM or debit card machine
- 35% have reduced or stopped giving their credit card to waiters or gas station attendants

Safe online practices are also important to protect personal information, and Canadian consumers report the following practices:

- 75% use hard-to-break passwords all of the time or most of the time
- 59% use different passwords for different applications all of the time or most of the time
- While most consumers change their important passwords at least every 2-5 years, 30% report that they never change these passwords

Fully 20% of consumers report that they have eliminated or reduced the amount of shopping that they do online because of a concern about identity theft and fraud. Nine percent report that they have eliminated or reduced online banking activities because of

similar concerns. These results show that the threat of identity theft and fraud is having a significant and detrimental effect on e-commerce in general.

Frequent and careful monitoring of accounts is the best way to detect and minimize the effects of identity frauds. Eighty-five percent of respondents have online access to at least one of their bank accounts and 96% of these consumers check their account balances online. The majority of people do this every few days or better. Other detection practices reported in the survey include:

- 49% had never requested a copy of their credit report
- 77% had never checked land registry records

Forty-one percent of respondents reported that they had received an email from a bank or other company asking them to verify or update their account information. This describes an identity theft practice known as phishing. Of those that had received such an email, 2.7% report that they responded and 1.0% report that they do not know or were not sure if they had responded. This potential response rate of 3.7% is an improvement over a rate of 4.9% found in an earlier survey.

2.0 INTRODUCTION

2.1 The ORNEC Identity Theft Program

This report is the second report produced by the McMaster eBusiness Research Centre (MeRC) for the Ontario Research Network for Electronic Commerce (ORNEC) identity theft program. Funded by the Ontario Research and Development Challenge Fund, in partnership with the Universities of Ottawa, McMaster, Carleton and Queen's, ORNEC is the focal point and driving force for electronic commerce research in Ontario, Canada and internationally.

In 2005 ORNEC began its flagship research program on identity theft. There was little information on the problem of identity theft in Canada and no coordinated efforts within the academic community to examine the problem. It was believed that, if unchecked, the problems around identity theft and fraud could have a significant negative impact on e-commerce.

The ORNEC research program on identity theft was divided into four projects as follows:

- Defining and Measuring Identity Theft in Canada
- Legal and Policy Approaches to Identity Theft
- Management Approaches to Combating Identity Theft
- Technical Tools to Address the Identity Theft Problem

Private sector funding for ORNEC's identity theft research program was provided by the following companies:

- Bank of Montreal (BMO)
- Royal Bank of Canada (RBC)
- Canadian Imperial Bank of Commerce (CIBC)
- TD Canada Trust
- Bell Security Solutions

Other interested organizations that have attended workshops and provided advice are:

- Department of Justice, Canada
- Industry Canada
- The Ontario Ministry of Government Services
- Royal Canadian Mounted Police (RCMP)
- Ontario Provincial Police (OPP)

2.2 Defining Identity Theft and Identity Fraud

Each of the above mentioned projects has a number of different research components. The first of these projects, the 'Defining and Measuring' project, is the focus of this paper. This project has the following major components:

1. Develop commonly accepted terminology
2. Conduct national consumer survey
3. Measure identity theft in organizations

4. Describe national impact and develop an index to track this impact over time

This section describes our efforts to address the first of these project components.

Identity theft has become a major area of public concern throughout the world; however there is no consensus on what the term 'identity theft' includes or how it is related to other crimes. Our initial workshops for the ORNEC program brought together researchers and subject matter experts from many different backgrounds. We found little agreement on how the terms identity theft and identity fraud are used across these diverse domains. Following an approach based on the practice of terminology, we developed standardized terms for use within the ORNEC program. A detailed discussion of this approach can be found in Sproule and Archer (Sproule and Archer 2007).

Our researchers and subject matter experts agreed to use the term **identity theft (IDT)** to describe the unauthorized collection, possession, transfer, replication or other manipulation of another person's personal information for the purpose of committing fraud or other crimes that involve the use of a false identity.

IDT includes various activities associated with the unauthorized collection of personal information (e.g. hacking, phishing, skimming, insider theft, etc.) as well as activities associated with the development of a false identity (e.g. counterfeiting, document breeding, ID trafficking, etc.).[2]

Identity fraud (IDF) is a class of crimes that may be committed with a false identity. Specifically, it is the gaining of money, goods, services, other benefits, or the avoidance of obligations, through the use of a false identity. We exclude major crimes such as drug smuggling or terrorism, where the use of a false identity is peripheral to the crime. Examples of identity fraud are credit card fraud, bank fraud, land title fraud and employment fraud.

Using these definitions, we can see that IDT and IDF describe different problems. To address IDT we need to look at , for example, problems associated with personal and agency guardianship of personal information, and we need new laws in order for law enforcement to act when they find someone with false identification documents or unauthorized copies of other people's personal information. To address IDF, for example, we need to look at stronger authentication processes that will recognize and defend against someone using a false identity.

2.3 Consumer Survey 2006

The second component of the "Defining and Measuring Identity Theft" project was to conduct a consumer survey to determine the nature and extent of the IDT and IDF problem in Canada. Our first survey was conducted in late November and early December 2006. It was conducted by Open Venue, a professional market research firm, using an Internet panel. An analysis of the results of this survey can be found in MeRC

[2] The Glossary in Appendix D provides definitions for terms that may be unfamiliar to the reader.

Working Paper #21 – Measuring Identity Theft in Canada: 2006 Consumer Survey, available from http://www.merc-mcmaster.ca/ (Sproule and Archer 2008).

In this section and the next, we highlight some of the differences between the 2006 survey and our most recent 2008 survey. Table 1 summarizes these differences. Note that while we refer to each survey by the year of its completion, there were only 14 ½ months between the surveys.

The first section of the 2006 survey presented a number of scenarios and asked respondents whether they considered each scenario to be a case of identity theft or fraud.

The second and main section of the 2006 ORNEC survey gathered historic information about the characteristics of identity theft and fraud in Canada. The cases described could have happened at any time in the past. They also could have happened to the respondent or to someone in the respondent's immediate family. We were therefore able to collect information about a large number of cases (1710).

In the 2006 survey, one of the categories of identity theft and fraud that was identified in the initial incidence question was 'identity theft only'. This referred to cases where the victim knows that his or her information has been accessed or taken by an unauthorized person, but is not aware of any frauds that have occurred as a result. These victims were also asked general questions about the characteristics of the theft or fraud, including questions about the method of detection, who was responsible, how information was accessed or taken, and costs.

The final section of the 2006 survey asked about the acceptability of various measures that individuals, governments or financial institutions might take to combat identity theft and fraud.

In 2006, the survey was developed in English only. As a result it was not administered to residents of Quebec and results are representative of the target population in English Canada only (excluding the province of Quebec).

2.4 Consumer Survey 2008

The 2008 survey continues to measure the nature and impact of identity fraud and identity theft in Canada and starts to address the fourth component of the "Defining and Measuring Identity Theft" project - developing an index to track the impact of identity theft and identity fraud over time.

To this end, the 2008 ORNEC survey gathered detailed information about the characteristics of identity theft and fraud cases that had happened to the respondent only (as opposed to family members), and in the last 12 months. While the number of cases is much smaller (212), we expect that the respondent's recall of the details should be more accurate.

We did not include the first section from the 2006 survey, where we asked respondents to identify scenarios that they considered to be identity theft. However, we wanted to provide similar examples to help clarify the types of identity fraud and identity theft that are included in our definitions and to establish some continuity between the two surveys. The 2008 questions to determine incidence rates[3] (Q7, Q12, Q16, Q19 and Q36) therefore included examples of each type of identity fraud and identity theft drawn from the scenarios provided in the 2006 survey.

In the 2008 survey we wanted to explore the extent and nature of data breaches that were known to the consumer. Rather than including "identity theft only" in the initial identity theft and fraud categories, we asked respondents who had not been victims of fraud, whether they were aware that their personal information had been accessed as part of a security breach or fraud operation. This would eliminate cases where information had potentially been compromised as a result of a stolen or lost wallet and other isolated or opportunistic access problems. If respondents reported that they had been victims of such a data breach, they were asked a set of detailed questions about the breach. They were not asked the general questions related to the characteristics of frauds.

In the final section, the 2008 survey asked a series of questions about behaviours that are linked to the prevention and detection of identity theft and fraud. We also included additional questions that would let us analyze the results in terms of the victim's financial and online exposure.

The 2008 survey was translated into French and was administered to panel subjects in Quebec. The results are therefore representative of the target population in all of the provinces of Canada.

Table 1 – Differences in detailed questions about the characteristics of the ID fraud between the two ORNEC consumer surveys

	2006 Survey	**2008 Survey**
Victim was…	Respondent or member of respondent's immediate family	Respondent
Geographic coverage	Provinces excluding Quebec	All provinces
Recency of fraud incident	Ever	Last 12 months
Includes cases of ID theft with no fraud to date	Yes	No

2.5 Other Surveys

The most comprehensive series of consumer surveys on identity theft and fraud have been conducted in the U.S. by the Federal Trade Commission (FTC) in 2003 (FTC 2003) and Javelin Strategy and Research in 2004, 2005, 2006, and 2007 (Javelin 2005; Javelin 2006; Javelin 2007; Javelin 2008). We provide comparisons to these surveys, where possible.

[3] Appendix A lists the questions used in the 2008 survey

In a 2006 Ipsos Reid survey, 29% of Canadians said that they "hear a lot about identity theft, but don't know what it means" (Ipsos-Reid 2006). In the first part of our 2006 survey, we found that our respondents did not have a common understanding of what constitutes identity theft and fraud (Sproule and Archer 2008). There are many other surveys, including Canadian surveys, which have investigated identity theft; however these surveys do not generally provide a sufficiently precise definition of identity theft and fraud. It is therefore difficult to know what these other surveys were measuring.

2.6 Classifications of Identity Fraud

The original 2003 FTC survey provided the categories that we use to classify different types of identity fraud. **Credit card fraud** describes frauds where someone makes purchases or otherwise puts charges on an existing credit card account without the cardholder's permission.

Existing account fraud occurs when someone gains access to an existing account, other than a credit card account, and runs up charges or takes money out of the account without the account-holder's permission. These accounts can include bank accounts, utility accounts, loans, line-of-credit accounts or online accounts such as eBay or PayPal. It should be noted that the FTC survey and our survey include debit card fraud in this category. Since 2005, Javelin surveys have classified debit card fraud with credit card fraud (Javelin 2006).

New accounts fraud occurs when someone uses another person's personal information to obtain new credit cards, loans or other accounts (i.e. utility or online accounts) and runs up debts. **Other frauds** are when a fraudster uses personal information to impersonate someone else and obtain benefits such as employment, housing, or health services or avoid criminal prosecution or obligations such as taxes. While we have separate measures for new accounts fraud and other frauds, they are often combined in order to make comparisons to the other surveys.

Some of the characteristics of frauds examined in Section 5 of this report differ between these types of fraud. Whether simple credit card fraud belongs in a study of identity fraud is a matter of debate within the research community (Anderson 2005; Gordon, Rebovich et al. 2007). Where our data shows a significant difference in the characteristics of fraud between these types of fraud, Appendix C contains detailed Figures that show these differences.

3.0 METHODOLOGY

The 2008 ORNEC survey was again conducted by OpenVenue, a professional marketing research firm. OpenVenue uses an online panel recruited through the Sympatico/MSN portal. Respondents were required to be at least 18 years of age, reside in one of the ten provinces in Canada, and have at least one bank account and one credit card.

Appendix A contains a copy of the survey questions.

The survey sample was targeted to the Canadian population on the basis of age (5 categories), gender (50/50) and region (West, Ontario, Quebec, Atlantic). The survey had a soft launch on February 6, 2008 and completed on February 13, 2008 with 3017 responses. The median time for completion of the survey was 7 minutes. Quotas for the demographic variables were met well within the 5-10% range specified in the OpenVenue contract.

Of the 3017 respondents, 693 indicated that they had been a victim of some kind of identity fraud in the past. Of these, 212 had been a victim in the last 12 months. These respondents were asked detailed questions related to the type of fraud that they had experienced.

For questions answered by all 3017 respondents, the maximum margin of sampling error is +/- 1.78% at the 95% confidence level. For questions answered by the 212 respondents who have been victims of identity fraud in the last 12 months, the maximum margin of sampling error is +/- 6.73% at the 95% confidence level. For questions answered by only a proportion of the victims, the sampling error varies and is greater than +/-6.73% at the 95% confidence level.

Another 200 people indicated that their personal information had been involved in a data breach of some sort, including 80 within the last year. These 80 respondents were asked detailed questions about the breach. For these questions the maximum margin of sampling error is +/-10.96% at the 95% confidence level.

3.1 Demographic Composition of the Sample

Table 2 shows the actual demographic composition of the sample and estimates of the population from the Canadian census. The differences introduce a form of non-response error. Under-represented groups include males, residents of Alberta and Ontario, the youngest and oldest age groups and the aged 45-54 group. See Table 3.

Table 2 - Demographic composition of the sample

Demographic Characteristic and Category		Canadian Census (%)[4]	2008 ORNEC Survey (%)	Diff from Census (%)
Gender				
	Male ***	49.1	46.7	-2.4
	Female ***	50.9	53.3	2.4
Residence				
	Newfoundland and Labrador ***	1.6	2.3	0.7
	Prince Edward Island	0.4	0.6	0.2
	Nova Scotia ***	2.9	3.8	0.9
	New Brunswick	2.3	2.7	0.4

[4] Residence data shown is the 2007 population estimates from the 2001 Canadian Census from: http://www.statcan.ca/Daily/English/070329/d070329b.htm Age and gender data is 2007, from: http://www40.statcan.ca/l01/cst01/demo10a.htm

	Quebec ***	23.5	27	3.5
	Ontario ***	38.9	35.6	-3.3
	Manitoba	3.6	3.6	0.0
	Saskatchewan	3.0	3.3	0.3
	Alberta ***	10.5	8.4	-2.1
	British Columbia	13.3	12.7	-0.6
Age				
	18-24 ***	12.3	10.6	-1.7
	25-34 ***	17.6	22.8	5.2
	35-44***	20.7	23.4	2.7
	45-54 ***	19.3	16.9	-2.4
	55-64 ***	13.6	18.5	4.9
	65 or older ***	16.6	7.8	-8.8

*** Differences in proportions are significant at p=.01

Table 3 – Over and under-represented demographic groups

Over-represented:	Under-represented:
Females	Males
Quebec Nova Scotia Labrador & Newfoundland	Ontario Alberta
Ages 25-44 Ages 55-64	Age 65 or older Ages 45-54 Ages 18-24

3.2 Weighting and Post-Stratification

Weights were created to eliminate the bias that is introduced by these over and under-represented groups. We used Statistics Canada's 2005 Annual Demographic Report to create the weights. This report uses 2001 census data with population estimates to 2005. Appendix B contains the full table of weights for the three demographic variables: age, gender and province. The results reported in the following sections use weighted data unless otherwise noted.[5]

3.3 Financial and Online Profile of Respondents

Respondents reported a median of two bank accounts. The distribution is shown in Figure 1. On-line access is very prevalent, with 85% percent of respondents reporting that they had on-line access for at least one of these accounts. Of those with on-line access, 96% report that they check account balances online and 94% use online access to conduct transactions such as paying bills and transferring funds.

[5] Note that when the results are weighted to correct for non-response bias, the number of cases reported in the analysis may differ from the absolute number of 212.

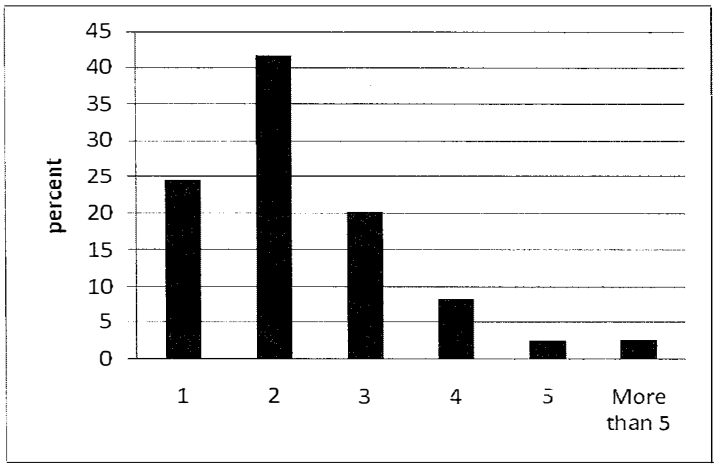


Figure 1 - Number of bank accounts

Respondents also reported a median of two credit cards. The distribution is shown in Figure 2.

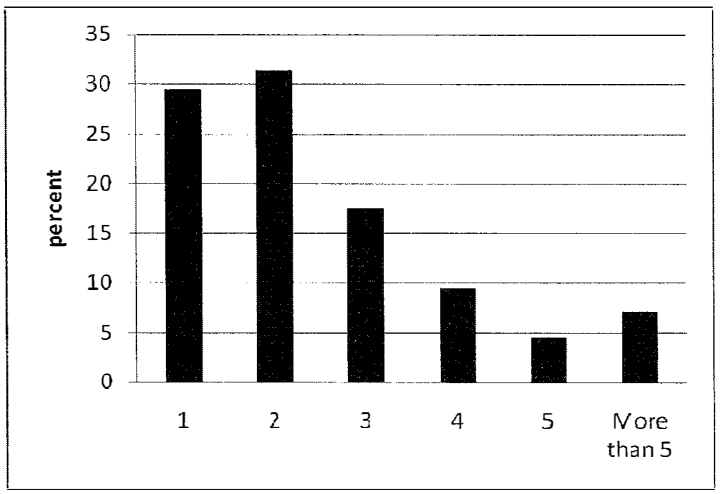


Figure 2 - Number of credit cards

The median number of email accounts (both personal and business) was also two. See Figure 3 for the distribution.

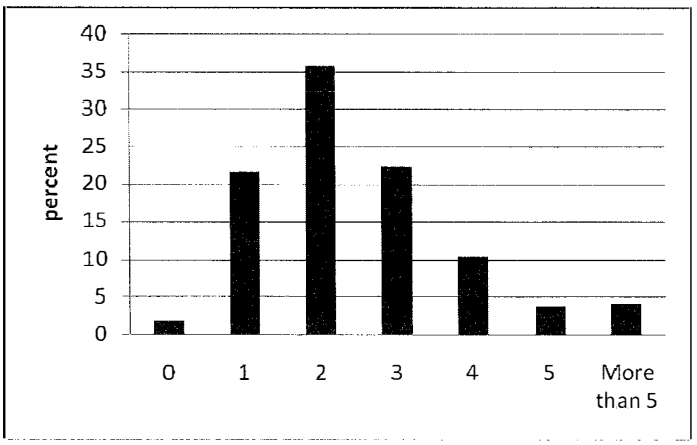


Figure 3 - Number of email accounts

We asked about other online accounts, in addition to email accounts and bank accounts. Just under half of the sample (46%) reported that they had no additional online accounts. The most frequent other online account was PayPal at 40% of the sample, followed by eBay at 23% of the sample. In addition, 3% of the sample reported having other online accounts at retailers such as Amazon and Chapters, or accounts for investments, bill-paying, gambling, etc.

Figure 4 shows the frequency of responses for the question "How often do you shop online". Seventeen percent had never shopped online and only 6% shop online often. The great majority shop online occasionally (39%) or seldom (37%).

