MeRC

McMaster eBusiness Research Centre

MEASURING IDENTITY THEFT IN CANADA: 2006 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. 21

January 2008

MEASURING IDENTITY THEFT IN CANADA: 2006 CONSUMER SURVEY

By

Susan Sproule and Norm Archer

MeRC Working Paper #21

January 2008

DeGroote School of Business

McMaster University

Hamilton, Ontario, L8S 4M4

Canada

sprouls@mcmaster.ca

archer@mcmaster.ca

NOTE: The Appendices referred to in this document contain tables and figures with detailed information from the 2006 consumer survey. The appendices are available on request from the authors at archer@mcmaster and sprouls@mcmaster.

EXECUTIVE SUMMARY

This is a report on a national analysis of consumer identity theft and fraud in Canada, undertaken in late 2006 by McMaster University's DeGroote School of Business, on behalf of the Ontario Research Network for Electronic Commerce (ORNEC). ORNEC is funded by the Ontario Research and Development Challenge Fund in partnership with the Universities of Ottawa, McMaster, Carleton and Queen's and leading corporate partners, and is the focal point and driving force for electronic commerce research in Ontario, Canada and internationally.

The survey was conducted through an Internet panel by OpenVenue, a professional market research firm. OpenVenue provided 1,500 of the sample from their frame of 400,000 Internet users sourced from the Sympatico.MSN.ca portal. They sub-contracted the remaining portion of the sample from a panel partner. The total number of responses was 3550. Respondents were screened to make sure that every respondent was 18 years or older and had at least one credit card and bank account. The sample was targeted to be representative of the Canadian population (excluding Quebec since the survey was available only in English) on gender, age and four geographic regions. There were no targets or quotas on questionnaire completion.

After removing respondents who had more than two inconsistent responses to the survey, the corrected sample size was 3539. 1710 of these respondents reported at least one incident of identity theft (IDT) or identity fraud (IDF) against themselves or someone in their immediate family in the previous five years.

There were five sections in the survey

- Part 1 – Defining identity theft and identity fraud
- Part 2 – Incidence rates
- Part 3 – Characteristics of identity theft and identity fraud
- Part 4 – Concerns about identity theft and identity fraud
- Part 5 – Attitudes towards preventative measures

A detailed methodological review and statistical analysis was performed on the data. These appear in detail in the report. Although a number of the findings have been omitted for brevity, here are the main findings from the survey:

Part 1 - Defining Identity Theft and Identity Fraud

Before giving any definition of identity theft or fraud, respondents were presented a list of 13 scenarios, and asked to indicate which scenarios were cases of identity theft. All of these scenarios were indicated by at least some respondents to be cases of identity theft, including three that would not normally be classed as identity theft or fraud. In general, financial and stranger frauds were perceived to be cases of identity theft or fraud more often than non-financial and friendly frauds. There did not appear to be a pattern as far as whether the case described a theft only, a fraud only or both theft and fraud. There also did not seem to be a pattern with respect to account-level versus identity-level theft or fraud. (Because accounts can be closed and new

accounts created, the damages resulting from a breach or theft involving only account-level information are generally smaller than those associated with identity-level breaches or thefts.) Our conclusion is that consumers tend to think about identity theft and identity fraud as a combination that has come to mean approximately the same thing.

Part 2 Incidence Rates

We designed the question on incidence rates to capture information about five classifications of IDT or IDF. These classifications are:

- Frauds involving existing credit card accounts
- Frauds involving other existing accounts (i.e. bank accounts, phone or utility accounts, etc.)
- Frauds involving new accounts (i.e. credit card accounts, bank accounts, phone or utility accounts, etc.)
- Other types of frauds (i.e. government benefits, tax fraud, leases, impersonation, etc.)
- Theft of personal information, when a fraud has not, or not yet, been committed.

Incidence Rates for Individual Consumers

The five classifications described above are non-exclusive. An incident of IDF may involve more than one type of these frauds. In order to compare our incidence rates to those from recent U.S. surveys, cases were assigned to three exclusive categories according to the most serious type of fraud. We also needed to establish the individual, rather than the family, as the unit of analysis. In some cases we know that the respondent was a victim of IDF at some point in time, but we do not know if he or she was the victim in the case being described. In other cases, we know that the respondent was the only victim in the family. As a result, we arrive at a range rather than a single figure in each category as shown below.

Incidence Rate for Individual Consumers – In The Most Recent Year

IDT or IDF Category	ORNEC		FTC 2003	Javelin 2004	Javelin 2005	Javelin 2006
	Minimum	Maximum				
Existing credit card fraud	2.0%	3.2%	2.4%		All existing accounts	2.1%
Other (non-credit card) accounts fraud	1.2%	2.8%	0.7%		2.5%	0.6%
New accounts or other fraud	0.8%	3.1%	1.5%		1.5%	1.1%
Total	4.0%	9.1%	4.7%	4.3%	4.0%	3.7%
Sample size (N)	3,539	3,539	4057	4000	5000	5000+

Except for other (non credit-card) accounts frauds, the rates from the US studies fall between our minimum and maximum values. However, they are generally much closer to our minimum values. Our incidence rates therefore seem to be higher than those reported in any of the US studies. This includes comparisons with other US surveys also discussed in the main body of this

report. There are two possible reasons for these differences that are related to our methodology:

1. Although the reasons are not clearly understood at the present time, reported rates from Internet surveys tend to be higher than those on telephone surveys (the U.S. surveys were all telephone interviews using Random Digit Dialing). There is no conclusive evidence of which is the most accurate survey method, but differences appear in responses from online surveys that usually lead to higher incidence rates compared to telephone interviews. For example, in August 2006, Gartner conducted a survey using an online Internet panel. The sample size was 5000. They reported an incidence rate that was 1.51 times greater than the FTC 2003 phone survey results of a similar sample (15 million American victims in the last 12 months versus 9.9 million). If we take the 2003 FTC total incidence rate of 4.7% and multiply it by 1.51, we get 7.1%, which is close to the mid-range between (4.0% and 9.8%) found in our study.

2. In addition to the differences between online and phone surveys, the inclusion of the 13 scenarios listed in the first part of the survey may have made certain types of IDT and IDF more salient in the minds of our respondents than is the case in the other surveys. Scenarios such as misappropriation of eBay accounts, someone using your email account, fraudulent phone charges and others, especially when committed by a family member or friend, may not have come to mind in the other surveys.

Costs of Identity Fraud in Canada

Using the same methodology as above, but with fraud amounts, victim's hours to resolve, and out-of-pocket costs estimated by victims of fraud, we calculated the lower and upper limits of the annual cost of identity fraud to Canadian consumers. Note that this does not include related costs to businesses and governments, such as costs incurred preventing, detecting and responding to IDT and IDF.

Annual Costs of Identity Fraud to Canadian Consumers

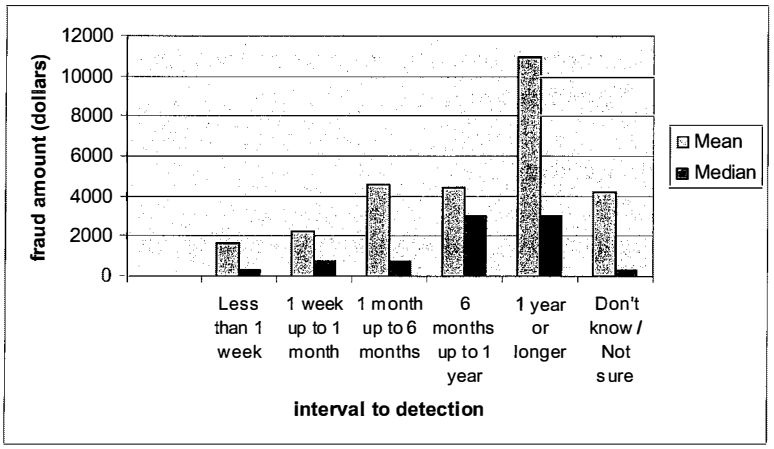
		Minimum	Maximum
Number of victims (last 12 months)	Percent of population	4.0%	9.1%
	Projected number of victims in Canada	993,672	2,260,603
Fraud amount	Mean amount per victim	$2947	$3188
	Total	$2,928,351,384	$7,206,802,364
Victim's hours to resolve	Mean hours per victim	18	23
	Total	17,886,096	51,993,869
Out-of-pocket costs	Mean cost per victim	$165	$396
	Total	$163,955,880	$895,198,788

From the table we see that there are over 1 million victims of IDF each year and the amount that perpetrators gain from IDF victims in Canada is over $3 billion. Dealing with identity frauds costs Canadian victims $164 million of their own money and they collectively spend over 18 million hours a year to resolve these problems.