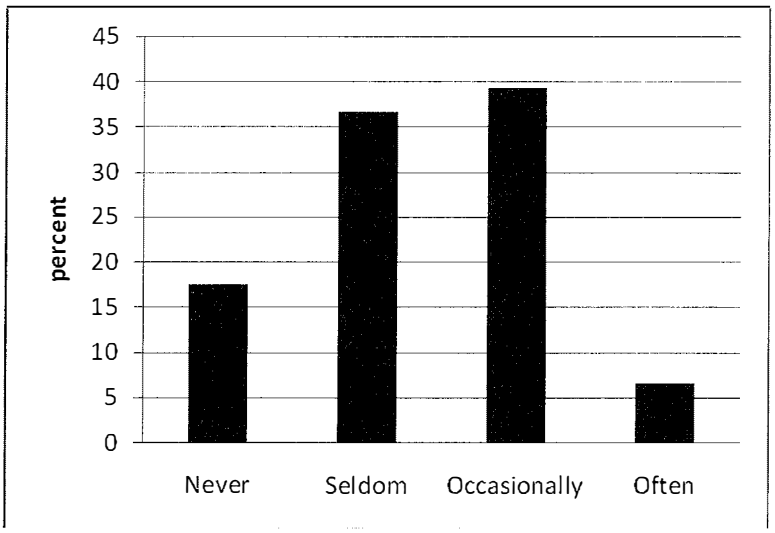


Figure 4 - How often do you shop online?

4.0 INCIDENCE RATES

23% of the sample reported that they had been a victim of some kind of identity fraud in the past[6], although almost 14% had experienced nothing more serious than the unauthorized use of a credit card.

In the past year, 6.5% of the sample reported that they had been victims of some sort of identity fraud.[7] Of these, more than half (3.6%) had experienced nothing more serious than the unauthorized use of a credit card.

In the results of our 2006 survey we were only able to establish a range for the incidence rate in the previous 12 months, since we did not know if the case being described had happened to the respondent or to someone in the respondent's family. Results from the 2008 survey put the 12 month overall incidence rate in the middle of the range that was

[6] At a 95% confidence interval (i.e. nineteen times out of twenty) the actual incidence rate will lie between 21.6% and 24.6%.

[7] At a 95% confidence interval (i.e. nineteen times out of twenty) the actual incidence rate will lie between 5.6% and 7.4%.

established in our 2006 survey. The incidence of credit card fraud is higher than the range established in the 2006 survey and the incidence of new accounts and other fraud is lower. This comparison is shown in Table 4.

Table 4 – Comparison of incidence rates from the 2006 and 2008 ORNEC surveys

IDF Category	2006 survey	2008 survey	
	percent	frequency	percent
Credit card fraud	2.0 - 3.2%	110	3.7%
Existing account fraud	1.2 - 2.8%	75	2.5%
New accounts and other fraud	0.8 - 3.1%	9	0.3%
Total	4.0 - 9.1%	194	6.5%
Sample size	3539	3003[a]	

[a] Weighted value. Un-weighted sample size was 3017

Our 2008 results are shown against historical data from the US studies in Table 5. Our overall incidence rates are higher than those reported in US telephone surveys. We find higher rates of credit card fraud and existing accounts fraud, but a lower rate of new accounts and other frauds.

Other researchers have found a similar difference between random digit dialing (RDD) telephone surveys and online surveys. In their 2006 online survey, Gartner reported incidence rates that were 1.51 times higher than those found in these same US RDD telephone surveys (Litan 2007) This means that Gartner found an overall incidence rate of 5.6 which is still at the low end of our 95% confidence level.

A second potential reason for our higher rates may be the way the questions were structured. For each type of identity fraud, we provided a number of examples of situations that would be classified in that category. These examples may have prompted respondents to include cases that would not have been salient without the examples.

Table 5 – Comparison of incidence rates to US surveys

IDF Category	% of the population who were a victim of identity frauds in the previous 12 months					
	FTC	Javelin				ORNEC
	2003	2004	2005	2006	2007	2008
Credit card fraud	2.4	n/a			n/a	3.6
Existing accounts fraud	0.7	n/a	2.5	3.3	n/a	2.5
New accounts and other fraud	1.5	n/a	1.5	1.1	n/a	0.3
Total	4.7	4.3	4.0	3.7	3.6	6.5
Sample size	4057	5004	5003	5006	5075	3017

5.0 COSTS

We collected information about three kinds of measurable costs: fraud amount, victim's hours spent resolving problems resulting from the fraud, and victim's out-of-pocket costs.

Fraud amount is the amount that the perpetrator obtained, to the best of the victim's knowledge. Victims were instructed to include the value of merchandise, loans, cash, services and anything else the perpetrator may have obtained. It should be noted that victims are often not held responsible for these costs. In these cases, they are generally using incomplete information to estimate the value of goods and money received by the fraudster. They are also often not aware if losses were recovered.

The victims' personal costs are measured in both the time to resolve problems arising from the identity fraud and their out-of-pocket costs. For out-of-pocket costs, victims were asked to include costs for postage, copying, legal fees, notarized documents, and payment of any fraudulent debts.

Table 6 shows the average costs when we include all identity frauds and for the subset of cases of more serious categories of frauds when we exclude simple credit card frauds

Table 6 – Average costs of identity fraud incidents

	Fraud amount	Victim hours	Out-of-Pocket Costs
ALL FRAUDS			
Mean	$1103	12.8	$92
Median range	$100-$499	2-9	$0
Median (interpolated)	$334	2.7	$0
SERIOUS FRAUDS (excluding cc fraud)			
Mean	$1210	16.9	$151
Median range	$100-$499	2-9	$0
Median (interpolated)	$422	4.1	$0

All of the costs reported in 2008 are much lower than the costs reported in the 2006 survey. Using the historical data from 2008, mean fraud amounts were $3209, with a median (interpolated) of $595. Mean victim hours were 27, with a median (interpolated) of 8 hours. Mean out-of-pocket costs were $436, with a median (interpolated) of $4.

These differences are reduced, but still evident, if we take only the 2008 cases where the individual was the victim and the fraud was discovered in the past 12 months. Using these cases only, the mean reported fraud amount in the 2008 survey was $2947, the mean victim hours were 18 and the mean out of-pocket cost was $165. There was no difference in how these questions were worded.

The FTC and Javelin surveys report even higher costs in the U.S. Fraud amounts are typically reported to be between $4000 and $6000, victim hours between 25 and 40 and out-of pocket costs between $400 and $700. Our wording is very similar to the wording in the original FTC survey.

5.1 Costs of Identity Fraud in Canada

We can use the incidence figures from Table 4 and fraud costs from Table 6 to arrive at a national estimate of identity fraud costs. Working from Statistics Canada figures for 2007, we estimated the Canadian population over 18 years of age, at 26,044,280.[8] Using an overall incidence rate of 6.5% we arrive at the results shown in Table 7.

Table 7 – Annual costs of identity fraud

Number of victims (last 12 months)	Percent of population	6.5%
	Projected number of victims in Canada	1,692,878
Fraud amount	Mean amount per victim	$1103
	Total	$1,867,244,434
Victim's hours to resolve	Mean hours per victim	12.8
	Total hours	21,668,838
Out-of-pocket costs	Mean cost per victim	$92
	Total	$155.744,776

With almost 1.7 million victims, the amount that fraudsters gained in the past year is close to $2 billion. Victims spent more than 21 million hours and $150 million to resolve problems associated with identity fraud.

If we do not include simple credit card fraud, the costs appear as shown in Table 8.

Table 8 – Annual costs of identity fraud excluding credit card fraud

Number of victims (last 12 months)	Percent of population	2.8%
	Projected number of victims in Canada	729,239
Fraud amount	Mean amount per victim	$1210
	Total	$882,379,190
Victim's hours to resolve	Mean hours per victim	16.9
	Total hours	12,324,139
Out-of-pocket costs	Mean cost per victim	$151
	Total	$110,115,089

As discussed previously, the fraud amount reported in a consumer survey will not reflect the true costs of identity fraud. If a business or financial institution is the victim of the fraud, only they know its true costs and they are reluctant to share this information. Other researchers have also estimated costs associated with preventing, detecting and investigating and prosecuting identity frauds, These business costs are estimated to be as least as much as the actual fraud amounts (Cuganesan and Lacey 2003).

6.0 CHARACTERISTICS OF IDENTITY FRAUD

The first four sub-sections of this section of the report provide detailed information about each of the four classifications of fraud that we investigated. Refer to Appendix A for detailed questions as numbered below.

[8]From: http://www40.statcan.ca/l01/cst01/demo10a.htm

6.1 Credit card fraud

- While respondents had an average of more than 2 credit cards (Q3), the vast majority (94%) of reported cases of credit card fraud involved just one credit card. (Q9)
- In 7.5% of the cases, there was an attempt to take over the account. (Q10)
- Bank-issued credit cards were involved in 98% of the cases. Store-issued credit cards were only involved in 4% of the cases. The total is more than 100% because some reported cases involved both bank and store-issued cards. (Q11)

6.2 Existing account fraud

- Over 75% of the cases involved a bank account (chequing or savings). Online accounts were the next most common target at 9% for PayPal accounts and 8% for eBay accounts. Line of credit accounts, conventional telephone accounts and wireless telephone accounts were involved in less than 5% of the cases and utility accounts in less than 1%. There were no cases of frauds involving existing loans or mortgages. (Q15)
- In 14% of the cases of existing accounts fraud, the perpetrator tried to take over the account by changing the associated address or other account details (Q14).

6.3 New account fraud

- Only six cases of new accounts fraud were reported, representing 0.2% of the sample. These six cases involved eight new accounts. Three cases involved bank-issued credit cards. There was one case each of a store-issued credit card, a chequing account, a wireless telephone account, an eBay account and a PayPal account.

6.4 Other frauds

- Five cases of other fraud were reported, representing less than 0.2% of the sample. These included an employment fraud, a government benefits fraud (other than health services), an apartment lease fraud, online harassment, and a case of "impersonation to obtain money".

The remaining sections report the results of general characteristics applicable to all of these types of fraud. Where possible, we compare the results to the 2006 survey to show how these recent cases differ from the previous study.

For each of these characteristics, we also provide a comparison between the 120 cases that involve simple credit card fraud and the 92 cases involving more serious types of identity fraud.

6.5 Method of Detection

Victims may discover that they have been a victim of identity fraud in a number of different ways. Overall, the most common method of detection was notification from the victim's bank (29% of cases), closely followed by monitoring accounts online (27%), notification from the credit card company (23%) and discovery on an account statement

received in the mail (23%). The remaining methods of detection were relevant in less than 5% (i.e. 10) of the cases. See Figure 5.

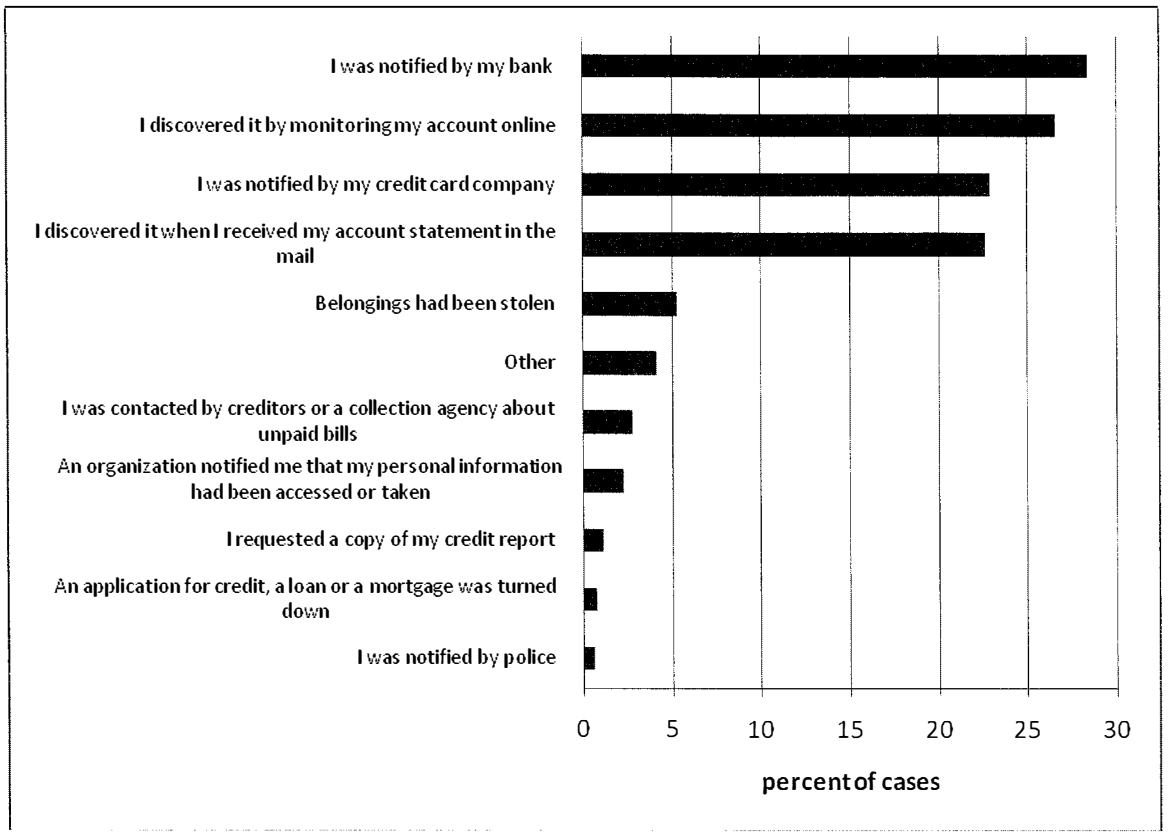


Figure 5 - Method of detection

Appendix C, Figure 1 contains a graph that details the differences in method of detection according to the type of identity fraud.

In simple credit card fraud, the most common methods of detection were notification from the credit card company (34%) and monitoring of accounts (30% through mailed account statements and 28% through online monitoring).

For existing accounts frauds, the most common method of detection was notification from the bank (51%), followed by monitoring of accounts (12% through mailed statements and 25% through online monitoring). Since there is often also a credit card fraud involved, notification by the credit card companies ranked fourth at 9% of cases. If we look only at cases where there was new account or other frauds, 26% discovered it through online monitoring and 22% were notified by their bank. Another 22% of victims found out after being contacted by a creditor or collection agency.

While the question responses were changed slightly, these results are fairly consistent with the results found in our 2006 survey. One notable difference is that in our 2008

results, discovery as a result of stolen belongings represented only 5% of the total. In the 2006 survey, historically, stolen belongings represented 13% of cases.[9]

6.6 Time to Detection

In more than half of the cases, the theft of information was discovered in less than a week. See Figure 6. Historically, our 2006 survey found that this was the case in only 30% of the cases and 37% of cases in the last year with IDF victims only. It would seem that detection is happening earlier in more recent cases.

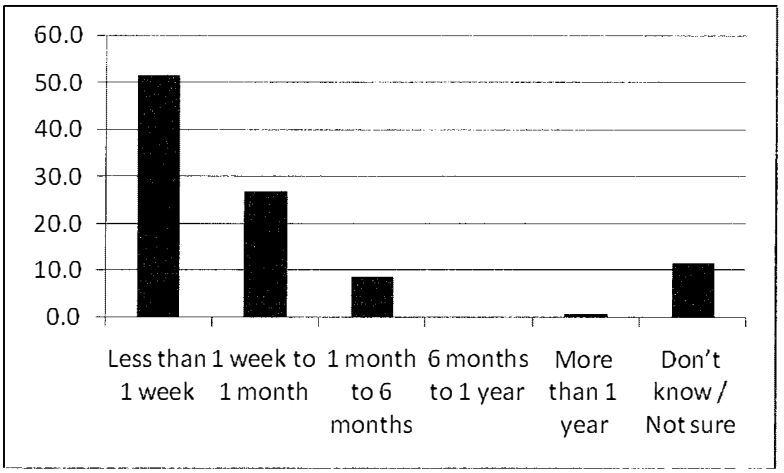


Figure 6 - Time to detection

Other studies have shown that early discovery of the theft can reduce losses associated with identity frauds (Javelin 2007). Our results show that there is a significant relationship between the time to detection and the victim's hours and out-of-pocket costs, but not to the fraud amount.

6.7 Awareness of How Information Was Obtained

In less than half the cases of identity fraud (43%), victims know, or think they know, how their information was obtained. This result is consistent with the Javelin surveys from 2005 and 2006 that reported values of 47% and 42% (Javelin 2006; Javelin 2007). However, the 2006 Gartner online survey found that 78% of victims knew how their personal information was obtained (Litan 2007).

Our results do not show a significant difference in awareness between victims of credit card frauds and victims of more serious frauds.

In the 2006 survey, we included a "maybe" response to this question. Our results for yes, no and maybe were 42%, 43% and 15% respectively. For the 2008 survey, we re-worded the question to include "or think you know" with the yes responses. We expected that the Yes responses from the 2008 survey (43%) would correspond with the yes and maybe

[9] We suspected the inclusion of IDT only victims in 2006 (where no frauds had yet occurred) might be responsible for part of this difference. From the 2006 data, if we take only the cases discovered in the previous 12 months and remove cases where there was IDT only and no fraud, the percent of stolen belongings is reduced to 11% - still more than twice the proportion found in 2008.

responses from the 2006 survey (42% + 15% = 57%). This is not the case. If we look at cases from the 2006 survey that were discovered in the last year and include IDF victims only, the combined "yes and maybe" responses represent 51% of the total. This would seem to indicate that victims are less likely to know how their information was obtained in more recent cases of identity fraud.

6.8 How the Information Was Obtained

When the method of access was known, business transactions, both in-person (25%) and online (15%), were the most frequent response to the question of how victims believed that their information was accessed or taken. The next most frequent response was debit card compromise (13%). The remaining responses were mentioned in less than 10% of cases. See Figure 7.

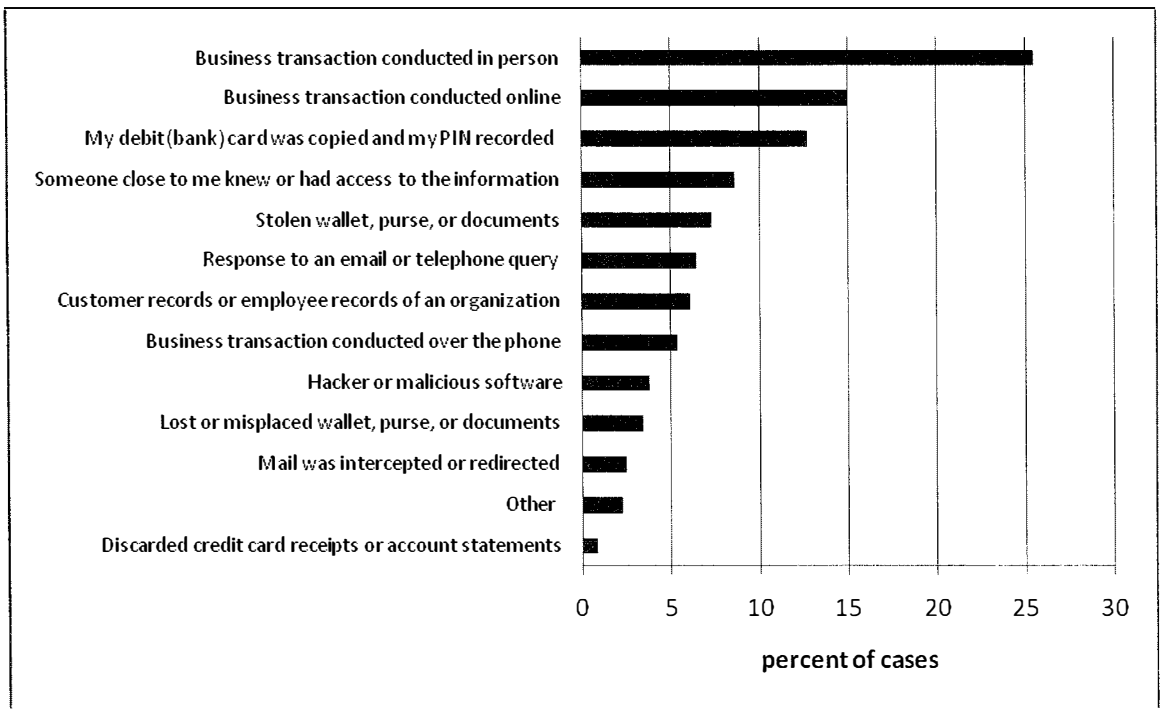


Figure 7 - How do you think the information was accessed or taken?

There are differences in how the information was accessed according to whether the victim experienced simple credit card fraud or more serious frauds. For simple credit card fraud, the most frequent responses were in-person business transactions (29%), online business transactions (20%), stolen wallets or purses (10%) and someone close to the victim (10%). Over 40% of existing accounts frauds involved debit card compromise and 20% occurred during an in-person business transaction. The cases of new accounts and other frauds had varying methods of access including two cases of mail interception or misdirection and one case each of phishing, discarded statements or receipts, lost wallet and in-person business transactions. These differences are detailed in Appendix C, Figure 2.

This survey question was changed in response to the 2006 survey results, so not all of the responses can be compared. For example, in 2006 we did not have a response for compromised debit cards, but 6% of our victims described this method in comments associated with an "other" response. For the 2008 survey we included a specific response for debit card fraud and it was chosen by 13% of our victims. In 2006, 21% of our victims said that their information was "taken from the home". We felt that this category was too general and could include theft as well as access by people close to the victim. We eliminated this response in the 2008 survey and added a response where the information was "known or accessed by someone close to me". This new response was chosen by 9% of victims.

When we compare the overall results to the historical data collected in the 2006 survey, the frequency of access through in-person business transactions has increased from 20% to 25% and access through online transactions has increased substantially from 5% to 15%. Access by stolen wallets or purses has dropped from 16% to 6%. It is interesting to note that the 2007 Javelin survey found that access through mail and telephone transactions grew from 3% to 40% between 2006 and 2007 (Javelin 2008). Telephone transactions were cited as the means of access for only 4% of our victims who knew how their information had been accessed.

6.9 Identity of the Perpetrator

Only 17% of victims know something about the identity of the person who accessed or obtained their personal information. This is much lower than the result in our 2006 survey, where historically 35% of victims reported that they knew something about the perpetrator's identity. There was no change in the question. If we take only the cases within the previous 12 months (and do not include ID theft only victims) the proportion in 2006 was 27%. This may be related to the increase in online frauds reported in the previous section.

Our 2006 survey found that, historically, victims of more serious frauds were more likely to know something about the identity of the perpetrator. The 2008 survey shows the same trend; however with the small number of cases, the difference cannot be determined to be statistically significant.

The victim knows something about the perpetrator in 17% of the cases; however this known perpetrator is still a complete stranger to the victim in 33% of these cases. An employee of an organization that the victim did business with was the perpetrator in 27% of the cases. We can classify these two categories of known perpetrators as "stranger fraud". In the remaining 40% of the cases, the perpetrator was known to the victim. We call this "friendly fraud". See Figure 8 for the remaining categories.

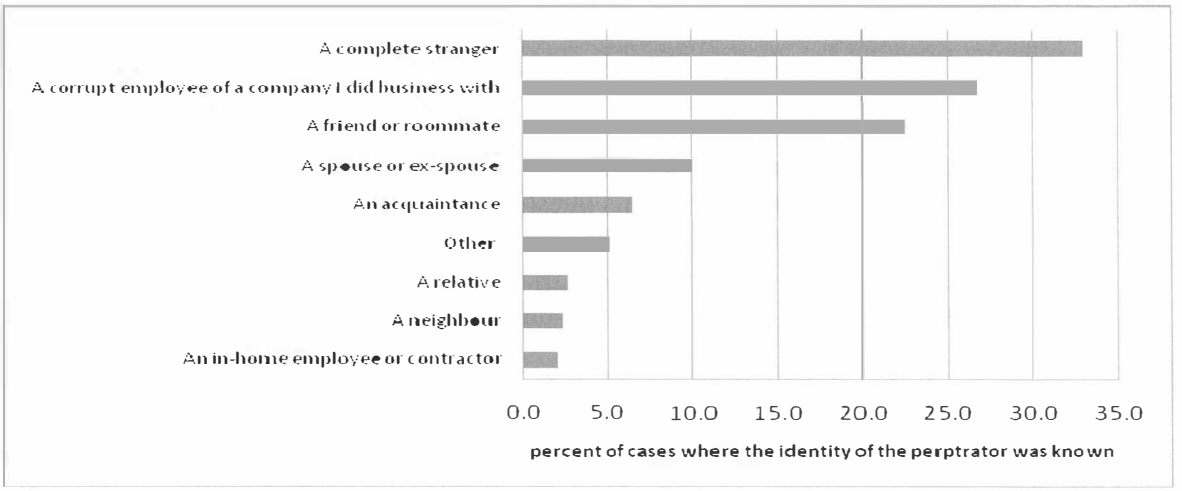


Figure 8 - Which of the following best describes the person who took the information?

There is not sufficient evidence to show a difference in awareness of who accessed the information or the identity of the person who accessed the information among the different types of identity fraud.

Figure 9 shows the time to detection according to whether the identity thief was known to the victim or a stranger. Identity frauds conducted by perpetrators who are known to the victim take longer to detect.

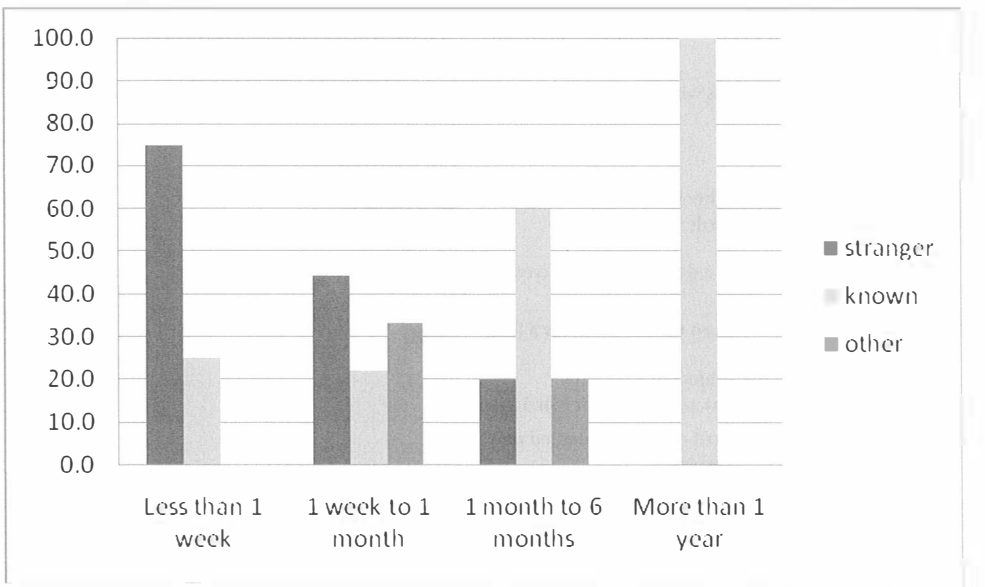


Figure 9 - Identity of perpetrator (known/stranger) and time to detection

In the 2006 survey, we found that something was known about the perpetrator in 35% of the cases and, within these cases, 66% of the frauds were committed by someone known to the victim. As a result, we concluded that, historically, 25% of all cases of identity fraud were committed by someone known to the victim (also described as "friendly fraud").

Our 2008 survey data indicates that only 7% of the total frauds committed in the last 12 months were friendly fraud. There are a few possible reasons for this difference.

- An increase in online fraud, where identities of perpetrators are not known

- Time to detection is longer for friendly fraud, so imposing a 12 month time-frame on the requirement to answer this question may mean that some of these friendly frauds are not captured in our 2008 survey.
- People may be less willing to report friendly fraud when they are the victim than when someone else in their family is the victim.

Our 2006 survey found that all three types of costs were greater with friendly fraud. In 2008, however, we do not have sufficient evidence to show a significant difference.

6.10 Other Costs

In addition to the costs outlined in Section 4., victims often suffer additional non-monetary and other costs. In 22% of the cases, victims reported having banking problems and 16% reported having problems with credit card accounts. Respondents who answered 'Other" generally specified minor problems associated with delays in getting new cards or accounts and time spent changing account numbers for pre-authorized billing or records of other suppliers. Two respondents noted that they suffered stress or anxiety about their personal security. See Figure 10.

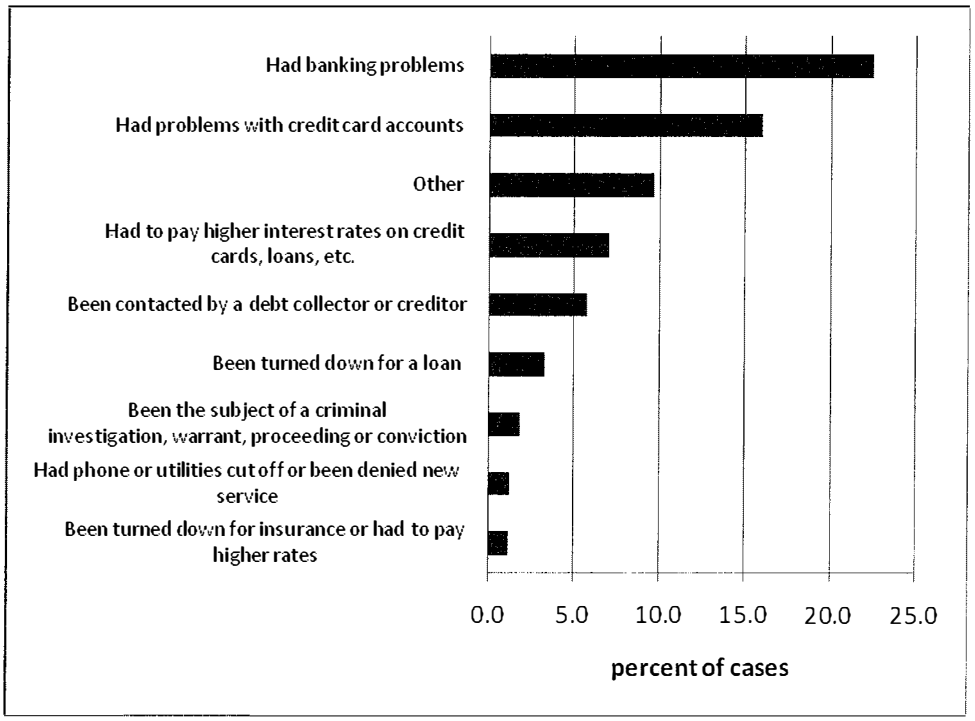


Figure 10 - Other costs

This was a multiple response question, so a chi-square test for significance is not available. However, the responses for different types of ID fraud are shown in Appendix C, Figure 3. Victims of credit card fraud were limited to other costs associated with credit card accounts. Victims of existing accounts fraud experienced banking problems and other problems associated with losing access to accounts and changing accounts and billing arrangements. Our nine victims of new accounts and other frauds reported problems with credit cards and banks, as well as debt collectors and creditors, problems

getting loans, paying higher interest rates, having utilities or phones cut off and being the subject of criminal investigation

6.11 Reporting

Respondents most frequently reported frauds to credit card companies (54% of cases) and banks (48% of cases). In only 13% of the cases was the fraud reported to police, and in only 6% of the cases was the fraud reported to the credit reporting agencies such as TransUnion and Equifax. Responses under the "Other" category included EBay (4 cases), PayPal (4 cases) and retailers (4 cases). Only 1 case was reported to PhoneBusters, the anti-fraud reporting centre operated by the Ontario Provincial Police and the RCMP. See Figure 11.

As expected, victims of credit card fraud reported to their credit card companies (78%) and victims of existing account fraud reported to their banks (75%). The reporting of victims of new accounts and other frauds reflects the variety of frauds in this category, with reports given to credit card companies (46%), banks (55%), utility companies (22%) and telephone companies (22%). They were also most likely to have reported the fraud to the police (34%). This was a multiple response question, so the significance of these differences cannot be determined, but detailed results of reporting by type of fraud can be seen in Appendix C, Figure 4.

Reporting rates to banks and credit card companies are similar to those reported in the 2006 survey. Historically, we found a higher rate of police reports (32%) and reports to the credit reporting companies (10%).

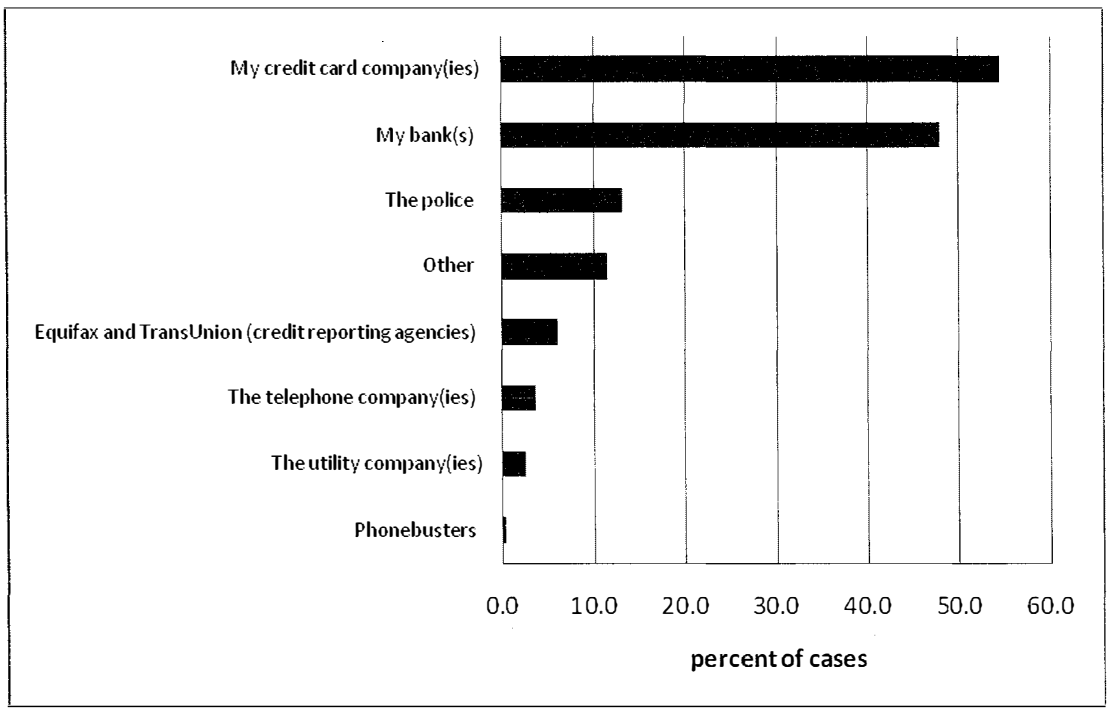


Figure 11 - Reporting

6.12 Victim Comments and Advice

Victims were asked if there was any other information that would help to describe the fraud. Most of the 129 comments were detailed descriptions of simple credit card or debit card frauds.

While many comments praised the banks and credit card companies for their help, there were a few comments indicating that the credit card companies or the police did not do enough to help (see below):

- "It really made me angry that the credit card company didn't really investigate the problem and take the information that I was trying to give them so that they could catch the person who reproduced my credit card. I had the employee's number from a cash receipt and the credit card company wasn't too interested in it. I was told that this happens hundreds of times a day and they just can't keep up with it. Well, I'm sorry but if I'm trying to help you catch this person the very least they could do was pretend to investigate it. It's no wonder that credit card fraud is such a huge problem. Credit card companies have the tools at their disposal to stop credit card fraud in its tracks and they are slow to implement it. Bring in the chip and stop allowing customers to pay for purchases without actually showing the credit card and a piece of photo ID."

- "I have never been repaid. Since I know who has stolen my credit card the bank told me that I need a police report to get reimbursed. The police did not want to help me because they believed he did not steal ENOUGH of my money to make it worth their time."

A few comments that indicated other types of identity fraud or more serious consequences include:

- "It was a long process to get things back to normal. It caused a lot of headache." "Violating and very inconvenient."
- "The fraudster would go into sex chat sites online posing as me looking for sex, set up rendezvous and then give my contact information…"

We also asked victims if there was any advice that they would give to others. We received 156 comments. The most frequent advice concerned monitoring accounts frequently and reviewing statements carefully (29 cases). Victims also advised caution when using debit and credit cards (26 cases). There were 4 warnings about phishing attempts and 4 warnings to stop shopping or banking online. A number of victims talked about keeping personal information to oneself:

- "Be careful anywhere with anyone."
- "Be aware that those who seem trustworthy may not be so."
- "Do always be careful of your wallet, even around family and spouses."
- "Never let anyone have access to your personal information."
- "Never let your personal stuff out of your hands."

A few victims seemed to feel that there is nothing that they can do to prevent a reoccurrence:

- "No, because fraud is too easy for people these days."
- "This type of fraud is very hard to avoid. I don't know how I can protect myself from that."
- "I do not think we can really protect ourselves against such fraud."

Other noteworthy advice included:

- "Buy a shredder! And shred all financial documents, for bills, taxes, statements."
- "Don't download movies and music from sites that leave your system open to hackers."
- "If mail is delivered to a multi box postal box where the whole panel is opened by the mail deliverer, have any credit cards mailed directly to the bank to be picked up there."
- "... Report to the police as soon as the fraud comes known. MAKE THE AUTHORITIES TAKE A REPORT. If the officer seems uninterested in taking your report or is being unhelpful ask to speak to his supervisor. It is the police agency's job to take the report. Keep records of everything. Don't throw anything away, backup computer info often, print and store all you can about the fraudster and what they are doing. When you find out what is happening, don't confront, entice or anger the fraudster in anyway. Make sure all your friends and co-workers are aware of the problem."

7.0 DATA BREACHES

Respondents who had never been the victim of any of the identity frauds discussed above were asked if they were aware of any situations where their personal information had been accessed or obtained by unauthorized people as part of a security breach or fraud operation. Over 250 respondents (8.4% of the total sample[10]) indicated that this had happened to them in the past, and 80 people (3% of the total sample[11]) indicated that this had happened to them in the last 12 months. This would represent over 700,000 adult Canadians.

Of the people who had experienced a data breach in the last 12 months, almost 50% said that this had happened in a store where they shopped in person[12]. The second most frequent place where information was accessed was at a bank or other financial

[10] At a 95% confidence interval (i.e. nineteen times out of twenty) the actual incidence rate will lie between 7.4% and 9.4%.

[11] At a 95% confidence interval (i.e. nineteen times out of twenty) the actual incidence rate will lie between 2.1% and 3.3%.

[12] A recent Gartner survey found that data breaches at retailers are responsible for 20% of all credit card and debit card fraud: McMillen, R. (2008). Most retailer breaches are not disclosed, Gartner says. IDG News Service. http://news.idg.no/cw/art.cfm?id=18560369-17A4-0F78-31A59A7821E0C048.)

institution, accounting for 17% of the breaches. It may not be a coincidence that the two most publicized data breaches in Canada in the last year were a breach at retailer TJX and the loss of a computer disk associated with CIBC's Talvest Mutual Funds. Affected customers of both of these incidents were notified by the respective organizations.

The remaining sources of the breaches each accounted for less than 10% of the cases. See Figure 12.