Part 3 Characteristics of Identity Theft and Identity Fraud

In 42% of the cases, the method by which the information was accessed is known. In another 15% the victim may not know for certain, but has a suspicion, of how the information was obtained. The results compare well with US survey data. For frauds involving new accounts and existing (non credit card) accounts, the information was most frequently reported to be taken from the home (30.2% and 32.6% respectively). Where credit card fraud was reported, the information was most frequently taken during an in-person business transaction (22.4% of cases) or from a stolen wallet or purse (20.2% of cases).

Information was also gathered and analyzed on the method of detection and the interval from actual information access or theft to the time it was discovered. More than half of the cases were detected within a month of the theft. However, there are a substantial group of victims (12.7%) who are not sure when the theft occurred. There is a significant relationship between the interval to detection and the average fraud amount. as illustrated in the Figure below.



Interval to Detection and Average Fraud Amount

In 35% of the reported cases, the victim knew something about the perpetrator of the theft or fraud. This result is similar to results found in other surveys, as shown in the following table.

Awareness of the Perpetrator – Comparison to Other Studies

	Other Surveys					ORNEC 2006
	FTC 2003	Javelin 2004	Javelin 2005	Javelin 2006	NCVS 2004	
Awareness of who	26%	unknown	36%	31%	unknown	35%

In general, victims are not as likely to know the identity of the perpetrator when the frauds involve credit cards (only 30.7%) and when a theft only has occurred (26.0%). They are more likely to know the identity of the perpetrator when the frauds involve new accounts (47.1 percent of cases), existing accounts (44.2%) and other frauds (41.7%).

Of the 35% of the cases where the perpetrator was known: 25.9% were a relative; 13.5% a corrupt employee of a firm where the victim did business; 13.1 were a friend or roommate, and 11.6% were a complete stranger.

The most common type of fraud experienced was purchases made on an existing credit card account (48.7% of the cases), followed by money taken from an existing bank account (24% of the cases) and cases where there had been no frauds discovered to date (12% of the cases). The remaining frauds each were experienced in less than 10% of the total fraud cases.

Document breeding refers to the practice of using one type of identification document to apply for another type of document (e.g. a birth certificate used to obtain a passport). Some form of document breeding is known to have occurred 3.5%of the cases. Driver's licenses are the most common breeder document acquired or counterfeited, appearing in two thirds of the cases where document breeding occurred, and social insurance cards and health cards were acquired in a third of the cases of known document breeding.

Sixty-five percent of victims know what information was obtained In 61% of these cases only account level information was obtained. Our results show that the costs of the IDF are highest when both identity level and account level information is obtained. The difference is most evident when we look at victim costs (both time to resolve and out-of-pocket costs). When both identity and account level information is accessed, the victim's costs in both time and money are more than three times the costs when just account level information is accessed.

The median amount gained by the perpetrator (fraud amount) was $595. Victims spent a median of 8 hours and $4 to resolve the problems. In almost half the cases the victim reported no out-of pocket costs. However, if we eliminate cases where there was only credit card fraud, victims' costs rise significantly to 12 hours and $18..

Almost half of the victims reported the fraud to a credit card company and almost 40% reported it to their bank. Surprisingly, while 32% reported to the police, only 2% reported to PhoneBusters (the RCMP and OPP's fraud call centre). This would indicate that either the police departments are not referring people to PhoneBusters or that victims do not make the call even after a referral.

Between 10 and 20 percent of respondents were unsure if the IDF misuse had stopped (18.1%) or if all problems had been resolved (10.1%). These results indicate that there is lingering anxiety over the IDF even when it has been detected and initial actions taken. In 23% of cases, the victim believed that the misuse of their identity was ongoing. 14% believed that the misuse had stopped, but did not believe that they had resolved all of the problems associated with this IDF episode.

Part 4 Concerns About Identity Theft and Identity Fraud

All respondents (not just victims of IDT or IDF) were asked how concerned they were about becoming a victim of identity theft in the future. On a five point Likert scale: 3.4% were not at all concerned; 22.9% were slightly concerned; 37.8% were somewhat concerned; 24.3% were very concerned, and; 11.7% were extremely concerned. These results are similar to those found in other similar surveys of Canadians. A comparison of those who had been victimized with

those who had not, indicated that the lowest level of concern was in the group who had experienced credit card fraud (themselves or through someone in their immediate family). This is probably because the credit card company assumes the risk in these cases. The level of concern was highest for those who had experienced new account or other frauds. As we saw from other results, this group suffered the most serious consequences in terms of costs. Their level of concern for a re-occurrence is therefore higher than others.

Two questions were used to elicit information on whether respondents had received e-mail requests for account information (commonly known as "phishing"). Just under 40% of our respondents indicated that they had received potential phishing emails. Over 95% of these respondents indicated that they had not responded to these e-mails. Unfortunately, 3.4% said that they had and 1.5% did not know whether or not they had responded. This is worrisome, as phishing continues to be a pervasive problem and phishing techniques are continuing to become more sophisticated.

Part 5 Attitudes Towards Preventative Measures

In this section 43 measures were presented that individuals, financial institutions and governments might take to prevent IDT or to minimize the impact of IDF. A Max-Diff analysis was used to rank these potential measures according to the respondent's willingness-to-act. The four highest ranking measures in decreasing rank order, indicating the respondent's willingness to take these measures, were:

- Refuse to give personal information over the phone to people that claim to do surveys, or people offering products or services at special prices.
- Use anti-virus, anti-spyware and firewall software that is updated on a regular basis on your computer
- Shred financial or important documents before discarding them
- Monitor your account balances and activity online on a regular basis

Data from the Max-Diff analysis were also used to segment the respondents according to similarities in their preferences. The preliminary segmentation analysis identified 8 segments of approximately equal size, ranging from 9% to 15% of the sample. The measures that contributed the most to segment identification were:

- Provide biometric data such as fingerprints, voice samples, or retina scans that would be used to verify your identity in association with government-issued identification documents such as passports, or driver's licenses
- Provide biometric data such as fingerprints, voice samples, or retina scans that would be used by your bank to authenticate your identity when using a 'smart' debit or credit card or when banking online.
- Reduce the amount of banking that you do online
- Reduce the amount of shopping that you do online

Initial implications from segment analysis are that different measures will have different degrees of acceptability within each of these segments, implying that approaches to introducing preventative measures must also vary among these different population segments.

Table of Contents

1. INTRODUCTION

1.1 The ORNEC identity theft program

This report has been produced for the Ontario Research Network for Electronic Commerce (ORNEC). Funded by the Ontario Research and Development Challenge Fund in partnership with the Universities of Ottawa, McMaster, Carleton and Queen's and together with leading corporate partners, 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 severe dampening effect on e-commerce.

1.1.1 Research projects

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

Defining and measuring identity theft in Canada
Each of the foregoing projects has a number of different research components. 'Defining and Measuring Identity Theft in Canada' was undertaken by researchers in the McMaster University DeGroote School of Business and is the exclusive focus of this report. It has the following major components:

1. Develop commonly accepted terminology
2. Conduct national consumer survey
3. Measure IDT in organizations
4. Describe national impact and develop an index to track this impact over time

In a paper titled Defining Identity Theft (Sproule and Archer 2007), we address the first of these components.[1] The rest of this paper reports the results from our initial consumer survey, the second of the components in Defining and Measuring Identity Theft in Canada.

1.1.2 Research partners

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)

[1] A summary of this paper can be found in Section 1.2 and at http://www.business.mcmaster.ca/IDTDefinition/defining.htm.
A copy of the paper is available upon request from Norm Archer (archer@mcmaster.ca).

- Canadian Imperial Bank of Commerce (CIBC)
- TD Canada Trust
- Bell Security Solutions

Other interested parties who 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)

1.2 Defining identity theft and identity fraud

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) and at http://www.business.mcmaster.ca/IDTDefinition/defining.htm.

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 IDF 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 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, we need to evaluate stronger authentication processes that will recognize and defend against someone using a false identity.

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

The rest of this paper describes the consumer survey that was conducted to give us some insight into the incidence and characteristics of IDT and IDF in Canada.

2. THE 2006 ORNEC CONSUMER SURVEY

The primary purpose of the 2006 survey was to determine the incidence and characteristics of IDT and IDF in Canada. Similar studies have been conducted in the United States since 2003. While the Canadian and American economies and their respective institutions are similar in many ways, there are some differences that could have an impact on how the problems of IDT and IDF develop within the two countries. Some of these differences include:

- Privacy legislation in the US is introduced on a sector by sector basis, whereas Canada has broader privacy legislation in place.
- The United States has introduced laws specific to IDT and IDF to its criminal code (1998). Canada is just now looking at and adopting amendments to include sanctions for certain IDT activities in the existing criminal code.
- While Canada moved to limit use of Social Insurance Numbers in the 1970s, the United States continues to use Social Security Numbers as identifiers in all kinds of commercial and institutional applications.
- Canada was a leader in debit card introduction and use.
- Canadian consumers lag behind their US counterparts in the adoption of e-commerce.

Throughout this report we will compare the findings from our 2006 survey to American studies conducted by the Federal Trade Commission (FTC) in 2003, Javelin Strategy and Research in 2004, 2005 and 2006, and the National Crime Victimization Survey conducted by the US Department of Justice in 2004. In general, we find incidence rates that are higher than those reported in the American surveys. This is discussed in detail in Section 7. Overall, however, there appear to be few differences in the nature and characteristics of IDT and IDF between the two countries

3. METHODOLOGY

There were five sections to the consumer survey:

Part 1 – Defining identity theft and identity fraud (See Section 6 of this paper)
Part 2 – Incidence rates (See Section 7 of this paper)
Part 3 – Characteristics of identity theft and identity fraud (See Section 8 of this paper)
Part 4 – Concerns about identity theft and identity fraud (See Section 9of this paper)
Part 5 – Attitudes towards preventative measures (See Section 10 of this paper)

Parts 1, 4 and 5 posed questions for the general population regarding their perceptions and concerns about IDT and their attitudes towards a variety of measures that can be taken by individuals and organizations to reduce the risks of IDT.

In Part 2, we determined whether our respondents or someone in their immediate family had been a victim of IDT or IDF. When the response in Part 2 was positive, Part 3 questions elicited descriptions of the characteristics of the theft or fraud and its impact on the victims.

Part 5 was designed to use a form of conjoint analysis called Max-Diff. Max-Diff provides "a metric representation of how the attributes are rated, by individuals and overall" (Poynter). In Part 5, respondents were shown a series of 25 screens. Each screen asked them to choose which of five different measures they were most likely to do, and which of the same five measures they were least likely to do. A sample screen is shown in Figure 1.

Please consider various measures that you might take to prevent the theft of your identity.

Considering only these 5 preventive measures, which one would you be Most Likely to Do and which one would you be Least Likely to Do?

Most Likely to Do		Least Likely to Do
○	**Use a locked mailbox for incoming mail**	○
○	**Support a requirement to use a personal identification number (PIN) every time you use your credit card.**	○
○	**Stop carrying unnecessary information or documents in your purse or wallet**	○
○	**Purchase an insurance package that would help restore financial and credit records and cover reasonable expenses if you become a victim of identity theft**	○
○	**Apply for and carry a new national multipurpose identity document that many organizations (both public and private) would accept to verify a person's identity**	○

Click the 'Next' button to continue...

Figure 1 – Sample screen for Part 5 (Max-Diff)

3.1 Pretest

Preliminary survey questions were sent to our ORNEC research partners and their comments and suggestions were implemented in the final version.

The survey was pre-tested by graduate students, other researchers, and employees of our research program partners. Two additional subjects, known to the researchers as victims of IDF, were also asked to complete the survey. The pretest was conducted through an online survey. The online survey tool used for the pretest could not accommodate the max-diff component. Instead, a series of questions were used to ask about attitudes toward the same list of preventative measures. Pretest respondents were asked to track the time that they spent completing the survey and identify any problems that they had in answering any of the questions.

Ten people completed the pretest. Four of the respondents reported that they or someone in their immediate family had been victims of IDF. The average time to complete the survey was 12.17 minutes for non-victims and 14.5 minutes for victims. Feedback from the pre-testers was incorporated into the final questionnaire (page 70).

3.2 OpenVenue

The survey was conducted by OpenVenue, a professional market research firm. OpenVenue provided 1,500 of the sample from their frame of 400,000 Internet users sourced from the Sympatico.MSN.ca portal. They sub-contracted the remaining portion of the sample from a panel partner. The total number of responses was 3550.

Respondents were screened to make sure that every respondent was 18 years or older and had at least one credit card and bank account. The sample was targeted to be representative of the Canadian population (excluding Quebec since the survey was available only in English) on gender, age and four geographic regions. There were no targets or quotas on questionnaire completion.

The survey had a 'soft launch' on Monday November 27th, with the main blast of invitations taking place on the evening of Tuesday November 28th. The survey was closed on December 8th with 3550 responses. See Figure 2.

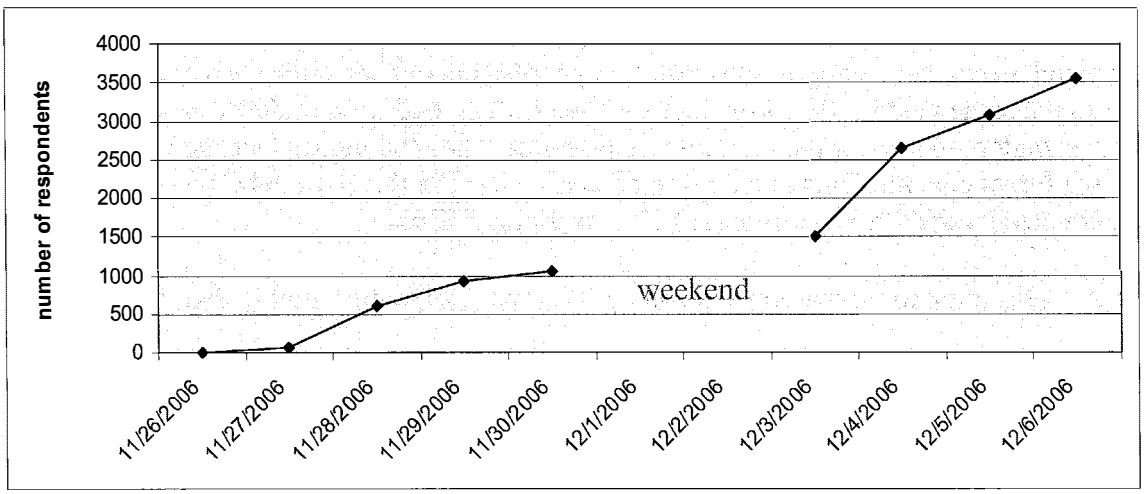


Figure 2 – Cumulative responses over survey duration

3.3 Data cleaning

Question 2 established whether the respondent or someone in his or her immediate family had ever been a victim of IDT or IDF.