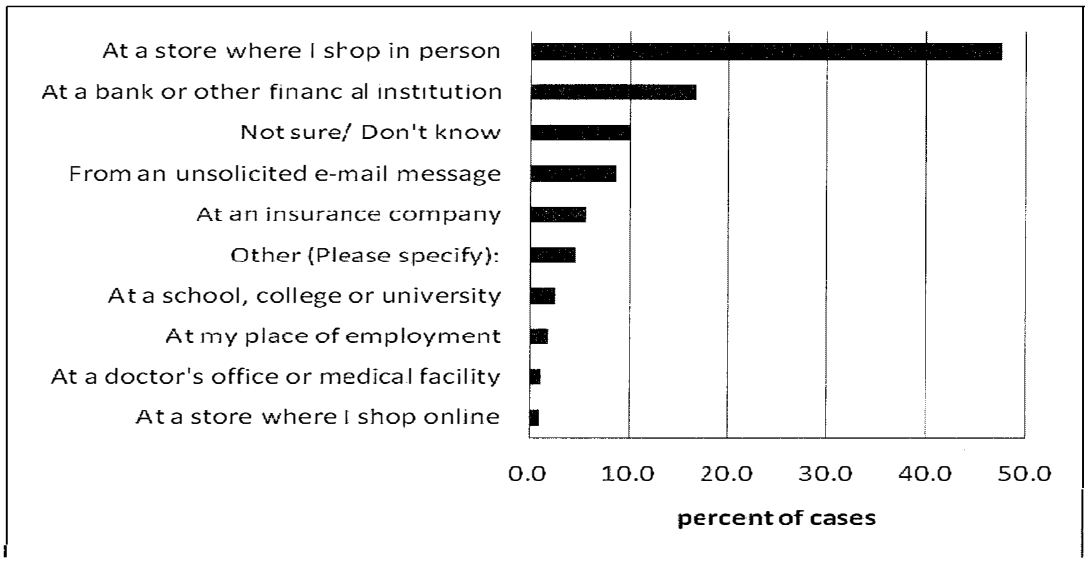


Figure 12 - Where was your personal information accessed or obtained?

Of those whose information was accessed from the files or records of an organization, almost two thirds (65%) were notified by the organization. Thirteen percent were aware that there had instances of fraud as a result of the breach.

ID Analytics suggests that it is useful to make a distinction between account-level breaches and identity-level breaches (ID Analytics 2006). Account-level breaches involve name and account information, such as account numbers, PINs and passwords. Account information can be changed easily, so frauds can be avoided in many cases and when frauds do occur, they can be stopped quickly after detection.

Identity level breaches involve information that can not be changed as readily, such as address, birth date, mother's maiden name as well as government-issued identity documents such as driver's license numbers, social insurance numbers and health card numbers. Frauds committed with identity level information tend to be of longer duration, more costly, and more difficult to resolve (ID Analytics 2006).

The differences can also be seen in the relative black-market values for different levels of personal information. An IBM study found that a standard identity, consisting of name, address, phone number and date of birth (identity-level information) is worth 500 credit card records (account-level information). If mother's maiden name, bank account number and bank account password are included with a standard identity (both identity and account-level information), its value is then equal to 2000 credit card records.

Figure 13 shows the type of information that was accessed in the breach. In 23% of the cases the victim did not know what information was taken. Of those who did know, 58% were account level only, 18% were identity level only and 24% involved both account and identity level information. Results from our 2006 survey were 61%, 10% and 29% respectively.

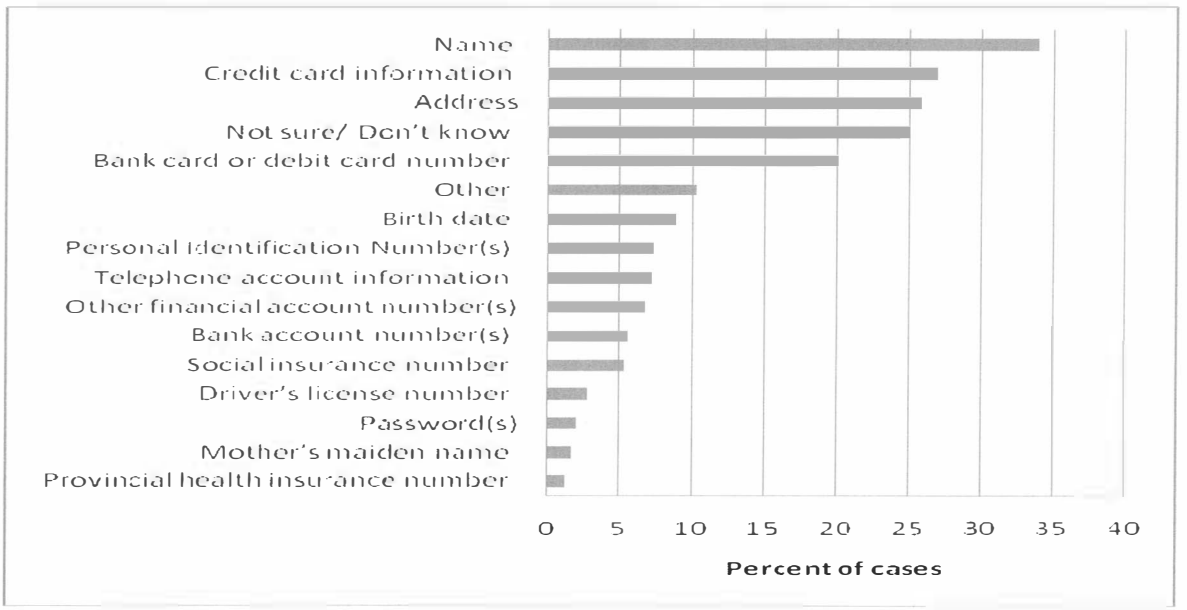


Figure 13 - What type of information was accessed?

8.0 CONCERN

All 3017 respondents were asked how concerned they were about becoming a victim of identity fraud in the future. The results are very similar to the results of the 2006 survey. The results from both surveys are shown in Figure 14.

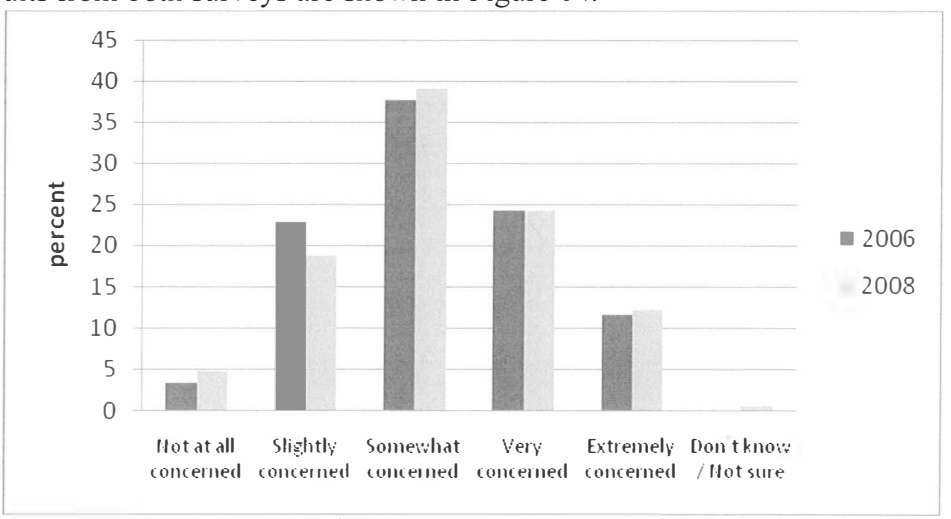


Figure 14 - Level of concern

We also asked if the respondent's level of concern was higher, lower or about the same as last year. Responses from both the 2006 survey and the 2008 survey are shown in Figure

15. It is interesting that while we cannot see a year on year difference in the general level of concern, the 2008 survey found that fully one-third of respondents believe that their level of concern is higher than it was a year ago.

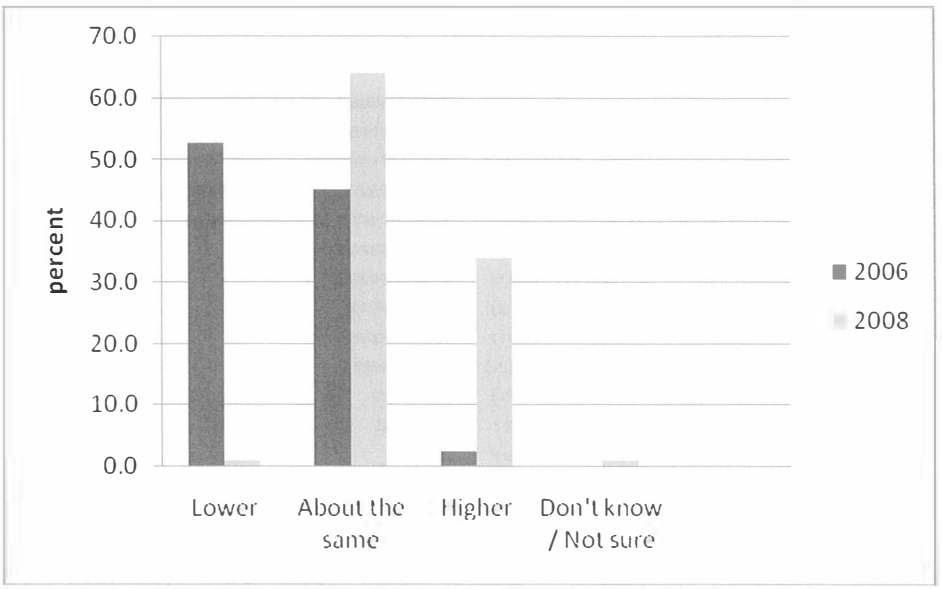


Figure 15 – Perceived change in level of concern

The level of concern generally increases with age (p=0.012). This is illustrated in Figure 16. Females also express a higher level of concern than males (p=0.003).

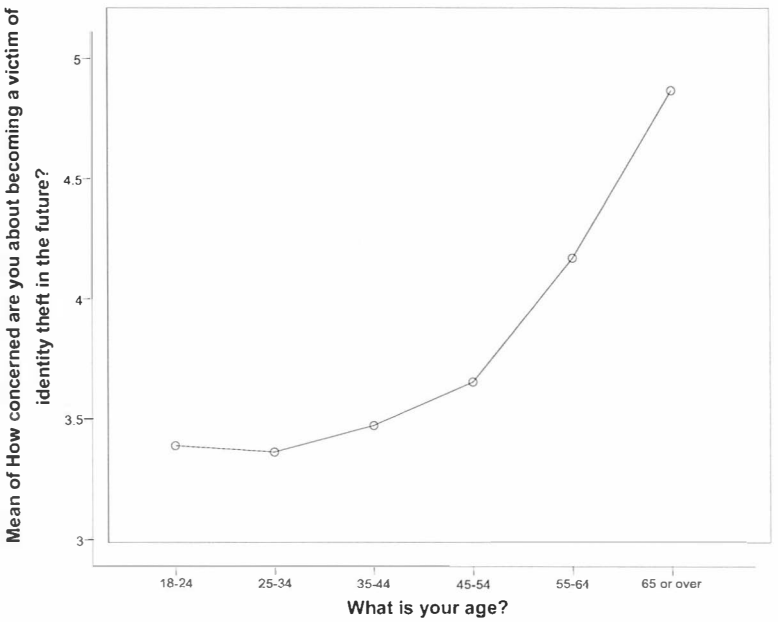


Figure 16 – Level of concern by age group

We looked at level of concern according to whether the respondent had ever been a victim of an identity fraud. In both our 2006 and 2008 surveys we find that the least concerned group was those who had experienced credit card fraud in the past. The most concerned were those who had experienced new accounts or other frauds. See Figure 7.

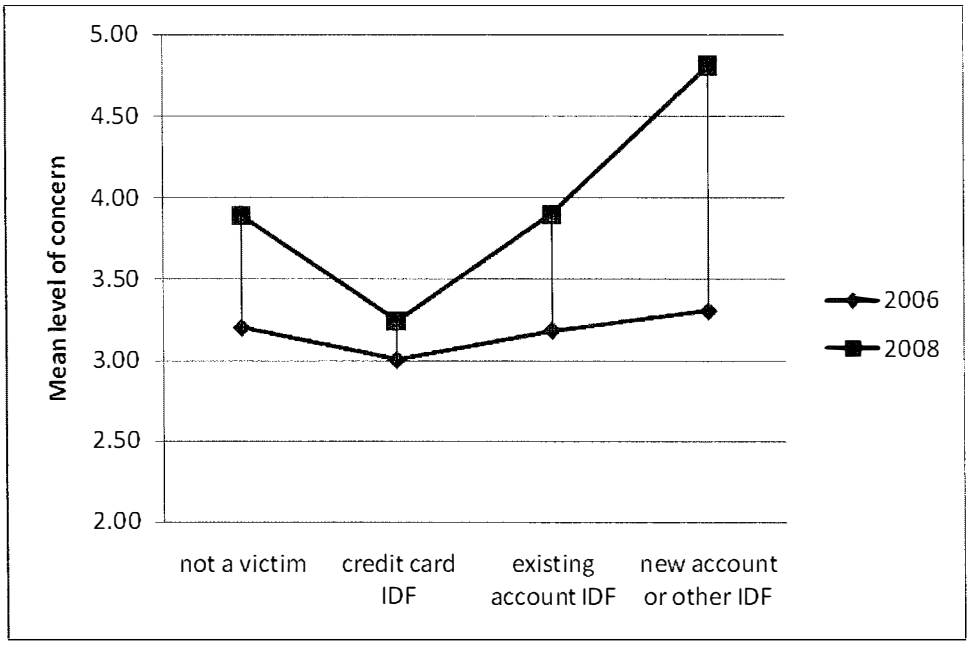


Figure 17 - Level of concern by fraud experience

We believe that this result provides a compelling argument that credit card fraud should not be included when we discuss the nature and impact of identity fraud. The processes that credit card companies have developed for the prevention, detection and investigation of credit card fraud are mature and sophisticated. When there are losses, the losses are generally absorbed by the credit card company or the retailer. As far as the consumer is concerned, the problem is easily and quickly resolved, at little to no personal cost other than obtaining a new credit card under a different account number.

9.0 PHISHING

In both the 2006 and 2008 consumer surveys we asked respondents whether they had received an e-mail from a bank or other company asking them to verify or update their account information. This describes an identity theft practice known as phishing. The link provided in a phishing e-mail will direct the responder to a Web site that appears to be the legitimate site, but is actually operated by the fraudsters. Any information that the respondent enters on this site is then accessible to the fraudsters.

Our 2008 results show that 41% of respondents had received a phishing e-mail, approximately the same proportion as in 2006. Of those that received such e-mails, 2.7% report that they responded and another 1.0% did not know/were not sure if they had responded. Encouragingly, these percentages are down from 3.4% and 1.5%,

respectively, reported in 2006.[13] We expect that greater media attention and more general awareness of the phishing problem have contributed to this decrease in potential victims.

10.0 BEHAVIOUR

10.1 Prevention and Detection Activities

The first behavioural question asked respondents about various activities that are often recommended to reduce the risk of identity theft or to reduce the impact of identity frauds. Figure 18 shows the percentage of people who responded that they do these activities never, rarely, some of the time, most of the time, or all of the time (where applicable).

The most frequent activities that people do to protect themselves (i.e. most of the time or all of the time) are to use anti-virus software (93%) and to know the approximate balance of their accounts and check it when they use an ABM (92%). When it comes to the physical security of documents and other sources of information, 88% make sure that no one is watching when using an ABM or debit card machine, 79% shred financial and other important documents, 59% use a locked mailbox and 57% keep sensitive information in a secure location, such as a locked drawer or box.

Passwords are the most common form of online authorization, and 75% of respondents say that they use hard to break passwords most of the time or all of the time. Only 59% say that they use different passwords for different applications or services most of the time or better. Another 24% of people do this some of the time.

Two of the questions were reverse questions, where the activity described is a risky behaviour. Of these, 92% said that they never or rarely gave information over the phone to people claiming to conduct surveys or offer promotional goods or services. To the question of whether people will respond to a business by clicking a link in an email, 37% said never, 31% said rarely and 25% said that they do this some of the time.

It is often recommended, as a security precaution, that people not take advantage of software features that will "remember" account numbers or passwords. Others argue that using such features is good as long as the computer is physically secure, as it eliminates the need to use easy to remember passwords or to write down sensitive account information. While we found that 44% never use these features, between 10% and 15% use them either rarely, some of the time, most of the time, or all of the time.

[13] The difference between a total of 4.9% (2006) and 3.7% (2008) potential victims, out of the total sample is significant at a 95% confidence level.

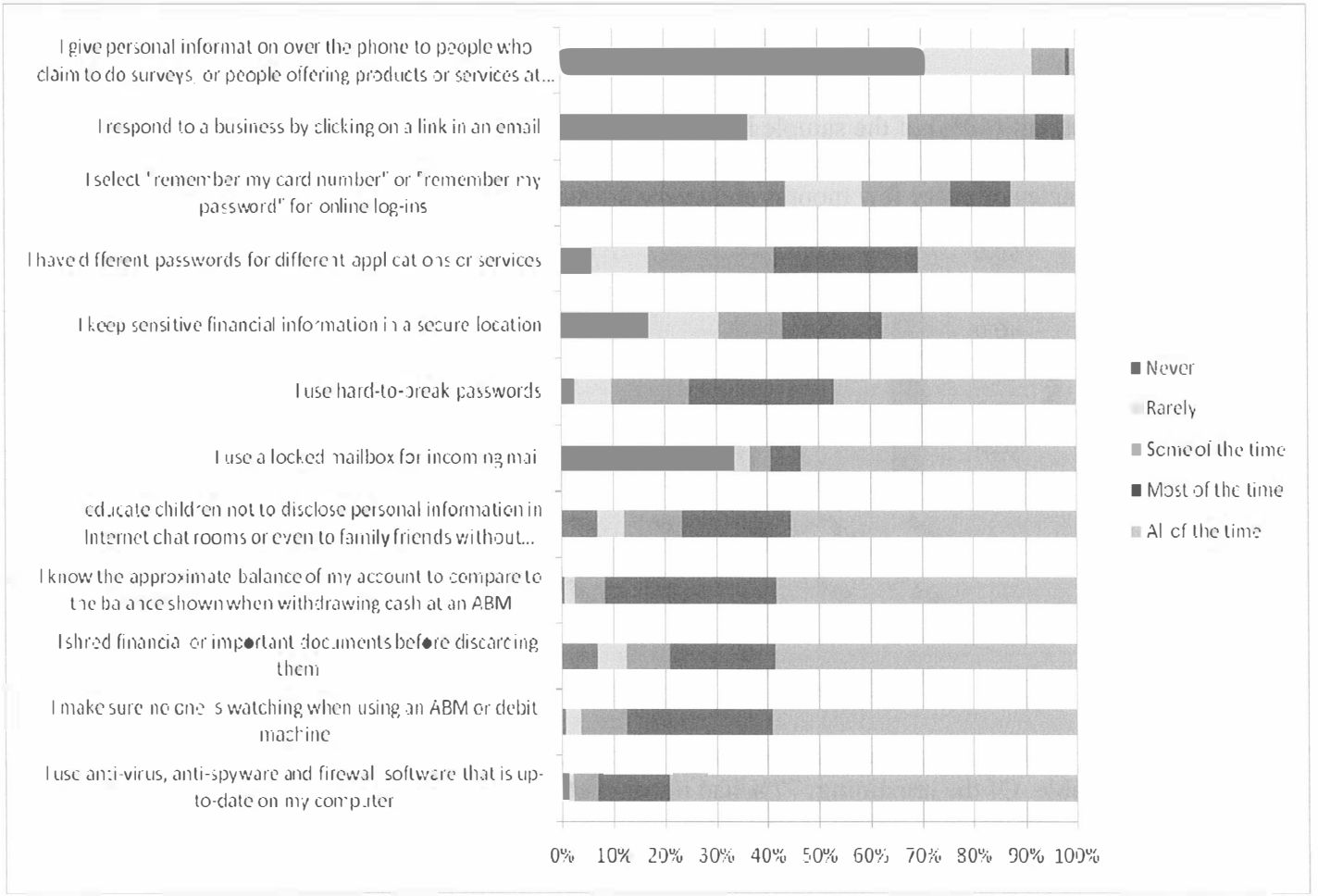


Figure 18 – Frequency of prevention and detection activities (where applicable)

The second behavioural question asked about how frequently people conducted certain behaviours that can lead to early detection of identity fraud. Early detection is important in minimizing the impact of most identity frauds (Javelin 2007). In general, people do check their bank accounts and credit accounts on a regular basis. The median and mode of the frequencies for both of these activities was "every few days". People check their bank accounts more frequently than their credit card accounts. See Figure 19.