Question 2 - Assume that the following general scenarios describe different types of identity theft or fraud. Have any of them EVER happened to you or to anyone in your immediate family?

- Someone used a credit card and put charges on the account without the account holder's permission (EXISTING CREDIT CARD FRAUD)
- Someone gained access to an existing account other than a credit card account – for example, a bank account or a telephone or utility account – without the account holder's permission to run up charges or to take money from the account (EXISTING (NON-CREDIT CARD) ACCOUNT FRAUD)

- Someone used personal information to impersonate you (or your family member) to obtain new credit cards or loans in your (or your family member's) name, run up debts, open other accounts, or otherwise commit theft or financial fraud. (NEW ACCOUNT FRAUD)
- Someone used personal information to impersonate you (or your family member) to gain employment, receive benefits, avoid criminal prosecution or otherwise commit fraud or some other crime. (OTHER FRAUD)
- Someone has accessed your (or your family member's) personal information without permission, although that information has not yet been used to commit frauds or other crimes. (IDENTITY THEFT ONLY)

An opportunity to conduct a validity check was available by comparing the responses to Question 2 and the responses to Question 14 (What type of frauds were attempted or committed?). There are 17 different types of fraud listed in Question 14. Each of these frauds can be matched to one or more of the types of IDF described in Question 2. See Appendix A, Table A1 for these mappings.

While we can map responses from Question 14 to Question 2, we cannot map from Question 2 to Question 14. Answers to Question 2 may reference multiple episodes of IDT and IDF. These multiple episodes may have happened to different people (i.e. to both me and someone in my family) or to the same person. Question 3 established if there had been multiple episodes and asked the respondent to answer the remaining victim questions (including Question 14) only with respect to the **latest** episode. This is the same procedure used in the National Crime Victimization Survey conducted by the US Department of Justice (Baum 2006).

Question 3 – Was there more than one episode of this type of identity theft or fraud?

[If yes] You have indicated that there have been (or may have been) multiple episodes of identity theft experienced by you or someone in your immediate family. Please answer the following questions only with respect to the LATEST EPISODE of identity theft.

We examined the questionnaire responses of the respondents whose answers to Question 14 were inconsistent with their answers to Question 2. Some people answered 'yes' to many of the frauds in question 14 even though in question 2 they had not indicated the corresponding type of IDT. We felt that respondents who were not paying enough attention to the questions should be removed from the database before any analysis.

For the case of IDT only, a respondent could have indicated in Question 14 that 'attempts' were made on various frauds, while still answering in Question 2 that no frauds had been committed. Inconsistent responses to "No frauds have been committed to date" were therefore not included in the study of inconsistencies.

In total, 316 of our 1721 victim reports had some sort of inconsistent responses to these two questions. See Figure 3. There were three respondents who checked off all of the frauds, with 16 inconsistencies. Two more had 14 inconsistencies and one had 11 inconsistencies. Another five respondents had either four or five inconsistent responses. These eleven respondents were eliminated from the database as we did not feel that they were giving sufficient care and attention

to the task. This brings our total responses to the survey down to 3539 and the number of victim reports down to 1710.

There remain 305 respondents who gave between one and three inconsistent responses. In most cases they also gave one or more consistent responses as well. Considering the complexity of the questionnaire, we did not feel justified in eliminating these responses. The respondents were obviously reporting that something had happened to them. Rather than eliminating these 305 cases, they were flagged in the data file so that we could do comparative analysis at a later time, if desired.

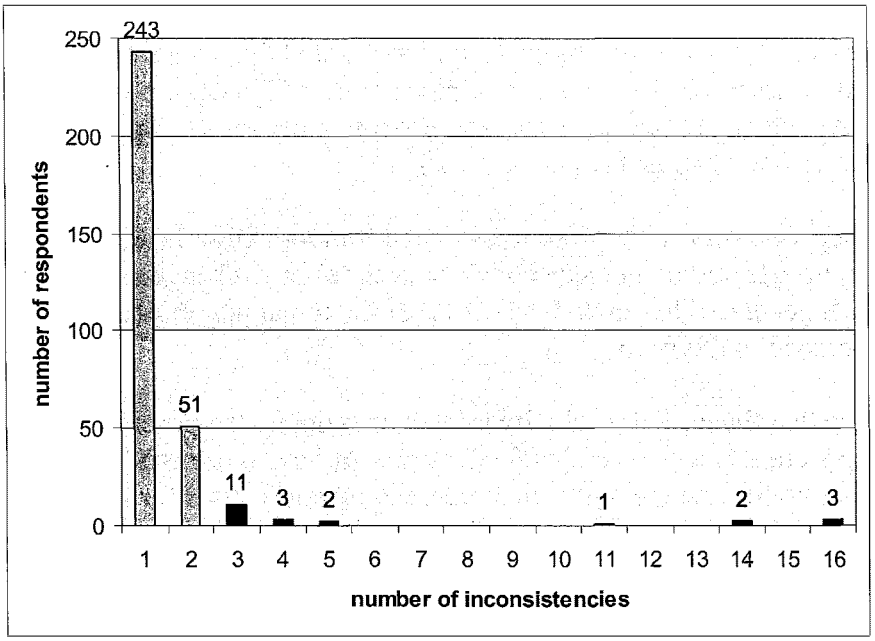


Figure 3 – Histogram of inconsistencies between Q2 and Q14
(questionnaires with more than 2 inconsistencies were removed from further analysis)

3.4 Creating subsets of responses

Further to the discussion in Data Cleaning, above, there is another caution that must be understood when examining the cases described. Answers to Question 2 show that there were often multiple cases of IDT or IDF within a family. In these cases, we do not know whether the victim of the episode described (i.e. the 'latest' episode) was the respondent or someone in his or her immediate family.

There are situations where we want to be able to look at the individual as the unit of analysis. If we include cases where either the response "this has happened to me" or the response "this has happened to both me and to someone in my immediate family" was chosen for any of the items in question 2, the number of cases is 1167. We can use this subset, called SELF_POSSIBLE, to calculate incidence rates at an individual level, as long as we are not evaluating victim demographics, imposing a timeline, or trying to determine any other characteristics of the episode being described in Questions 4 through 30. This is because, although we know that *something* happened to the respondent, we do not know if the respondent was the victim in the episode

being described (i.e. the latest episode, per Question 3). In some of these cases, the episode being described could have happened to someone in their family.

When we want to look at any of the results from Questions 4 through 30 and relate them to the respondent, we need another subset, where we know for sure that the respondent was the victim in the episode being described. We call this the SELF_VICTIM subset. The SELF_VICTIM subset contains 643 cases.

4. ONLINE SURVEYS VERSUS RANDOM DIGIT DIALING TELEPHONE SURVEYS

There are many advantages to using the Internet and the World Wide Web to conduct surveys. Marginal costs are low, so surveys can be administered to larger samples for the same cost. Large amounts and various types of information can be presented during the survey. In many cases the subject can also be assessed as he or she completes the survey. Online surveys allow for rapid collection of data and can allow researchers to economically reach respondents with relatively rare characteristics (Berrens, Bohara et al. 2003).

Professional telephone surveys use a process called Random Digit Dialing (RDD). Geographical populations can be selected by country codes, area codes or exchange codes. The actual phone numbers are then generated by random selection of the remaining digits, ensuring that unlisted numbers are included in the frame.

At the same time that the growth of the Internet is opening up the possibility of online surveys, a number of factors are making the use of RDD phone surveys more problematic. Pervasive telemarketing has contributed to a general decline in response rates for phone surveys. The increase in cellular phones and corresponding decrease in land-lines means that traditional ways of establishing geographic sampling frames are being lost. It is also becoming more time consuming and expensive to fulfill informed consent requirements during a telephone survey (Berrens, Bohara et al. 2003).