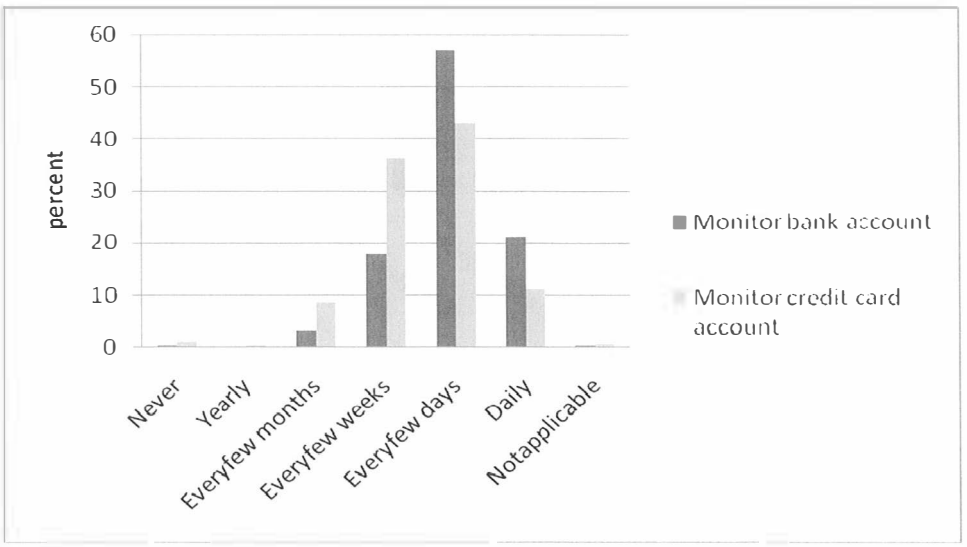


Figure 19 - Frequency of monitoring bank and credit card accounts

Almost half (49%) of the sample had never requested a copy of their credit report.[14] Of the proportion of the sample who request copies of their credit report, 72% fall between frequencies of every few months and every 2-5 years. See Figure 20.

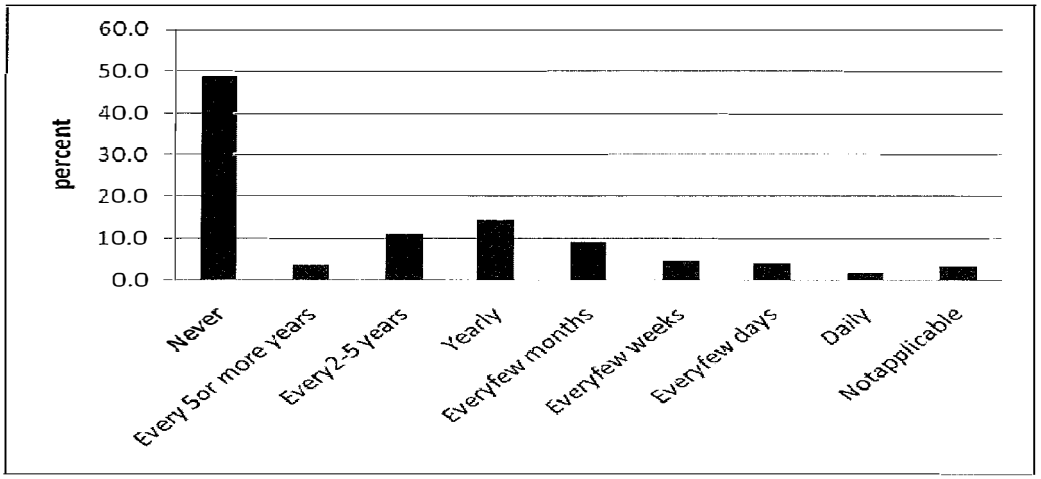


Figure 20 - Frequency of requests for credit report

Twenty-five percent of our sample indicated that checking land registry records was not applicable. Of the remaining, 77% had never checked land registry records. Eighteen percent had checked yearly or less frequently while 5 % reported checking more frequently than once a year.

In the previous question, we asked about using hard-to-break passwords and about using different passwords for different applications. In this question we asked how often people changed their important passwords (i.e. for online banking, email accounts, etc.). While almost 30% report that they never change their important passwords, over one half (50.1%) report that they change them with a frequency somewhere between every few months and every 2-5 years. See Figure 21.

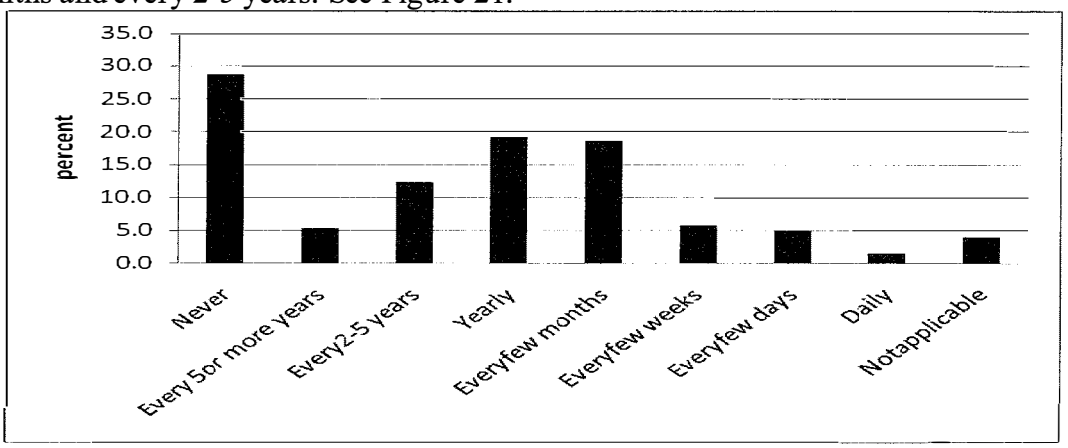


Figure 21 - Frequency of changing important passwords

[14] A telephone survey conducted at approximately the same time found that 74% of respondents had never asked for a credit report.
Sigma Assistel (2008). Identity theft: many Canadian adults still in the dark about the serious repercussions this phenomenon could have on their lives. http://www.assistel.com/en-CA/InMd/

10.2 Adoption of Pro-Active Risk Management Tools

The third behavioural question asked about the adoption of proactive risk management tools that have recently become available or gained popularity because of the threat of identity theft and fraud. Ninety percent of the sample had not subscribed to a credit monitoring service or purchased identity theft insurance. Although there is no significant difference in the adoption of these tools between all victims and non-victims, the proportion is reduced to 79% and 74% respectively for victims of new accounts or other frauds.

Credit alerts are placed on a credit record to alert potential creditors that there may be a problem with new applications. Eighty-seven percent of the sample had never had a credit alert put on their credit report; however this is reduced to 79% of victims, regardless of the type of fraud. When we look at the different categories of fraud, credit alerts were placed on 22% of credit card fraud victims, 17% of existing account fraud victims and 33% of new account and other fraud victims. There is no significant difference in the use of credit alerts between people who were subject to a data breach and non-victims in general.

As Figure 22 shows, although the use of these tools is not widespread, their use has increased in the last year.

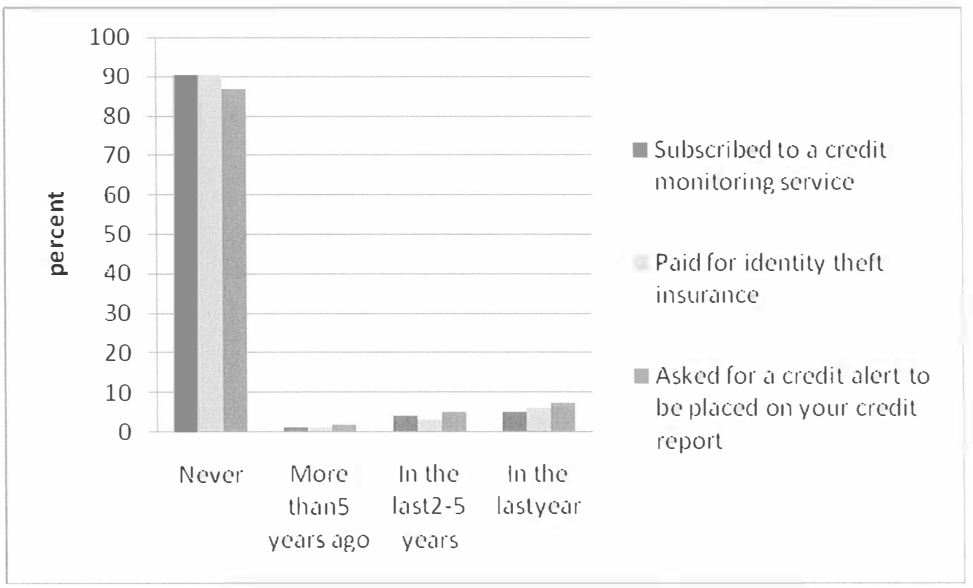


Figure 22 - Use of pro-active risk management tools

10.3 Changing behaviours

The fourth and final behavioural question asked how people had changed certain behaviours because of the threat of identity theft. Two of the behaviours relate to on-line activities (shopping and banking), one concerns an evolution from off-line to on-line (receipt of account statements), and two relate to off-line activities (credit card and document handling).

The results show that, while 60% of people had not changed their on-line shopping activities, fully 20% had reduced or stopped shopping on-line. (Twenty percent said this question was not applicable.) The threat of identity theft has had less of an impact on on-line banking, with 79% reporting no change in activities. Still, 9% had stopped or reduced their on-line banking. (Only 12% reported that on-line banking was not applicable.) See Figure 23

A *Consumer Reports* survey, conducted by Princeton Survey Research Associates in 2005, found that 9 out of 10 Internet users had changed their behaviours because of the threat of identity theft, with 30% reporting a reduction in overall usage. Twenty-five percent said that they had stopped shopping online and 29% said that they had reduced their frequency of purchases (Princeton 2005).

While our results do not show as large of an effect as the Princeton study, both show that the threat of identity theft is having a significant and detrimental effect on e-commerce in general.

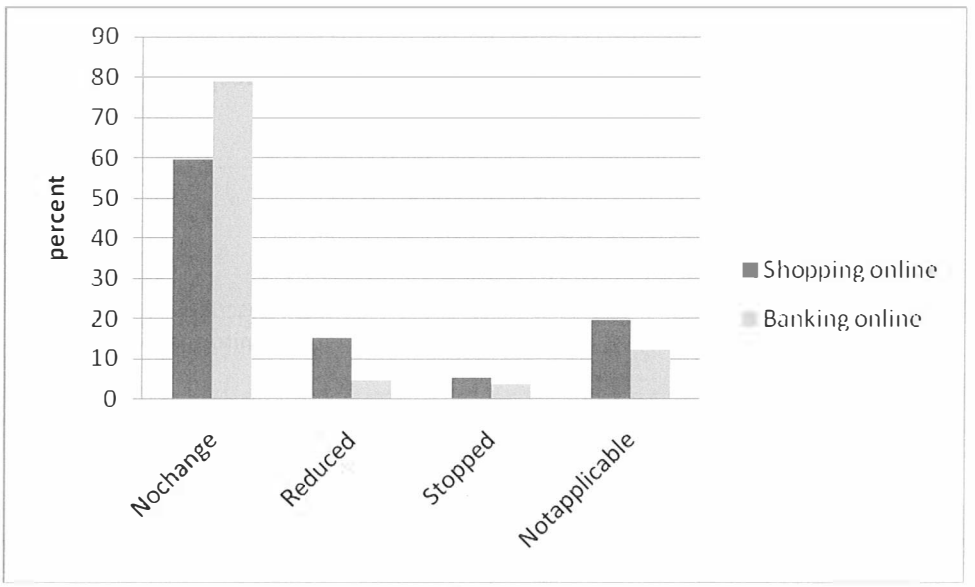


Figure 23 - Change in on-line activities

In the past, identity theft was commonly conducted by intercepting mailed statements for bank accounts, utility accounts or credit cards. Many companies are now offering the option of on-line statements, as both a cost efficient and more secure method of information delivery. Our results show that while 64% of respondents had not changed their methods of receiving statements, 22% had reduced the number of paper statements they received and 8% had stopped receiving paper statements. See Figure 24.

We asked whether people had changed how they handle their credit cards in gas stations or restaurants, where the service person usually takes the card out of the sight of the cardholder. Fifty-five percent of respondents have not changed their behaviour, but 24% say that they have reduced the number of times that they hand over their cards in these situations and 11% have stopped entirely. See Figure 24.

The final question asked if people had stopped or reduced the carrying of unnecessary information or documents in their purse or wallet. Of those that said this was applicable to them, 50% had either reduced (33%) or stopped (17%), carrying unnecessary information or documents. See Figure 24.

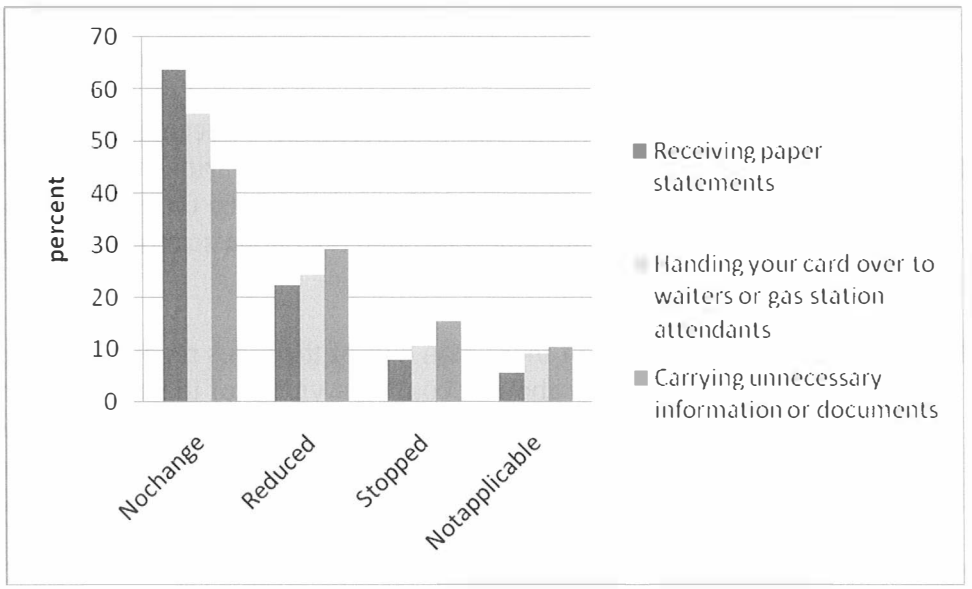


Figure 24 - Change in off-line behaviours

11.0 NEXT STEPS

This paper, and the working paper prepared from the 2006 survey (Sproule and Archer 2008), provide only a preliminary analysis of the results of these two surveys. We continue to examine the results of specific questions in detail. Further studies are underway to look at the effects of demographics on victimization and barriers to reporting. We will be responding to specific queries from government and other interested parties.

If a source of ongoing funding can be obtained, we would like to conduct a MeRC survey similar to the 2008 ORNEC survey on an annual basis. The results from such surveys would become part of an "identity theft index" that could provide ongoing, reliable information about the problem of identity theft and fraud in Canada.

We have also been working with the Canadian Centre for Justice Statistics (CCJS) in Statistics Canada on the design of a more general survey on consumer fraud in Canada. If funded, the identity theft and fraud questions in this survey would eliminate the need for an ongoing MeRC survey. The CCJS is also working on a survey of businesses to determine the nature and costs of fraud in the banking, retail and insurance sectors. Relevant results from this survey could also form part of an "identity theft index".

12.0 SUMMARY

The survey conducted by ORNEC in late 2006 provided a large amount of historical data about the characteristics of identity theft and fraud in Canada. The survey conducted in early 2008 provides a much smaller but more focused snapshot of cases that have happened on the past year. Although it is too early to try to identify trends, our results can be compared to results from similar surveys in the US and to this historical data.

We find a higher incidence rate than the US studies, probably because we provide more specific examples of what is included in our definition of the various types of identity fraud. Identity theft as a result of online transactions seems to be on the rise. While recent US studies show an increase in identity theft through telephone scams, we did not see a similar increase.

Simple credit card fraud accounts for more than half of the cases reported. Victims of this type of fraud are the least concerned about becoming a victim of identity theft and fraud in the future, reflecting the fact that these problems are resolved quickly and easily by the credit card company, often at little or no cost to the consumer. Any future research needs to recognize this in survey designs that isolate cases of simple credit card fraud from more serious frauds. Only then will we be able to properly address the problems associated with other types of identity fraud.

ORNEC initiated their identity theft research program because it was believed that the threat of identity theft and fraud could have a detrimental effect on e-commerce. Our results validate this concern as they show that 20% of Canadian consumers have reduced or stopped shopping online because of this threat.

13.0 REFERENCES

Anderson, K. B. (2005). Identity Theft: Does the Risk Vary with Demographics? Bureau of Economics, Federal Trade Commission. **Working Paper no. 279**. http://www.ftc.gov/be/workpapers/wp279.pdf

Cuganesan, S. and D. Lacey (2003). Identity Fraud in Australia: An Evaluation of its Nature, Cost and Extent. Sydney, Australia, Securities Industry Research Centre of Asia-Pacific (SIRCA): 1-126.

FTC (2003). Identity Theft Survey Report, Federal Trade Commission and Synovate. http://www.ftc.gov/os/2003/09/synovatereport.pdf

Gordon, G. R., D. J. Rebovich, et al. (2007). Identity Fraud Trends and Patterns: Building a Foundation for Proactive Enforcement, Center for Identity Management and Information Protection. http://www.utica.edu/academic/institutes/cimip/publications/index.cfm

ID Analytics (2006). National Data Breach Analysis, ID Analytics Inc.: 2-36.

Ipsos-Reid (2006). Concern Over Identity Theft is Changing Consumer Behaviour, Ipsos-Reid on behalf of Capital One. http://www.ipsos-na.com/news/pressrelease.cfm?id=3294#

Javelin (2005). 2005 Identity Fraud Survey Report (Complimentary Overview). Pleasanton, CA, Javelin Strategy & Research. http://www.javelinstrategy.com/reports/2005IdentityFraudSurveyReport.php

Javelin (2006). 2006 Identity Fraud Survey Report, Javelin Strategy and Research, co-released with the Better Business Bureau, sponsored by Visa USA, Wells Fargo Bank and CheckFree Corporation. http://www.javelinstrategy.com/research

Javelin (2007). 2007 Identity Fraud Survey Report: Identity Fraud is Dropping, Continued Vigilance is Necessary. Pleasanton, CA, Javelin Strategy and Research. http://www.javelinstrategy.com/uploads/701.R_2007IdentityFraudSurveyReport_Brochure.pdf

Javelin (2008). 2008 Identity Fraud Survey Report: Identity Fraud Continues to Decline, But Criminals More Effective at Using All Channels.