A lot of research is currently examining how online surveys differ from other types of surveys and how they can be used in applications requiring rigorous statistical analysis. However, although results from the two types of surveys tend to differ, there is no conclusive evidence as yet on which is the most accurate survey method. For a good discussion of the types of errors that can be found in surveys in general and how these types of errors apply to online surveys see Couper (2000) and Fricker, Galesic, et al (Fricker, Galesic et al. 2005). The authors observe that survey errors can be classified into non-observation errors (coverage, sampling and non-response errors) and observation errors (or measurement errors).

4.1 Coverage error

Coverage error "results from a mismatch between the target population and the frame population" (Couper 2000, p. 467). In online surveys, coverage errors result when not everyone in the target population has Internet access. In our survey, OpenVenue uses the popular Canadian MSN/Sympatico portal to recruit their panel members, so our coverage is further restricted to only MSN/Sympatico portal users. As a result, we cannot be assured that characteristics of the sample are representative of the adult Canadian population at large.

Comparative studies have shown that coverage problems with Internet surveys echo the demographic differences often described by the term "the digital divide" (Fricker, Galesic et al. 2005). For example, the old and the poor are generally underrepresented in online surveys. In one study, the demographic differences between an online sample and a phone sample was documented at 9% and differences in opinion items at greater than 20% with no predictable patterns (Couper 2000). However, other research has shown that there can be similar magnitudes of differences between the demographics of phone survey respondents and census figures (Roster, Rogers et al. 2004).

Although the proportion of the general population in Canada and the US with Internet access is growing, there is concern that the coverage of online surveys will never be a good as the coverage of telephone surveys because of the literacy requirements for Internet use (Couper 2000).

It has been suggested that the use of large samples with weighting techniques can be used to reduce coverage errors. With appropriately large samples, responses can be weighted along demographic factors. Additional weighting that takes into account attitudinal and behavioural factors is called propensity weighting. See Berrens, Bohara et al (2003) for a detailed explanation of how propensity weighting is done.

4.2 Sampling error

In online surveys, sampling errors result from the lack of a 'frame' to be used for sampling Internet users. There is no comprehensive list of everyone with access to the Internet or of everyone with email addresses. Both telephone and online surveys may also have issues around the use of panels (Braunsberger, Wybenga et al. 2007). OpenVenue has a large (400,000 person) base from which to draw its panels, but it is not a complete list of all Internet users or of all Sympatico/MSN users, as it includes only those who have volunteered and registered to do surveys. Even if such a list existed, or a technical solution to the frame problem is developed, researchers who wish to use online surveys will be confronted with prohibitions against spamming whereas RDD telephone survey methodologies have not been subjected to similar prohibitions (Berrens, Bohara et al. 2003). A national "do not call" system is currently under development in Canada, but it is not known whether this new legislation will apply to marketing research and/or public opinion firms.

Theories of sampling error can only be applied to probability-based sampling where we know the probability of selection for every member in the frame. Without probability sampling we cannot make inferences about the population or calculate confidence intervals (Couper 2000). Online surveys can address the sampling problem in two ways. The first is to recruit panel members through a probability-based method such as a RDD telephone approach and then issue invitations to surveys through the Internet. (Note that this method still has coverage issues: the population of interest must be Internet users only.) The second method is to recruit panel members through a method such as RDD, and then provide the necessary equipment, training and support so that both Internet users and non-users are included with equal probability. The firm Knowledge Networks uses this technique and provides WebTV technology to assemble its Internet panel.

As several researchers note, making inferences about a population is not the only objective when we conduct surveys. Some surveys are only interested in determining the relationships between variables. In these cases, sampling error is not as important (Best, Krueger et al. 2001; Berrens, Bohara et al. 2003; Coderre, Mathieu et al. 2004). Berrens, Bohara, et al (2003) found that their relational inferences from telephone and online surveys were very similar. In a different survey on the same topic (the 2000 US federal election), Best, Krueger, et al (2001) observe that there are decision-making hypothesis that are "uniformly applicable to the entire population" and in these cases a "diverse convenience sample" derived from heavily trafficked Web-sites is sufficient.

4.3 Non-response error

Non-response errors occur as a result of differences between those who respond to the invitation for the survey and those who do not. In order to calculate non-response error, we need to have a frame and know the probability of selection (Couper 2000). Even where probability-based sampling has been used, research has found lower response rates and greater non-response error for online surveys when compared to RDD telephone surveys.

4.4 Measurement error

In addition to the non-observation errors discussed above, every survey is subject to observation or measurement errors. These errors can arise from a number of different factors including mode differences, panel effects, and survey design. In the literature on online surveys versus telephone surveys, we find discussion of the following differences in measurement error:

- Self-administered surveys, including online surveys, are generally considered to reduce measurement error when the subject of the survey is a sensitive topic (Couper 2000).
- Opinions are mixed on whether online surveys convey a heightened sense of privacy and confidentiality (Braunsberger, Wybenga et al. 2007) or a weakened sense (Coderre, Mathieu et al. 2004).
- Respondents to online surveys expressed more extreme concerns and more demanding requirements (Roster, Rogers et al. 2004; Braunsberger, Wybenga et al. 2007).
- Results are mixed on the differences in "no response" answers between online and telephone surveys; most likely this is a result of differences in the survey design and interviewing scripts (Smith 2001; Roster, Rogers et al. 2004; Fricker, Galesic et al. 2005).
- Results are mixed on whether online respondents have less differentiated responses (Fricker, Galesic et al. 2005), more neutral and negative responses (Roster, Rogers et al. 2004) or more extreme responses (Smith 2001).
- Online respondents do better on knowledge questions (Fricker, Galesic et al. 2005), possibly because they rely less on memory and therefore provide more accurate and reliable responses (Braunsberger, Wybenga et al. 2007).
- Panel conditioning is not considered to be a pervasive problem (Dennis 2001; Berrens, Bohara et al. 2003).

As the literature suggest, there are both pros and cons to the use of online surveys versus RDD telephone surveys. We believe that online survey methods will continue to improve and that the problems associated with RDD telephone surveys will continue to grow. On balance, the advantages of online surveys, led by the enormous differences in costs, out-weigh the

disadvantages, especially for preliminary and exploratory information gathering such as this study.

5. DEMOGRAPHIC COMPOSITION OF THE SAMPLE

The demographic makeup of our sample is summarized in Table 1. Comparisons are shown to the 2001 Census figures for the Canadian over-18 population[3]. Coverage and sampling errors are present in the sample that OpenVenue asked to respond to the survey. However, since OpenVenue targeted the request to match the Canadian population by gender, age and region, differences in the demographic characteristics are primarily due to non-response error.

Table 1 – Demographic comparison between sample and 2001 Canadian census

Demographic Characteristic and Category		ORNEC Survey (%)	2001 Canadian Census (%)
Gender			
	Male ***	51.8	49.0
	Female ***	48.2	51.0
Residence			
	Newfoundland and Labrador	2.0	2.3
	Prince Edward Island	0.7	0.6
	Nova Scotia **	3.2	4.0
	New Brunswick ***	6.1	3.2
	Ontario ***	43.1	50.1
	Manitoba ***	6.1	4.9
	Saskatchewan ***	3.0	4.3
	Alberta ***	16.0	13.1
	British Columbia ***	19.8	17.2
Age			
	18-24 ***	12.0	9.6
	25-44 ***	39.5	44.9
	45-54 ***	19.2	22.9
	55-64 ***	12.4	18.2
	65 or older ***	16.9	4.4

*** Differences in proportions are significant at p=.01
** Differences in proportions are significant at p=.05

Table 2 highlights over-represented and under-represented demographic groups. It is somewhat surprising that the age group 65 and older is over-represented in an on-line survey, but we must remember that this difference is due to non-response error. We propose that the younger (18-24) and older (>65) age groups may have more time to respond to a survey than those in the intervening age categories. We also have some concern that Ontario is significantly under-represented.

[3] Statistics Canada Web sites: http://www.statcan.ca/Daily/English/070329/d070329b.htm and http://cansim2.statcan.ca/cgi-win/CNSMCGI.EXE?Lang=E&ArrayId=051-0001&Array_Pick=1&Detail=1&ResultTemplate=CII/CII___&RootDir=CII/

Weighting procedures could be investigated to adjust our results for these over and under represented groups, however at this stage of our investigations we do not believe that weighting would make any differences in the main conclusions reached in this report.

Table 2 – Over and under-represented demographic groups

Over-represented:	Under-represented:
Males	Females
New Brunswick Manitoba Alberta British Columbia	Nova Scotia Ontario Saskatchewan
Ages 18-24 Age 65 or older	Ages 25-64

6. DEFINING IDENTITY THEFT AND IDENTITY FRAUD (QUESTIONNAIRE PART 1)

In a recent survey, 29% of Canadians agreed with the statement "I hear a lot about identity theft, but I don't know what it means" (Ipsos-Reid 2006).

Question 1 - In your opinion, which of the following scenarios describes a case of identity theft? (multiple response)

The purpose of the first question in our questionnaire was to try to gain some insight into what the Canadian public considers to be IDT or IDF. Although we use the terms IDT and IDF in the following analysis, we did not try to make a distinction between IDT and IDF when we posed this question. We assumed that the respondents would take the term 'identity theft', as used in the question, to mean the acquisition of personal information for the purposes of fraud as well as the commission of frauds by using a false identity. This is how the term is commonly used in the popular press.

Some of the dimensions that may affect whether people include a specific case as an example of IDT or IDF are believed to be:

- Financial frauds versus non-financial frauds
- Friendly fraud (fraud by people known to the victim) versus stranger fraud (fraud by people unknown to the victims)
- Theft only (where there has been no known case of fraud) as opposed to cases where both the theft and fraud are known.
- Fraud only (where the victim does not know how their personal information was obtained) as opposed to cases where both the theft and fraud are known.
- Account-level information that can be easily changed versus more sensitive identity-level information that cannot be easily changed. (See Section 8.8.1 for a further discussion of these categories.)

Table 3 shows the scenarios that were presented in the question and how each scenario is described by the above dimensions. The scenarios in Table 3 are ordered from the one that was

most often selected as a case of IDT or IDF to the one that was least often selected. The percentage of people who indicated each scenario as a case of IDT or IDF is shown in the last column. Percentages add to over 100 because respondents were asked to choose all those cases they thought were cases of identity theft.

Table 3 – Question 1 Scenario Dimensions

	Financial ($) or Other (O)	Friendly fraud (F) or Stranger fraud (S) or Unknown (U)	Theft (T) only, Fraud (F) only, or Theft and Fraud (T&F)	Account-level (A) or identity level (I)	Percent of respondents who indicated that this was a case of IDT
1) You find out that someone who worked in your home used your personal information to get a replacement Health Card and obtain health care services under your name.	O	F	T&F	I	88.3%
2) You give your credit card to the attendant at a gas station who swipes the card through an illicit machine that reads the information on the card's magnetic strip. The attendant then sells the information to criminals who manufacture counterfeit credit cards.	$	S	T&F	A	86.5%
3) You receive a notice from the Canada Revenue Agency that you owe income tax from a job that you never held.	$	U	F	I	78.6%
4) You receive an email from your bank, asking you to respond and confirm your account information. You do this and then later find out that the email was not sent by the bank.	$	S	T	A	75.7%
5) 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.	$	U	F	A	77.0%
6) While ordering a service, you give your credit card number to a company representative over the phone. You later learn that the company has fired one of their representatives for selling customers' names and credit card numbers to a fraud ring.	$	S	T	A	73.5%
7) Someone steals your wallet and uses your credit card to make purchases at a store	$	S	T&F	A	71.7%
8) You have an eBay account and a roommate uses your computer to list fraudulent items for auction under your name and account.	O	F	T&F	A	69.5%
9) A family member takes your cheque-book and forges your name on a number of cheques.	$	F	T&F	A	63.6%
10) You find out that a friend has received threatening emails that appear to come from you, but you did not send them.	O	U	F	I	61.6%
11) An underage person borrows another person's identification in order to obtain alcohol or cigarettes	O	F	F	I	52.8%

12) Your insurance company advises you that they have lost a computer disk that had unencrypted customer information on it including names, addresses, birth dates, and drivers' license numbers.	O	S	T*	I	48.8%
13) Your boss promotes an idea you had to improve how your group works, and takes credit for the result.	n/a	F	n/a	n/a	24.9%
* This scenario describes loss of information only, not necessarily a theft					

In general, financial and stranger frauds are perceived to be cases of IDF more often than non-financial and friendly frauds. There does not appear to be a pattern as far as whether the case described a theft only, a fraud only or both theft and fraud. There also does not seem to be a pattern with respect to account-level versus identity-level information. It would be interesting to do a cluster analysis at some future time to see if there are identifiable groups of people with common understanding of what is included in the IDT and IDF concepts. Finch and Huynh (2000) and Finch (2005) describe clustering techniques for variables with dichotomous data.

Some interesting observations on the results from this question:

- Scenario 1) describes a fairly classical case of IDT and IDF. It is somewhat surprising that only 81% of respondents identified it as such. Those who did not identify it as a case of identity theft may be considering the fact that in this scenario the costs of the fraud are not borne by the victim.

- Scenario 2) describes a case of "skimming" and was chosen by 86.7% of our respondents as a case of IDT. In a comprehensive Australian study of IDF, the authors suggest that "skimming" should not be considered a case of identity fraud because it does not involve an explicit act of impersonation (Cuganesan and Lacey 2003). This highlights the problems of trying to define or rigorously limit the area of "identity theft" when the term is widely used and abused in the general language.

- Scenario 4) describes a case of "phishing" and scenario 6) describes a data breach. Neither of these scenarios implies that an actual fraud that has been committed. The relatively high ranking of these scenarios may indicate that people feel vulnerable and violated merely by knowing that their personal information has been compromised.

- Just over 70% of respondents believe that common credit card fraud, resulting from a stolen wallet, is a case of IDF (Scenario 7) and friendly fraud by a family member was chosen as a case of IDF by only 64% of our respondents (Scenario 9). Because these are fairly common occurrences of IDF, they provide an excellent example of the dangers of relying on surveys that just ask if respondents "have been a victim of identity theft". Our results show that if we survey 1000 people, 170 have been victims of credit card fraud in the last year. However, since only 71% of these people believe that this is IDF, only 120 of these people would report themselves as victims of IDF. Similarly, 44 of 1000 people have been victims of fraud by a family member in the last year, but only 64% believe this to be IDF, therefore only 28 of these people would report themselves as victims of IDF

- The last three scenarios (11, 12 and 13) are generally not considered to be cases of IDT or IDF. We still find between 25% and 50% of our respondents indicating that they consider these to be cases of identity theft.