Javelin (2008). Overall Fraud Down 12%, Criminals Trapping Victims Over the Phone. Press Release. http://www.javelinstrategy.com/2008/02/11/new-research-confirms-identity-fraud-is-on-decline

Litan, A. (2007). The Truth Behind Identity Theft Numbers, Gartner, Inc.

McMillen, R. (2008). Most retailer breaches are not disclosed, Gartner says. IDG News Service. http://news.idg.no/cw/art.cfm?id=18560369-17A4-0F78-31A59A7821E0C048

Princeton (2005). Leap of Faith: Using the Internet Despite the Dangers. Princeton Survey Research Associates International. Yonkers, NJ, Consumer Reports WebWatch. http://www.consumerwebwatch.org/pdfs/princeton.pdf

Sigma Assistel (2008). Identity theft: many Canadian adults still in the dark about the serious repercussions this phenomenon could have on their lives. http://www.assistel.com/en-CA/InMd/

Sproule, S. and N. Archer (2007). Defining Identity Theft. Eighth World Congress on the Management of eBusiness (WCMeB 2007), Toronto, IEEE. http://ieeexplore.ieee.org/iel5/4285290/4285291/04285319.pdf

Sproule, S. and N. Archer (2008). Measuring Identity Theft in Canada: 2006 Consumer Survey. McMaster eBusiness Research Centre (MeRC) - Working Paper #21. Hamilton.

14.0 APPENDIX A - 2008 CONSUMER IDT/F QUESTIONNAIRE

English / French bifurcation screen (French translation available on request)

Introduction

This survey is part of a research project being carried out by a group of researchers at McMaster University. This research will help to develop current estimates of the nature and extent of identity theft and identity fraud in Canada. It will also provide insight into how the threat of identity theft is changing the behaviours of Canadian consumers. If you would like to see the results of the survey, watch for updates on the McMaster eBusiness Research Centre web site at http://merc.mcmaster.ca/projects.html.

Screening and Quotas

2. How many bank accounts (chequing or savings) do you have?
   - 0 (participant to be screened out)
   - 1
   - 2
   - 3
   - 4
   - 5
   - More than 5

3. How many credit cards do you have?
   - 0 (participant to be screened out)
   - 1
   - 2
   - 3
   - 4
   - 5
   - More than 5

4. What is your age?
   - Under 18 (participant to be screened out)
   - 18-24
   - 25-34
   - 35-44
   - 45-54
   - 55-64
   - 65 or over

5. Are you?
   - Male
   - Female

6. Where do you live?

Newfoundland and Labrador
Prince Edward Island
Nova Scotia
New Brunswick
Ontario
Quebec
Manitoba
Saskatchewan
Alberta
British Columbia

Note: See the last page of this document for a routing diagram for the next few sections.

Credit Card Fraud

7. *Credit card fraud* occurs when someone makes purchases or otherwise puts charges on a credit card account without your permission. Credit cards include bank-issued credit cards such as Visa, MasterCard, and American Express, as well as retail store-brand credit cards, such as The Bay, Sears, Canadian Tire and others.

Examples of *credit card fraud* include:

- Someone steals your wallet and uses your credit card to make purchases at a store
- The credit card company phones to verify a purchase that you have not made or authorized.
- You notice unauthorized purchases on your monthly statement.

Has *credit card fraud* ever happened to you?

Yes **(Go to 8.)**
No **(Go to 12.)**

8. Has *credit card fraud* happened to you in the last year?

Yes **(Go to 9.)**
No **(Go to 12.)**

9. How many of your existing credit card accounts were affected?

1
2
3
4
5
More than 5

10. Did someone attempt to take-over the credit card account(s), for example, by changing the billing address or having themselves added as an authorized user of the account?

Yes
No

11. What kinds of credit card(s) were involved in the fraud? (Check all that apply.)

Card (s) issued by a bank or other financial institution (e.g. MasterCard, Visa, American Express, etc.)
Card(s) issued by a retail store (e.g. The Bay, Sears, Canadian Tire, etc.)
Other cards (please specify)

(Go to 12.)

Existing Account Fraud

12. *Existing account fraud* occurs when someone gains access to one of your existing accounts (other than a credit card account) without your permission and runs up charges or takes money from the account. This could be a bank account, a telephone account, a utility account, a line-of-credit or loan, or an online account such as an eBay or PayPal account.

Examples of *existing account fraud* are:

- Someone takes your cheque book and forges your name on a number of cheques
- Someone obtains your debit/bank card information, including your PIN, and money is withdrawn from your bank account.
- You receive your phone bill and there are a number of expensive long distance calls that you did not make. The phone company representative tells you that someone used your calling card number and your PIN to make the calls.
- You move, but the new resident continues to have telephone and electric utility services billed to your account.
- Your roommate uses your computer to list fraudulent items for auction under your name and your eBay account.

Has *existing account fraud* ever happened to you?

Yes **(Go to 13.)**
No **(Go to 16.)**

13. Has *existing account fraud* happened to you in the last year?

Yes **(Go to 14.)**
No **(Go to 16.)**

14. Did someone attempt to take over the account(s), by changing the billing address or other account details?

Yes
No

15. What kind of existing account(s) were involved in the fraud? (Check all that apply)

Bank chequing or savings account

Bank line-of-credit account
Bank loan
Mortgage
Wireless telephone account
Conventional telephone account
Electric utility account
eBay account
PayPal account
Other (please specify)

(Go to 16.)

New Account Fraud

16. *New account fraud* occurs when someone uses your personal information to obtain new credit cards, loans, or other accounts, such as telephone accounts or utility accounts, and runs up debts in your name.

Examples of *new account fraud* are:

- Someone opens up a new credit card account in your name and charges purchases on the card which you are then expected to pay for.
- Someone takes out a loan, opens a line of credit or takes out a mortgage on your house in your name
- Someone gives your personal information to open a new cellular telephone account and runs up a phone bill in your name.

Has *new account fraud* ever happened to you?

Yes **(Go to 17.)**
No **(Go to 19.)**

17. Has *new account fraud* happened to you in the last year?

Yes **(Go to 18.)**
No **(Go to 19.)**

18. What kind of new account(s) were involved in the fraud?

Bank-issued credit cards (MasterCard, Visa, American Express, etc.)
Store-issued credit cards (The Bay, Sears, Canadian Tire, etc.)
Bank chequing account
Bank savings account
Bank line-of-credit account
Bank loan
Mortgage
Wireless telephone account
Conventional telephone account
Electric utility account
Natural gas utility account

eBay account
PayPal account
Other (please specify)

(Go to 19.)

Other Identity Fraud

19. *Other identity frauds* occur when someone uses your personal information to impersonate you to gain employment, receive benefits, avoid criminal prosecution or otherwise commit fraud or other crimes.

Examples of *other identity frauds* are:

- You receive a notice from the Canada Revenue Agency that you owe income tax from a job that you never had.
- A friend or neighbour gives your name and address as his or her own when he or she is arrested.
- Someone applies for car insurance using your personal information
- You find out that someone used your personal information to get a replacement health card and obtain health care services under your name.

Has *other identity fraud* ever happened to you?

Yes **(Go to 20.)**
No **(Go to 22.)**

20. Has *other identity fraud* happened to you in the last year?

Yes **(go to 21.)**
No **(go to 22.)**

21. What type(s) of other identity frauds happened to you in the last year? (Check all that apply.)

Someone impersonated you to gain employment
Someone impersonated you to obtain health care services
Someone impersonated you to obtain government benefits other than health care services
Someone impersonated you to avoid criminal prosecution
Someone impersonated you to rent an apartment or a house
Someone impersonated you to obtain insurance
Someone impersonated you to change the title of your home or to sell your home without your knowledge
Other (Please specify)

(Go to 22.)

22. Question 22 is a routing question in the pretest. This question was not be required in the final version as OpenVenue programmed in the following routing logic:

If any of the answers to 8, 13. 17, or 20 are YES (i.e. been a victim of at least one type of fraud in the last year), go to 23.
If all of the answers to 7, 12, 16, and 19 are all NO (i.e. never been a victim), go to 36.
Otherwise (i.e. been a victim of at least one type of fraud, but not in the last year), go to 42.

Additional Victim Questions

23. How was the fraud discovered? (Check all that apply)

Belongings had been stolen
I requested a copy of my credit report
An application for credit, a loan or a mortgage was turned down.
I was notified by my bank
I was notified by my credit card company
I discovered it when I received my account statement in the mail
I discovered it by monitoring my account online
I was notified by police
I was contacted by creditors or a collection agency about unpaid bills
An organization notified me that my personal information had been accessed or taken by an unauthorized person.
Other (please specify)

24. What was the interval between the time your personal information was stolen and your discovery of the theft? (Check one)

Less than 1 week
1 week to 1 month
1 month to 6 months
6 months to 1 year
More than 1 year
Don't know / Not sure

25. Do you know, or think you know, how the personal information obtained in the identity theft was accessed or taken? (Check one)

Yes **(Go to 26.)**
No **(Go to 27.)**

26. How do you think the information was accessed or taken? (Check one)

Lost or misplaced wallet, purse, or documents
Stolen wallet, purse, or documents
Mail was intercepted or redirected
It was taken from public records
The information was provided in response to an email or telephone call from what appeared to be a legitimate source
It was taken during a business transaction conducted online
It was taken during a business transaction conducted over the telephone
It was taken during a business transaction conducted in person

It was taken from the customer records or employee records of an organization
Someone close to me knew or had access to the information
It was taken from discarded credit card receipts or account statements
My computer was compromised by a hacker or by malicious software such as a virus or spyware
My debit (bank) card was copied and my PIN recorded at a compromised ATM machine
Other (please specify)

27. Do you know anything at all about the person who accessed or took the information? (For example, you may not know their name, but know where they worked or lived.) (Check one)

Yes **(Go to 28.)**
No **(Go to 29.)**

28. Which of the following best describes the person who took the information? (Check one)

A complete stranger
A relative
A friend or roommate
An in-home employee or contractor
A spouse or ex-spouse
A neighbour
An acquaintance
A corrupt employee of a company I did business with
A coworker
Other (please specify)

29. How much money did the perpetrator obtain through the fraud? (Include the value of merchandise, loans, cash, services, and anything else the person may have obtained.) (Check one)

Less than $100
$100 - $499
$500 - $999
$1,000 - $4,999
$5,000 - $9,999
$10,000 - $24,999
$25,000 - $49,999
$50,000 - $99,999
$100,000 or more

30. How many hours of your time have been spent resolving problems associated with this fraud? (Check one)

1 hour or less
2 to 9 hours

10 to 39 hours
40 to 79 hours
80 to 159 hours
160 to 239 hours
240 hours or more

31. How much of your own money was spent to resolve problems associated with the fraud? (Include costs for postage, copying, legal fees, notarized documents, and payment of any fraudulent debts.) (Check one)

$0
Less than $50
$50 - $99
$100 - $499
$500 - $999
$1,000 - $4,999
$5,000 - $9,999
$10,000 or more

32. What other (non-monetary) costs resulted from the fraud? (Check all that apply)

Been turned down for a loan
Had banking problems
Had problems with credit card accounts
Had phone or utilities cut off or been denied new service
Had to pay higher interest rates on credit cards, loans, etc.
Been turned down for insurance or had to pay higher rates
Been contacted by a debt collector or creditor
Been the subject of a civil suit or judgment
Been the subject of a criminal investigation, warrant, proceeding or conviction?
Other (please specify)

33. To whom was the fraud reported? (Check all that apply)

My credit card company(ies)
My bank(s)
The utility company(ies)
The telephone company(ies)
The police
Phonebusters (an anti-fraud call centre operated by the RCMP and the Ontario Provincial Police)
Equifax and TransUnion (credit reporting agencies)
Other (please specify)

34. Is there any other information that would help to describe this episode of fraud?

35. Is there any advice that you would give to others to protect themselves from similar frauds?

Go to 42.

Data breaches

Note: Question 36 is asked if the respondent has never been a victim of any kind of identity fraud. We do not ask this question of people who have ever been victims.

36. Even if you have not been a victim of any of the above frauds, are you aware of any situations in which your personal information has been accessed or obtained by unauthorized people as part of a security breach or fraud operation?

Examples of this could include:

- You receive a notice from your insurance company that a computer or a disc with client information has been lost or stolen.
- You hear that a fellow employee has been charged with fraud for accessing other employees' personal information and selling it to a fraud ring.
- You receive a notice from a company informing all of their clients that someone has hacked into their database and stolen clients' personal information.

Have any of these situations ever happened to you?

Yes **(Go to 37.)**
No **(Go to 42.)**

37. Have any of these situations, where your personal information was accessed or obtained by unauthorized people, happened to you in the last year?

Yes **(Go to 38.)**
No **(Go to 42.)**

38. Where was your personal information accessed or obtained? (Check one)

At my place of employment
At a store where I shop in person
At a store where I shop online
At a store where I shop by telephone
At a bank or other financial institution
At a school, college or university
At a doctor's office or medical facility
At an insurance company
From an unsolicited telephone call
From an unsolicited e-mail message
Not sure/ Don't know
Other (Please specify)

39. What kind of personal information was accessed or obtained? (Check all that apply)

Name
Address

Credit card information
Bank card or debit card number
Bank account number(s)
Other financial account number(s)
Social insurance number
Provincial health insurance number
Telephone account information
Birth date
Driver's license number
Mother's maiden name
Password(s)
Personal Identification Number(s)
Not sure/ Don't know
Other (please specify)

40. If your information was accessed from the files or records of an organization, were you notified by that organization?

Yes
No
Not applicable
Not sure/ Don't know

41. Are you aware of any frauds (with yourself or others as victims) that occurred as a result of this situation?

Yes
No
Don't know/ Not sure

(Go to 42.)

Concern

42. How concerned are you about becoming a victim of identity theft in the future? (Check one)

Not at all concerned
Slightly concerned
Somewhat concerned
Very concerned
Extremely concerned
Don't know / Not sure

43. Would you say that your level of concern about becoming a victim of identity theft is higher, lower or about the same as it was one year ago? (Check one)

Higher
About the same
Lower
Don't know / Not sure

Phishing

44. In the last year, have you received emails from a bank or other company asking you to verify or update your account information? (Check one)

Yes **(Go to 45.)**
No **(Go to 46.)**

45. Have you responded to any of these emails by providing account information? (Check one)

Yes
No
Not sure/ Don't know

Behaviour

46. For each of the following activities, please check the most appropriate answer.

MATRIX COLUMNS

- All of the time
- Most of the time
- Some of the time
- Rarely
- Never
- Not applicable

MATRIX ROWS

- I use a locked mailbox for incoming mail
- I shred financial or important documents before discarding them
- I keep sensitive financial information in a secure location, such as a locked drawer or box.
- I make sure no one is watching when using an automated banking machine (ABM) or debit machine at a checkout counter.
- I use anti-virus, anti-spyware and firewall software that is up-to-date on my computer
- I select "remember my card number" or "remember my password" for online log-ins. (REVERSE)
- I have different passwords for different applications or services
- I use hard-to-break passwords. (i.e. avoid using family member's names or common dictionary words and include special characters and numbers in passwords.)
- I give personal information over the phone to people who claim to do surveys, or people offering products or services at special prices. (REVERSE)
- I educate children not to disclose personal information in Internet chat rooms or even to family friends without parents' approval.
- I respond to a business by clicking on a link in an email. (REVERSE)
- I know the approximate balance of my account to compare to the balance shown when withdrawing cash at an Automated Banking Machine (ABM).

47. How often do you do the following?

MATRIX COLUMNS

- Daily
- Every few days
- Every few weeks
- Every few months
- Yearly
- Every 2-5 years
- Every 5 or more years
- Never
- Not applicable

MATRIX ROWS

- Monitor bank account balances and activity
  Monitor credit card accounts and activity
- Request a copy of your credit report
- Check Land Registry Office records to ensure validity of ownership
- Change important passwords (i.e. for online banking, email accounts, etc.)

48. Because of a concern about identity theft, have you done any of the following?

MATRIX COLUMNS

- In the last year
- In the last 2-5 years
- More than 5 years ago
- Never

MATRIX ROWS

- Subscribed to a credit monitoring service
- Paid for identity theft insurance
- Asked for a credit alert to be placed on your credit report

49. Because of a concern about identity theft, have you stopped or reduced your activities in any of the following areas?

MATRIX COLUMNS

- Stopped
- Reduced
- No change
- Not applicable

MATRIX ROWS

- Shopping online
- Receiving paper statements from banks, utilities, and other sources
- Handing your card over to waiters or gas station attendants
- Carrying unnecessary information or documents in your purse or wallet
- Banking online

Additional Demographics

50. What is your highest level of education?
    Some/completed elementary school
    Some/completed high school
    Some/completed technical school
    Some/completed community college/ CEGEP
    Some/completed university
    Some/completed graduate school
    Prefer not to answer

51. What is your marital status?
    Single, never married
    Married or living together
    Separated or divorced
    Widowed
    Prefer not to answer

52. Including yourself, how many people are there in your household who are…
    Adults 18 years and older
    Teens 13 to 17 years of age
    Children 7 to 12 years of age
    Children 6 and under
    Prefer not to answer

53. What is your total household income?
    Less than $25,000
    $25,000-49,999
    $50,000-74,999
    $75,000-99,999
    $100,000 or more
    Prefer not to answer

Online exposure

54. How often do you shop online?
    Never
    Seldom
    Occasionally
    Often

55. How many email accounts (business or personal) do you have?

0
1
2
3
4
5
More than 5

56. Do you have online access for any of your bank accounts?

Yes **(Go to 57.)**
No **(Go to 59.)**

57. Do you check the balances of these bank account(s) online?

Yes
No

58. Do you conduct bank transactions online, such as paying bills or transferring funds?

Yes
No

59. In addition to email accounts and online bank accounts, do you have any other online accounts which you use to conduct transactions?

eBay account
PayPal account
Other (Please specify)