- An analysis of the difference in proportions shows that significantly more women than men consider scenarios 3), 10) and 9) to be cases of IDF. See Table 4

Table 4 – Gender differences in scenario classification

Scenario:	Males	Females	Total	
3) You receive a notice from the Canada Revenue Agency that you owe income tax from a job that you never held.	1366 (49.7%)	1385 (50.3%)	2751	*
9) A family member takes your cheque-book and forges your name on a number of cheques.	1061 (49.1%)	1100 (50.9%)	2161	**
10) You find out that a friend has received threatening emails that appear to come from you, but you did not send them.	1071 (48.9%)	1120 (51.1%)	2191	**
Sample	1832 (51.8%)	1707 (48.2%)	3539	
* differences in proportions are significant at p=.10				
** differences in proportions are significant at p=.05				

7. INCIDENCE RATES (QUESTIONNAIRE PART 2)

Incidence rates are derived from the answers to Question 2. (See Section 3.3 for the full text of Question 2.) We designed question 2 to capture information about five classifications of IDT or IDF. These classifications are:

- Frauds involving existing credit card accounts
- Frauds involving other existing accounts (i.e. bank accounts, phone or utility accounts, etc.)
- Frauds involving new accounts (i.e. credit card accounts, bank accounts, phone or utility accounts, etc.)
- Other types of frauds (i.e. government benefits, tax fraud, leases, impersonation, etc.)
- Theft of personal information, when a fraud has not, or not yet, been committed.

The first four classifications are derived from consumer surveys conducted in the United States. The first comprehensive consumer survey was conducted in 2003 for the Federal Trade Commission (FTC) by Synovate, a commercial research company (FTC 2003). The survey was part of an omnibus survey of US adults over 18 years of age, conducted by telephone using a Random-Digit-Dialing (RDD) sampling methodology. The survey was done in four waves in March and April of 2003, and resulted in interviews with 4057 people. The full questionnaire is available online (FTC 2003).

Javelin Strategy Research has conducted similar surveys in late 2004, 2005, and 2006 involving between 4000 and 5000 telephone interviews each year. The published reports are respectively

dated 2005, 2006 and 2007. The Better Business Bureau assists in the publication of these reports. Sponsoring organizations are listed as CheckFree Services Corporation, Visa USA and Wells Fargo Bank.

Javelin does not make its questions available, but states that the 2003 FTC survey was "closely mirrored in order to provide longitudinal trends" (Javelin 2005). Synovate conducted the first Javelin survey using the same methodology used in the 2003 FTC survey. Javelin added some questions about personal behaviours and removed some specific questions related to telephone accounts. The next year, Synovate was no longer using RDD sampling methods so the survey work was contracted to the Discovery Research Group to remain consistent in methodology. Another change for the 2006 report was that debit card fraud is categorized as Existing Card Accounts Fraud rather than Existing Non-Card Accounts Fraud (Javelin 2006). There were no other major changes reported in the 2007 report (Javelin 2007).

Another comprehensive US survey that was used to develop our questions was conducted in the last half of 2004 by the US Department of Justice (DOJ). The DOJ conducts the National Crime Victimization Survey (NCVS) each year and 2004 was the first year that questions related to identity theft were added to the NCVS. As opposed to the FTC and Javelin surveys, the NCVS frames its questions on a household basis. The report is based on telephone interviews with 40,000 people. The demographics reported in the NCVS describe the head of the household, and not necessarily the victim of the IDF. A report on the pre-testing of the NCVS survey is available (Hughes 2004).

In Appendix A, Table A2 shows the precise wording of the incidence questions from the FTC (and by assumption Javelin), NCVS and our ORNEC surveys . Note that there is a different unit of analysis (individual, household and immediate family) used in each of these surveys. The NCVS survey also differs from the other two in that it asked about both attempted and actual frauds. Our ORNEC survey asked separately about New Accounts frauds and Other Frauds. We also asked about cases where IDT had occurred, possibly through notification of a data breach, but no fraud had been committed.

In the following sections we also discuss results from some other surveys, however in these surveys the term identity theft is often not defined or the definition provided is not available. As we indicated in Section 6, if the term IDT is not specifically defined for respondents there will be under-reporting of common types of identity fraud such as credit card fraud and friendly fraud.

7.1 Base incidence rates for each type of identity fraud and theft

In total, 1710 or 43% of our respondents reported some kind of IDT or IDF in their family. Table 5 shows the base incidence rates for the five different types of IDF and IDT described in Question 2. These base rates show the number of responses for each choice in each type of IDF or IDT. These are non-exclusive categories. Since each respondent is reporting for potential multiple victims (themselves and members of their family) and each victim may have been subject to more than one type of fraud, the total number of reports in the base incidence rates (3103) adds up to more than the total number of victim reports (1710). The incidence rates in Table 5 apply to the family as a unit of analysis. For example, 30.7% of respondents report that someone in their family has been a victim of existing credit card fraud.

Comparable data can also be found in a U.S. survey by Chubb Group of Insurance Companies in 2005. They found that 27% of respondents reported that their or a family member's credit card was used fraudulently. Eight percent reported that fraudulent cheques had been written on their or a family member's bank account. This is only one form of Other (non-credit card) accounts fraud.[4]

Table 5 - Base incidence rates for identity frauds and identity theft (family)

Type of IDF or IDT	Incidence rate for family	
	Number of positive responses	Percent
Existing credit card fraud	1087	30.7%
Other (non-credit card) accounts fraud	735	20.8%
New accounts fraud	405	11.4%
Other fraud	268	7.6%
Identity theft only	608	17.2%
Total	3103	
Total number of respondents N=3539		

Table 6 – Base incidence rates for identity frauds and identity theft (self)

Type of IDF or IDT	Incidence rate for individual	
	Number of positive responses	Percent
Existing credit card fraud	602	17.0%
Other (non-credit card) accounts fraud	389	11.0%
New accounts fraud	203	5.7%
Other fraud	154	4.4%
Identity theft only	412	11.6%
Total	1760	
Total number of respondents N=3539		

The incidence rates in Table 6 have the individual as the unit of analysis.[5] In total, 1167 or 33% of our respondents reported that they had been a victim of some type of IDT or IDF. Again, the categories in Table 6 are non-exclusive, totaling 1760 reports for 1167 victims. For example, 5.7% of respondents report that they have personally been a victim of new accounts fraud. For comparison, a recent survey by Queen's University reports that 14% of Canadians have been the victim of credit card fraud (Zuriek and Harling-Stalker 2006). Our incidence rate of 17% is slightly higher than that result.

7.2 Incidence rate using FTC/NCVS categories

In the previous section, we showed the incidence rate for each type of IDF or IDT, however each episode of IDF may result in more than one type of fraud being committed, and respondents may

[4] Chubb Group of Insurance Companies, http://chubb.com/corporate/chubb3875.htm (viewed Oct. 31, 2005)

[5] For overall (i.e. 'ever') incidence rates, we do not have to worry about what was the latest episode when there were multiple episodes or multiple victims. We can therefore use the SELF_POSSIBLE subset of 1167 cases where the respondent chose either "this has happened to me" or "this has happened to both me and someone in my family" as their response to items in Question 2.

be reporting more than one episode of IDT or IDF. In order to allocate each response to a single category of IDF, the FTC, Javelin and NCVS reports establish a hierarchy of categories of IDF. These categories are ordered from least serious to most serious as follows:

- Existing Card Account Fraud
- Existing Non-Card Account Fraud
- New Account and Other Frauds

Each case is then placed in the category where the most serious type of fraud was committed. For example, if a victim reports that someone used their credit card number to charge purchases to their account and also used personal information to set up a new wireless phone account in their name, that case would be placed in the New Account and Other Frauds category.

Our victim reports include another category, where an identity theft has occurred, but no identity fraud is known to have happened to date. We include this new category as the least serious category. For comparison purposes, we have also combined our results for new account fraud and other fraud. Our results, using the FTC categories are shown in Table 7. Note that in this case, the total number of cases (1710) is equal to the number of victim reports, because the categories are exclusive and comprehensive.

The unit of analysis in Table 7 is the family. For example, 16.4% of people report that someone in their family has experienced fraud related to an existing credit card and no more serious IDFs have occurred to anyone in their family. In total, 44.8% of our respondents report that they or someone in their family has been a victim of some kind of IDF (credit card, other accounts or new accounts).