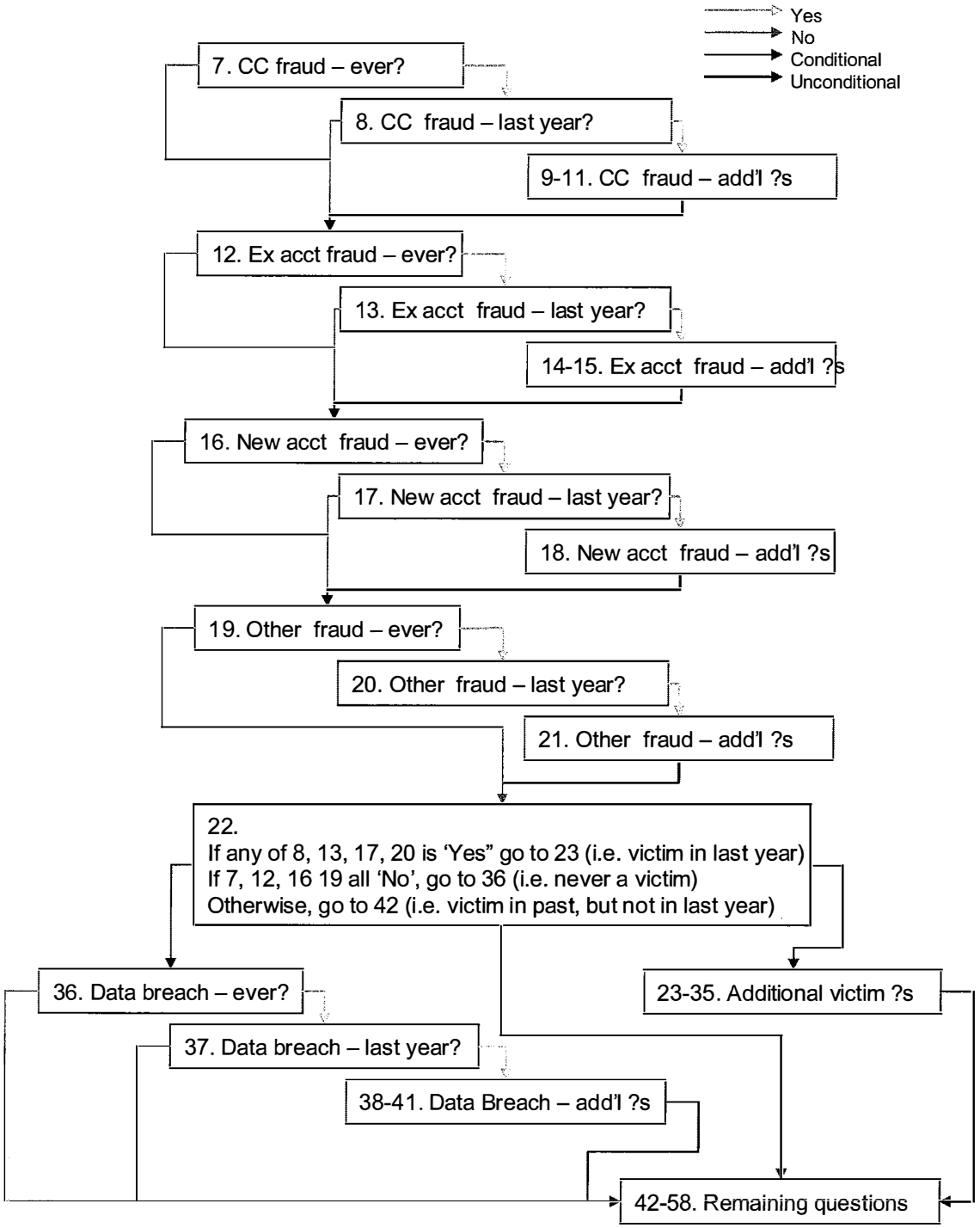
15.0 APPENDIX B - WEIGHTS FOR POST-STRATIFICATION

Province	Gender	Age group	Population	Prop of Popl'n	Sample	Prop of Sample	Weight
Nfld&Lab	M	18-24	24,903	0.0010	0	0.0000	1.0000
		25-44	71,283	0.0028	17	0.0056	0.5000
		45-64	74,940	0.0030	11	0.0036	0.8123
		65 or older	30,314	0.0012	4	0.0013	0.9036
	F	18-24	24668	0.0010	4	0.0013	0.7353
		25-44	74449	0.0029	22	0.0073	0.4035
		45-64	76515	0.0030	10	0.0033	0.9123
		65 or older	37431	0.0015	1	0.0003	4.4631
PEI	M	18-24	7025	0.0003	0	0.0000	1.0000
		25-44	17908	0.0007	3	0.0010	0.7118
		45-64	18329	0.0007	6	0.0020	0.3642
		65 or older	8423	0.0003	1	0.0003	1.0043
	F	18-24	6992	0.0003	2	0.0007	0.4169
		25-44	18758	0.0007	3	0.0010	0.7455
		45-64	19121	0.0008	2	0.0007	1.1400
		65 or older	11028	0.0004	0	0.0000	1.0000
NS	M	18-24	45605	0.0018	1	0.0003	5.4378
		25-44	130275	0.0051	26	0.0086	0.5974
		45-64	129172	0.0051	19	0.0063	0.8106
		65 or older	57529	0.0023	8	0.0027	0.8574
	F	18-24	43679	0.0017	4	0.0013	1.3020
		25-44	133328	0.0053	41	0.0136	0.3877
		45-64	132769	0.0052	15	0.0050	1.0554
		65 or older	76042	0.0030	1	0.0003	9.0670
NB	M	18-24	36778	0.0015	3	0.0010	1.4618
		25-44	107454	0.0042	21	0.0070	0.6101
		45-64	104795	0.0041	13	0.0043	0.9612
		65 or older	44857	0.0018	5	0.0017	1.0697
	F	18-24	34268	0.0014	5	0.0017	0.8172
		25-44	106948	0.0042	18	0.0060	0.7085
		45-64	106268	0.0042	14	0.0046	0.9051
		65 or older	59854	0.0024	2	0.0007	3.5684

Province	Gender	Age group	Population	Prop of Popl'n	Sample	Prop of Sample	Weight
Quebec	M	18-24	350417	0.0138	52	0.0172	0.8035
		25-44	1125853	0.0445	192	0.0636	0.6992
		45-64	1046995	0.0414	159	0.0527	0.7852
		65 or older	439012	0.0174	32	0.0106	1.6358
	F	18-24	334214	0.0132	94	0.0312	0.4239
		25-44	1082141	0.0428	218	0.0723	0.5919
		45-64	1074784	0.0425	60	0.0199	2.1359
		65 or older	606649	0.0240	7	0.0023	10.3335
Ontario	M	18-24	610467	0.0241	31	0.0103	2.3481
		25-44	1900336	0.0751	171	0.0567	1.3251
		45-64	1559225	0.0616	195	0.0646	0.9534
		65 or older	702037	0.0277	52	0.0172	1.6098
	F	18-24	587286	0.0232	55	0.0182	1.2732
		25-44	1895247	0.0749	291	0.0965	0.7766
		45-64	1602498	0.0633	244	0.0809	0.7831
		65 or older	906661	0.0358	36	0.0119	3.0030
Manitoba	M	18-24	60488	0.0024	5	0.0017	1.4425
		25-44	167041	0.0066	19	0.0063	1.0483
		45-64	145046	0.0057	23	0.0076	0.7519
		65 or older	67729	0.0027	4	0.0013	2.0189
	F	18-24	57241	0.0023	3	0.0010	2.2751
		25-44	160860	0.0064	32	0.0106	0.5994
		45-64	145691	0.0058	20	0.0066	0.8686
		65 or older	90860	0.0036	2	0.0007	5.4169
Sask	M	18-24	55002	0.0022	4	0.0013	1.6396
		25-44	129625	0.0051	20	0.0066	0.7728
		45-64	121621	0.0048	15	0.0050	0.9668
		65 or older	63962	0.0025	4	0.0013	1.9067
	F	18-24	51056	0.0020	5	0.0017	1.2175
		25-44	128323	0.0051	32	0.0106	0.4781
		45-64	120447	0.0048	19	0.0063	0.7559
		65 or older	83140	0.0033	2	0.0007	4.9567
Alberta	M	18-24	179140	0.0071	12	0.0040	1.7800
		25-44	519567	0.0205	45	0.0149	1.3767
		45-64	402768	0.0159	44	0.0146	1.0915

Province	Gender	Age group	Population	Prop of Popl'n	Sample	Prop of Sample	Weight
		65 or older	152098	0.0060	17	0.0056	1.0668
	F	18-24	168239	0.0066	16	0.0053	1.2538
		25-44	489812	0.0194	61	0.0202	0.9574
		45-64	393297	0.0155	49	0.0162	0.9570
		65 or older	188455	0.0074	10	0.0033	2.2471
BC	M	18-24	213967	0.0085	8	0.0027	3.1891
		25-44	617119	0.0244	60	0.0199	1.2264
		45-64	570088	0.0225	77	0.0255	0.8828
		65 or older	265531	0.0105	29	0.0096	1.0918
	F	18-24	203362	0.0080	15	0.0050	1.6165
		25-44	621748	0.0246	102	0.0338	0.7268
		45-64	580583	0.0229	75	0.0249	0.9230
		65 or older	321225	0.0127	17	0.0056	2.2530
Grand Total			25302654		3017		

Skip logic and routing for identity theft and fraud questions



16.0 APPENDIX C

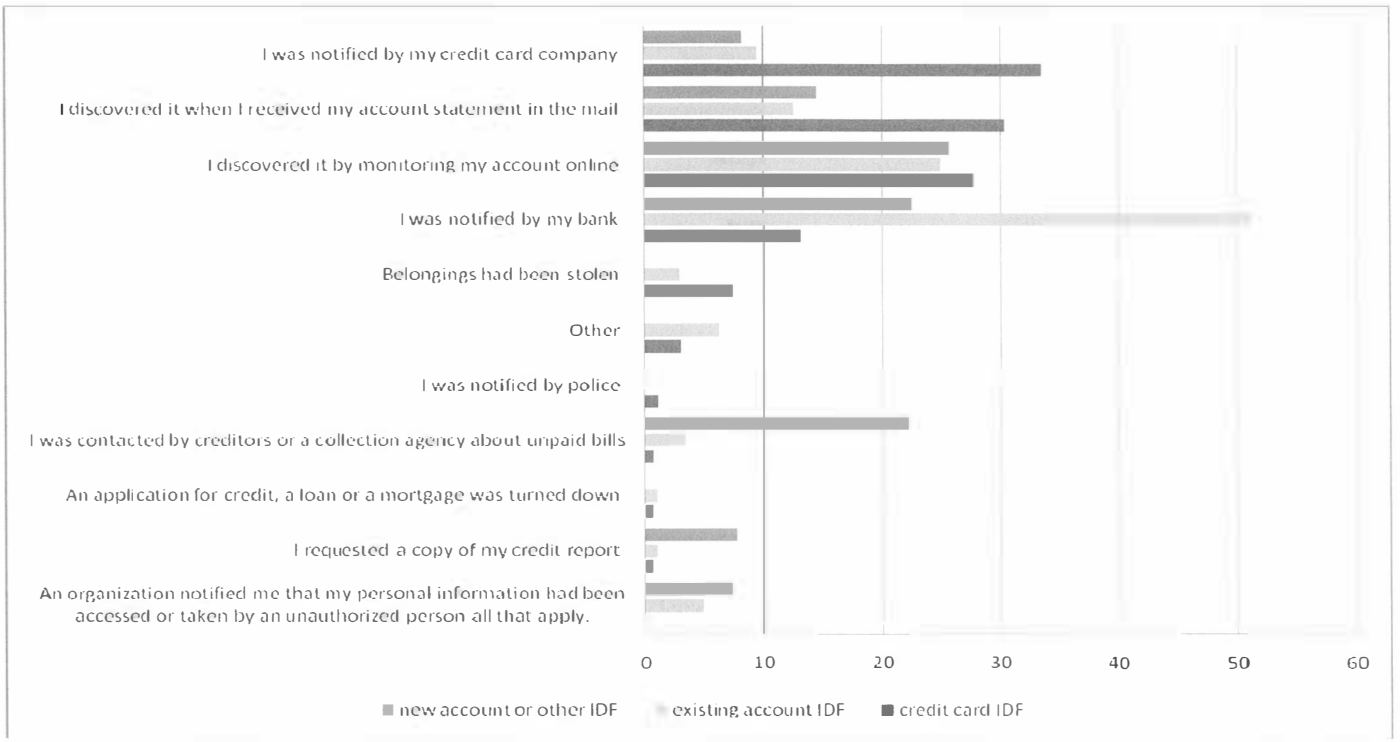


Figure 1 – Method of detection (% of cases)

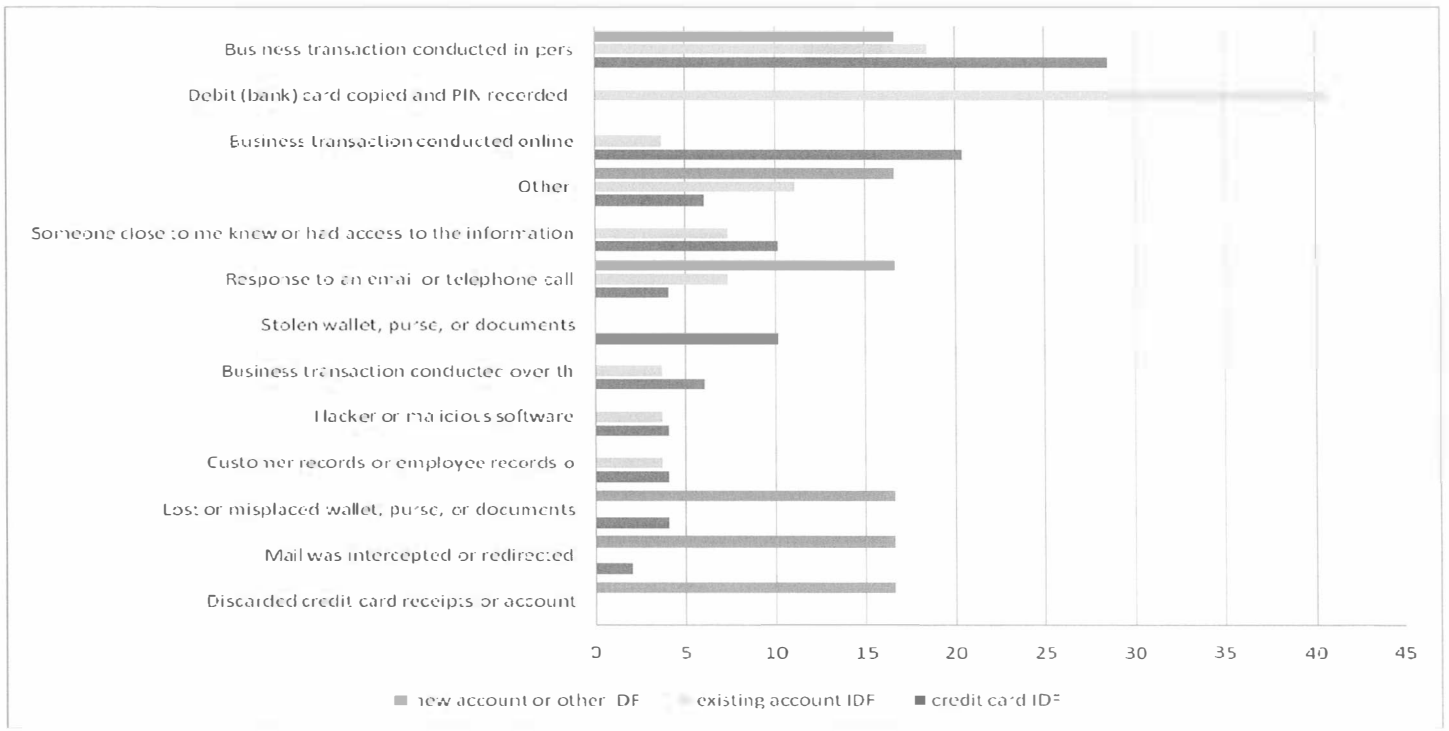


Figure 2 – How do you think the information was accessed or taken? (% of cases)

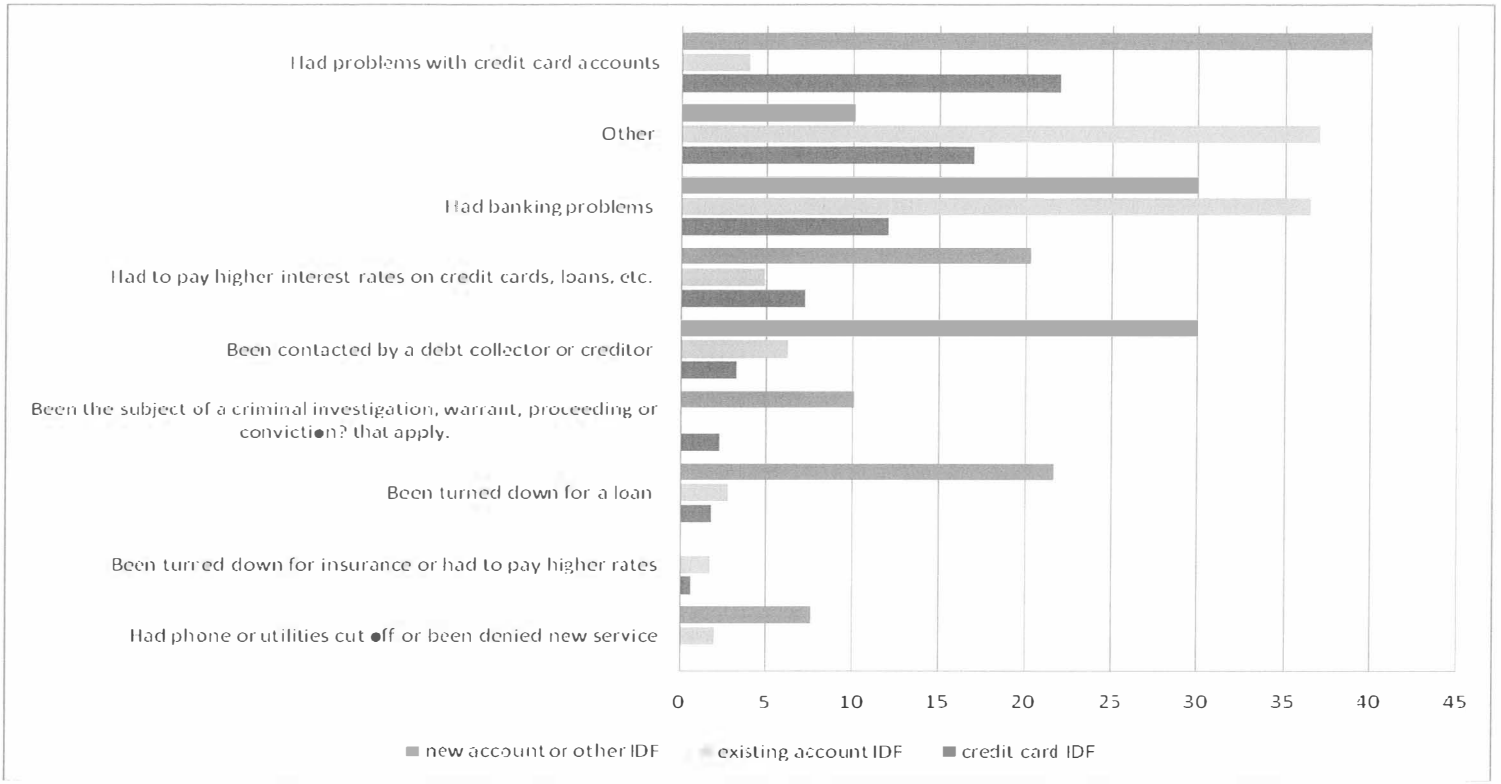


Figure 3 – Other costs (% of cases)

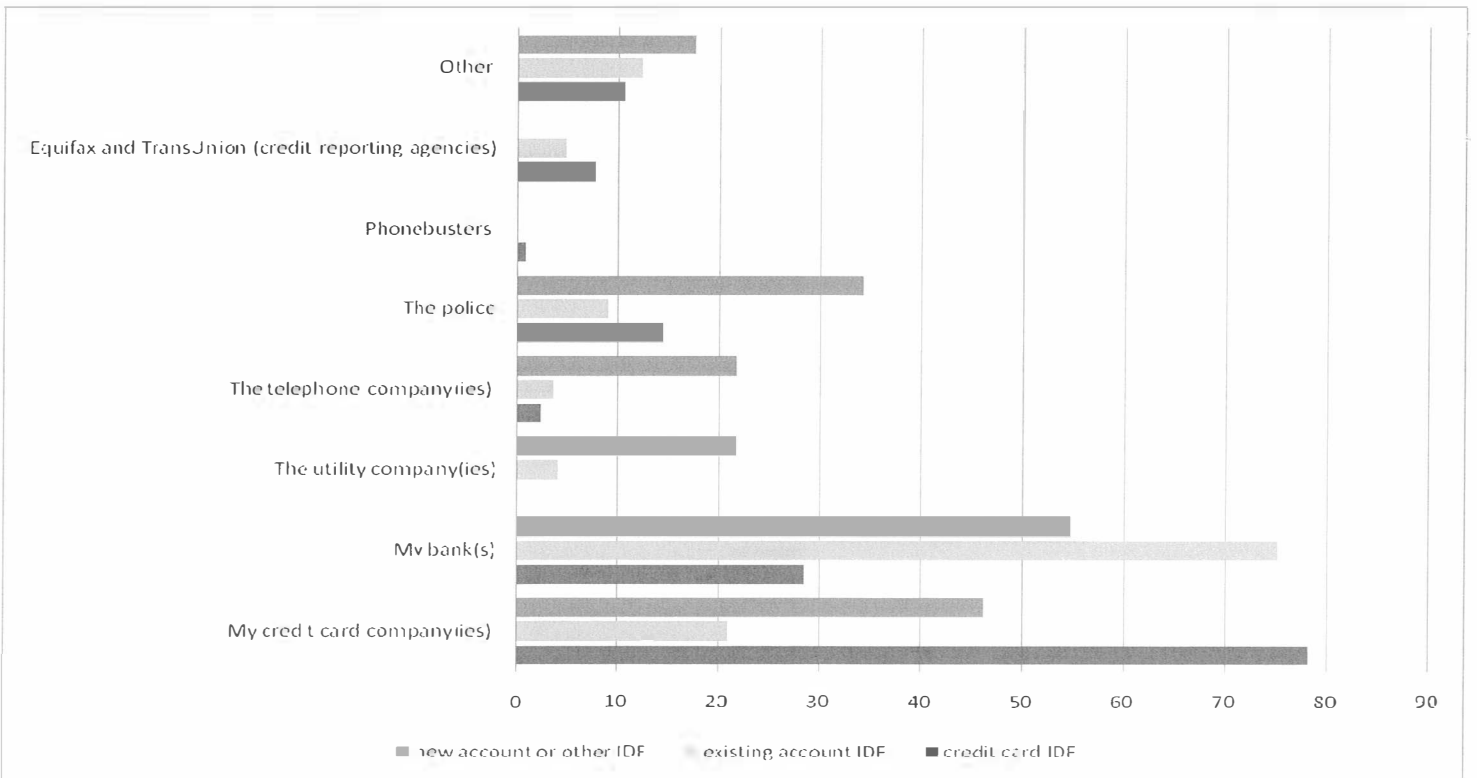


Figure 4 – Reporting (% of cases)

17.0 APPENDIX D – GLOSSARY

(References for the Glossary appear at the end of this Appendix.)

account-hijacking
"the assumption of a customer's identity on a valid existing account" (FDIC 2004)
Also known as "account takeover"

'account level' breach
"the compromise of a consumer name in connection with a credit card account number and possibly additional information such as expiration date of the account and CVS number (Card Verification System)" (ID Analytics 2006).
See also 'identity level' breach

account origination
the process of identification authentication and the issuance of unique identifiers (identification numbers, passwords, PINs, documents, tokens, etc.) when a person first establishes a relationship with a business or organization (FFIEC 2005).
Also known as "enrollment".

account takeover
"the assumption of a customer's identity on a valid existing account" (FDIC 2004)
Also known as "account-hijacking"

authentication
1. "the process of validating and verifying a claimed identity. This includes: establishing that a given identity exists; establishing that a person is the true holder of that identity; and enabling the genuine owner of the identity to identify themselves for the purpose of carrying out a transaction …" (Cabinet Office July 2002)
2. "the process of verifying the identity of a person or entity. Authentication is typically dependent upon customers providing an "identifier" such as an identification card or an identification number followed by one or more authentication factors, or credentials, to prove their identity." (FFIEC 2005)
3. "the techniques, procedures and processes used to verify the identity and authorization of prospective or established clients." [15]
4. "authentication" for the purpose of identification documents is the testimony of a court certified document examiner, or in some cases the manufacturer, that a document is genuine and unaltered (Lyons 2006)
See also "authentication factor", "multi-factor authentication", "single-factor authentication" and "credentials management"

authentication factor
secret or unique information linked to a specific customer identifier that is used to verify that customer's identity. There are three types of authentication factors:

[15] Canadian Payments Association - Risk Guide, http://www.cdnpay.ca/news/pdfs_news/Risk%20Guide.pdf

- Something a person knows – commonly a password or PIN (see shared secrets)
- Something a person has – most commonly a physical device referred to as a token
- Something a person is – most commonly a physical characteristic, such as a fingerprint, voice pattern, (etc.)…This type of authentication is referred to as biometrics (FFIEC 2005)

See also "multi-factor authentication" and "single-factor authentication"

biometrics
a group of authentication factors based on physiological or physical characteristics

breeder document
a document, such as a birth certificate, that is used by an identification issuer to establish the identity of an applicant

corporate identity theft
the unauthorized collection, transfer, replication or manipulation of a business's identifying information for the purpose of committing fraud or other crimes. (A business's identifying information can include its name, address, telephone number, corporate credit card information, bank account information, tax identification numbers, employer identification numbers, e-business Web sites, URL addresses, articles of incorporation and company profile.). Additional information on corporate identity theft can be found in the following sources:

- Bunton, C. (2005) Corporate ID theft - is your company vulnerable? **Strategic Direction** 21(2):3-4
- Collins, J.M. (2003) Business Identity Theft: The Latest Twist. **Journal of Forensic Accounting** IV: 303-306
- Smiley, N. (2004) Corporate Fraud: Identity Theft with a Difference. **Law Pro** June:8-10
- Sullivan, B. (2004) Fake companies, real money. **MSNBC**

Also known as commercial identity theft or business identity theft

credentials management
"authentication of the identity of parties accessing data." (Spiotto 2003)
Also known as "authentication"

credit alert
"an alert that ... credit reporting agencies attach to your credit file. When you, or someone else, attempts to open a credit account the lender should contact you by phone to verify that you want to open the new account. If you cannot be reached by phone, the credit account should not be opened. However, a creditor is not required by law to contact you if you have fraud alert in place. Fraud alerts can legally be ignored by creditors."[16]
See also "credit freeze"

[16] Equifax Web site, http://www.equifax.com

credit freeze
"a security freeze that is placed on a consumer's credit file to prevent the file from being shared with anyone, thus forestalling new accounts from being opened in the consumer's name." (Javelin 2007)
See also "credit alert "

data breach
an instance when personal information contained in a set of paper records or an electronic database is compromised by theft, loss or unauthorized intrusion. Breaches can be classified as account-level or identity level (ID Analytics 2006)
Also known as "security breach" or "privacy breach"

document breeding
the process of using one or more identity documents to apply for and receive additional documents in the same name

Domain Name Service (DNS) poisoning
a method of collecting personal information by misdirecting consumers to a fraudulent World Wide Web site. The consumer types in the correct URL, however the criminal has surreptitiously changed some of the address information that Internet Service Providers store to speed up Web browsing (Liberty Alliance 2005)
Also known as "pharming"
See also "redirector"

dumpster diving
a method of collecting personal information by searching through trash; "the information found in this way may be used to access accounts and perform account maintenance" (Liberty Alliance 2005).

encrypted payload
"encryption of portions of transmitted data, while leaving headers and non-confidential data as plain-text" (Liberty Alliance 2005).

encryption
"any procedure used in cryptography to convert plaintext into cipher-text in order to prevent any but the intended recipient from reading that data" (Liberty Alliance 2005).

enrollment
1. the process of introducing people into a biometric-based system…Samples of data from one or more physiological or physical characteristic are taken, …converted into a mathematical model or template …and registered in a database" (FFIEC 2005).
2..describes the process of identification authentication and the issuance of unique identifiers (identification numbers, passwords, PINs, documents, tokens, etc.) when a person first establishes a relationship with a business or organization.
Also known as "account origination".

evil twin
"a wireless network that pretends to offer trustworthy Wi-Fi connections like the kind commonly found in local coffee houses, airports and hotels, but is actually a ruse designed to steal the consumer's passwords and credit card numbers" (Liberty Alliance 2005).

fictitious identity
a false identity that is not based on a real person's personal information.
Also known as a "synthetic identity".

hacking
"obtaining unapproved access into an organization's computer systems, databases or intranet to steal confidential information" (Liberty Alliance 2005).

identity crime
"offenses involving the use of a false identity" (ACPR 2004)

identity harvesting
a term that can be used for the collection of personal information when a method targets a group of people. This would include methods such as hacking, insider access, phishing, pharming, etc.

identity information
information that is unique to an individual or that can be used alone or in combination with other information to identify an individual or to allow access to goods, services, locations or benefits.
Also known as "personal information" or "means of identification".

'identity level' breach
the compromise of a consumer name in connection with a Social Security Number (US) or Social Insurance Number (Canada), and possibly address, date-or-birth, or associated phone numbers as well (ID Analytics 2006)
See also 'account level' breach

identity manipulation
the alteration of one's own identity (ACPR 2004)

identity theft
the unauthorized collection, possession, transfer, replication or other manipulation of another person's personal information, and/or identification documents, for the purpose of committing fraud or other crimes that involve the use of a false identity (Sproule and Archer 2007).

insiders
employees or other participants in transactions or with authorization to access systems and/or places where personal information is stored

keyboard loggers

"a piece of software that is designed to permit an attacker to record all the keystrokes that are made on a PC keyboard and upload the information to another location" (Liberty Alliance 2005)

loggers (keyboard)
"a piece of software that is designed to permit an attacker to record al the keystrokes that are made on a PC keyboard and upload the information to another location" (Liberty Alliance 2005)

'man in the middle'
"an attack in which a perpetrator is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised" (Javelin 2007)

means of identification
"any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual" (1998)
Also known as "personal information" or "identity information "

multi-factor authentication
1. a process that uses two or more authentication factors to verify customer identity.
2. "Combining two or more authentication techniques together to form a stronger, more reliable level of authentication. This usually involves combining two or more of the following types:
   - Secret – something the person knows
   - Token – something the person has
   - Biometric – something the person is " (Liberty Alliance 2005)

mutual authentication
a process whereby customer identity is authenticated and the target Web site is authenticated to the customer (FFIEC 2005).

one-time-password (OTP)
a unique pass-code generated by an electronic password-generating token or contained on a scratch card. OTP tokens are often used in multi-factor authentication schemes (FFIEC 2005)..

out-of-band authentication
"any technique that allows the identity of an individual to be verified through a channel different from the one the (individual) is using to initiate the transaction" (FFIEC 2005).

personal information
information that is unique to an individual or that can be used alone or in combination with other information to identify an individual or to allow access to goods, services, locations or benefits.
Also known as "identity information" or "means of identification"

personally identifiable information
"in information security and privacy, any piece of information which can potentially be used to uniquely identify, contact, or locate a single person." [17]
Also known as 'personal identifying information'

pharming
a method of collecting personal information by misdirecting consumers to a fraudulent WWW site. The consumer types in the correct URL, however the criminal has surreptitiously changed some of the address information that Internet Service Providers store to speed up Web browsing (Liberty Alliance 2005).
Also known as "Domain Name Service (DNS) poisoning".

phishing
1. "the act of sending an email to a user falsely claiming to be an established legitimate enterprise, in an attempt to scam the user into surrendering private information, that will be used for identity theft."[18]
2. "criminals' creation and use of e-mails and websites--designed to look like e-mails and websites of well-known legitimate businesses, financial institutions, and government agencies--in order to deceive Internet users into disclosing their bank and financial account information or other personal data such as usernames and passwords"[19]
See also: "vishing", "smishing", "pharming", "spear phishing "

pretexting
"the collection of information about an individual under false pretenses (the "pretext"), usually done over the phone, such a calling a bank while posing as a customer to find out personal information" (Javelin 2007)

privacy breach
an instance when personal information contained in a set of paper records or an electronic database is compromised by theft, loss or unauthorized intrusion. Breaches can be classified as account-level or identity level (ID Analytics 2006)
Also known as "security breach" or "data breach".

redirector
"Crimeware code which is designed with the intent of redirecting end-users' network traffic to a location where it was not intended to go. This includes crimeware that changes hosts files and other DNS specific information, crimeware browser-helper objects that redirect users to fraudulent sites, and crimeware that may install a network level driver or filter to redirect users to fraudulent locations."[20]
See also "pharming", "DNS poisoning"

---

[17] Wikipedia, http://en.wikipedia.org/wiki/Personally_identifiable_information
[18] Canadian Payments Association - Risk Guide, http://www.cdnpay.ca/news/pdfs_news/Risk%20Guide.pdf
[19] United States Department of Justice, http://www.usdoj.gov/criminal/fraud/docs/phishing.pdf
[20] Anti-phishing Working Group, http://www.antiphishing.org

Secure Sockets layer (SSL)
"the leading security protocol on the Internet. Developed by Netscape, SSL is used to do two things:

- Validate the identity of a Web site, and
- Create an encrypted connection for sending data" (Liberty Alliance 2005)

security breach
an instance when personal information contained in a set of paper records or an electronic database is compromised by theft, loss or unauthorized intrusion. Also known as privacy breach or data breach. Breaches can be classified as account-level or identity level. (ID Analytics 2006)

shared secrets
information elements that are known or shared by both the customer and the authenticating entity (FFIEC 2005)

shoulder surfing
a method of collecting PINs, user IDs, passwords or other personal information by eavesdropping, looking over someone's shoulder or otherwise standing in close proximity as they operate an ATM, telephone, computer or other data collection equipment.

single-factor authentication
a process that uses only one authentication factor to verify the identity of a customer. An example is the use of a password to gain access to a computer system or Web site. *See also "multi-factor authentication"*

skimming
"The act of producing unauthorized copy of an electronic security device while it is being used for its intended purpose. Note: Originally, skimming meant making an illegal copy of a credit card or a bank card when the original was being used correctly. Typical methods of skimming involve use of a modified reader that reads and stores all the information that the original card contains." [21]

smishing
"a version of phishing sent by SMS messaging (text messaging) which sends a cell phone message that directs victims to a Web site that downloads malicious spyware (Trojan Horse) onto the victim's cell phone or computer" (Javelin 2007).

social engineering
a method of collecting personal information that involves exploiting human nature; "often (an identity thief) gets information by simply asking for it, pretending that they are someone in authority who has a right to get it or to gain access to something" (Liberty Alliance 2005).

---

[21] ATIS Telecom Glossary 2000, http://www.atis.org/tg2k/_skimming.html

spear phishing
the technique of using harvested personal information to mount more convincing phishing attacks on users
See also "phishing".

spyware
"computer software that collects personal information about users without their informed consent."[22]

synthetic identity
a false identity that is not based on a real person's personal information.
Also known as a "fictitious identity".

token
a physical device that may be part of a multi-factor authentication scheme. Examples are ABM cards, USB token devices, smart cards, password generating tokens (FFIEC 2005).

Transport Secure Layer (TSL)
"a security protocol from the (Internet Engineering Task Force) IETF that is based on the Secure Sockets Layer (SSL) 3.0 protocol" (Liberty Alliance 2005)

validation
1. the process of determining that a specific identifier exists (Cabinet Office July 2002)
2. "a process that determines if data (e.g. address, phone, and SSN) are real. At this level there are two concerns:
- Do the specific personal identifiers , e.g. address, phone and SSN, exist?
- Are the elements in the appropriate format as identified by the issuer of the data (e.g. driver's license number and social security number)?" (Gordon and Willox 2005)

3. "validation" for the purposes of identification documents is the process of adding the legal attribution and registration number by the document issuer to the surface of a genuine identification document blank at the time of issue. The act of "bringing an genuine identification document blank into being" (Lyons 2006)

verification
1. the process of determining that a specific identifier belongs to the person who is presenting or claiming it as their own (Cabinet Office July 2002).
2. "a related but separate process from that of authentication. Customer verification complements the authentication process and should occur during account origination. Verification of personal information may be achieved in three ways:
- Positive verification to ensure that material information provided by the applicant matches information available from trusted third party sources…
- Logical verification to ensure that information provided is logically consistent (e.g. do the telephone area code, ZIP code and street address match).

[22] Wikipedia, http://en.wikipedia.org/wiki/Spyware

- Negative verification to ensure that information provided has not previously been associated with fraudulent activity…" (FFIEC 2005)

3. "a process that determines if data belong together and determines if information supplied is the best available information.
   - As an example, can the name, address, telephone, and SSN be confirmed together in multiple databases? through parallel searching/matching?
   - Are there keying errors?
   - Is data accurate based on best available data?" (Gordon and Willox 2005)

4. "verification" for the purpose of identification documents is the process of confirming with the identification document issuer that a document was issued to a person with the personal identifiers and registration number provided" (Lyons 2006).

vishing
"a version of phishing that uses a combination of email and the telephone, or just telephone; the victim is urged to resolve an account issue by a criminal posing as a financial institution, and is thereby prompted to provide personal information" (Javelin 2007)

wardriving
"finding and marking the locations and status of wireless networks" (Liberty Alliance 2005)

REFERENCES FOR GLOSSARY

(1998). Identity Theft and Assumption Deterrence Act. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_public_laws&docid=publ318.105

ACPR (Australasian Centre for Policing Research) (2004). Standardization of Definitions of Identity Crime Terms - Discussion Paper, Prepared by the ACPR for the Police Commissioners' Australasian Identity Crime Working Party and the AUSTRAC POI Steering Committee. http://www.acpr.gov.au/pdf/Standdefinit.pdf

Cabinet Office (July 2002). Identity Fraud: A Study. UK Cabinet Office. http://www.identitycards.gov.uk/downloads/id_fraud-report.pdf

FDIC (Federal Deposit Insurance Corporation) (2004). Putting an End to Account-Hijacking Identity Theft, Federal Deposit Insurance Corporation. http://www.fdic.gov/consumers/consumer/idtheftstudy/index.html

FFIEC (2005). Authentication in an Internet Banking Environment. Arlington, VA, Federal Financial Institutions Examination Council. www.ffiec.gov/pdf/authentication_guidance.pdf

Gordon, G. R. and N. A. Willox, Jr, (2005). Using Identity Authentication and Eligibility Assessment to Mitigate the Risk of Improper Payments. Utica NY, Economic Crime Institute of Utica College. http://www.utica.edu/academic/institutes/cimip/publications/papers.cfm

ID Analytics (2006). National Data Breach Analysis, ID Analytics Inc.: 2-36.

Javelin (2007). 2007 Identity Fraud Survey Report: Identity Fraud is Dropping, Continued Vigilance is Necessary. Pleaseanton, CA, Javelin Strategy and Research. http://www.javelinstrategy.com/uploads/701.R_2007IdentityFraudSurveyReport_Brochure.pdf

Liberty Alliance (2005). Liberty Alliance Glossary: Identity Theft Primer, Liberty Alliance Project. http://www.projectliberty.org/resources/Glossary_Id_Theft_Primer.pdf

Lyons, J. (2006). Threats of the new millenium: Policing identification-based crime. Blue Line Magazine. **November:** 8-11.

Spiotto, A. H. (2003). "Financial Account Aggregation: The Liability Perspective." *Fordham Journal of Corporate and Financial Law* Vol. **8**(2): pp. 557.

Sproule, S. and N. Archer (2007). Defining Identity Theft. Eighth World Congress on the Management of eBusiness (WCMeB 2007), Toronto, IEEE. http://ieeexplore.ieee.org/iel5/4285290/4285291/04285319.pdf

McMaster University

MeRC

McMaster eBusiness Research Centre

McMaster eBusiness Research Centre (MeRC)
DeGroote School of Business
McMaster University
1280 Main St. W. MGD A201
Hamilton, ON
L8S 4M4

Tel: 905-525-9140 ext. 23950
Fax: 905-528-0556
Email: ebusiness@mcmaster.ca
Web: http://merc.mcmaster.ca