Table 7 – Incidence rates by FTC Category

IDT or IDF Category		Frequency	Percent
1	Identity theft only	126	3.6%
2	Existing credit card fraud	579	16.4%
3	Other (non-credit card) accounts fraud	477	13.5%
4	New accounts or other fraud	528	14.9%
	Total	1710	100.0%

In 1998 and 1999, Privacy and American Business found that 20% and 21% of respondents, respectively, reported that they or a member of their family had experienced identity fraud (Privacy and American Business 2003). A 2004 survey sponsored by Unisys Corp. and conducted by International Communications Research (ICR) found that 1 in 5 US households had been affected by identity theft. We assume that one's household is smaller than one's immediate family. It must also be noted that neither of these surveys defined the term 'identity fraud' or 'identity theft', which may partially explain the differences between their results and ours.

7.3 FTC/Javelin comparisons

There are two differences in measurement between our survey and the FTC/Javelin surveys. Our basic incidence rates are for *families*, when the IDT or IDF could have happened at *anytime* prior

to the survey. The FTC/Javelin surveys report on incidence rates for *individuals* within the *last 5 years* and the *last year*.

Question 4 determined when the latest episode of IDT or IDF occurred. We can therefore use the responses from Question 4 to determine incidence rates for families within the last 5 years and the last year. The results are shown in Table 8. For example, 14.2% of people report that someone in their immediate family has been a victim of IDT or IDF in the last year.

Table 8 - Incidence rates for families

IDT or IDF Category	In the last year	In the last 5 years
Existing credit card fraud	5.4%	12.6%
Other (non-credit card) accounts fraud	4.5%	10.4%
New accounts or other fraud	4.3%	11.4%
Total	14.2%	34.4%

In order to get results for individuals, we can use our SELF_ONLY and SELF_VICTIM subsets of cases. This gives us a range in which the true value will reside. See Table 9 and Table 10. For example, the percentage of respondents who had been a victim of credit card fraud in the last five years is between 5.7% and 8.1%. In 2003, the FTC survey reported that 6.0% of Americans had been a victim of credit card fraud in the last 5 years. (These calculations do not include cases where only IDT occurred and no frauds have been reported, as this category of response was not included in the FTC/Javelin categories.)

Table 9 - Incidence rates for individuals - in the last 5 years

IDT or IDF Category	**ORNEC**		**FTC 2003**
	Minimum	**Maximum**	
Existing credit card fraud	5.7%	8.1%	6.0%
Other (non-credit card) accounts fraud	3.2%	6.4%	2.0%
New accounts or other fraud	2.5%	8.4%	4.7%
Total	11.4%	22.9%	12.7%
Sample size (N)	3,539	3,539	4057

Table 10 - Incidence rate for individuals – in the most recent year

IDT or IDF Category	ORNEC		FTC 2003	Javelin 2004	Javelin 2005	Javelin 2006[6]
	Minimum	Maximum				
Existing credit card fraud	2.0%	3.2%	2.4%		All existing accounts	2.1%
Other (non-credit card) accounts fraud	1.2%	2.8%	0.7%		2.5%	0.6%
New accounts or other fraud	0.8%	3.1%	1.5%		1.5%	1.1%
Total	4.0%	9.1%	4.7%	4.3%	4.0%	3.7%
Sample size (N)	3,539		4057	4000	5000	5000+

Comparable results are found in a Gartner survey, which found that 3.4% of U.S. adults had been victims of identity theft in the 12 months ending June 2003.[7] We do not know how the term "identity theft' was defined in this survey, which may explain why this result is lower than those shown in Table 10.

Except for other (non credit-card) accounts frauds, the rates from the US studies in table 10 fall between our minimum and maximum values. However, they are generally much closer to our minimum values. Our incidence rates would therefore seem to be higher than those reported in any of the US studies. There are two possible reasons for these differences that are related to our methodology.

1. Differences Between Online and Telephone Surveys

There may be a difference arising from using an online survey instead of telephone interviews. In August 2006, Gartner conducted a survey using an online Internet panel. The sample size was 5000. They report an incidence rate that is 1.51 times greater than the FTC 2003 phone survey results (15 million American victims in the last 12 months versus 9.9 million). If we take the FTC incidence rate of 4.7% and multiply it by 1.51, we get 7.1% which is closer to the mid-range between (4.0% and 9.8%) found in our study.

The Gartner report comments on a phone survey done in the same time frame and expands on the differences in the results of these two surveys as follows:

> "The survey conducted by Gartner yielded much higher fraud rates than those surfaced by a similar phone-based survey conducted by the same primary research company in the same time frame on behalf of another client, which has not issued its report on the finding. In Gartner's opinion, the questions in the two surveys

[6] From
Javelin (2007). Living the low life on your identity: From groceries to toilet paper, criminals now rely on ID theft for basic needs. **2007**. http://www.javelinstrategy.com/2007/02/12/living-the-low-life-on-your-identity-from-groceries-to-toilet-paper-criminals-now-rely-on-id-theft-for-basic-needs/

[7] http://www.gartner.com/5_about/press_releases/pr21july2003a.jsp (viewed Apr. 19, 2006)

> were not different enough to cause the large differences that appeared, although the survey company differs on that point (Litan 2007)."

When Javelin Strategy and Research released the results of their 2006 phone survey, it appears that this was the un-named phone survey that was conducted at the same time as the Gartner online survey. The comparison of the results of the two surveys is noted in Javelin's press release as follows:

> "The Javelin survey found a decline in the number of victims, with 500,000 fewer Americans falling prey to the crime in 2006... But others find a much higher rate: 14 million victims in 2006, up from 9.9 million reported by the Federal Trade Commission in 2003, said Avivah Litan, an analyst with Gartner Research, the Stamford Conn.-based firm. Litan cited figures from a soon-to-be-released Gartner online survey of 5,000 consumers. She said survey companies are as yet unable to determine why online and telephone surveys of identity theft victims result in such disparate numbers (Javelin 2007)."

The research on phone and online surveys presented in Section 4 showed how coverage, sampling, non-response and measurement errors can account for differences between phone and online surveys, but the differences found in the literature are small in comparison to the differences in incidence rates between the Gartner survey and the FTC/Javelin surveys. Two sources of measurement (or observation) error that may contribute to these differences are the sensitive nature of the topic and the complex nature of the questions.

People may be embarrassed that they were the victim of a scam or a fraud. There may be additional guilt or sensitivity if the fraud was committed by a family member. As a result, respondents may not be willing to describe such incidents to an interviewer. The impersonal nature of an online survey may elicit more responses. Subjects may be more confident that their confidentiality will be protected if they provide potentially embarrassing information. Our statements at the beginning of the survey and the fact that it was being conducted by a university may have also helped in this regard.

In an online survey, respondents have time to review questions and change their responses. It is believed that this can result in more accurate responses to complex questions, and may be a factor in the higher incidence rates reported in on-line surveys.

2. Differences Due to Inclusion of Question 1 in the Survey

In addition to the differences between online and phone surveys, the inclusion of Question 1 may have made certain types of IDT and IDF more salient in the minds of our respondents than is the case in the other surveys. Scenarios such as misappropriation of eBay accounts, someone using your email account, fraudulent phone charges and others, especially when committed by a family member or friend, may not have come to mind in the other surveys. These types of fraud are part of the existing (non-credit card) account fraud category and this is the category where our results differ the most. In this category, the FTC/Javelin results lie below the minimum incidence rate of our range.

7.4 NCVS comparisons

The NCVS survey used the same exclusive and comprehensive system of categories as the FTC/Javelin surveys, but measured the response rate for households in the last six months. Again, we can use the responses to Question 4 to get incidence rates for families within the last six months.

There is still, however a difference in the unit of analysis – households versus immediate family. Table 11 shows the 6-month incidence rates for households from the NCVS survey and for families from the ORNEC survey.

Relevant statistics from Statistics Canada show that the average size of a Canadian nuclear family (parents and children) is 3.0 people[8] and the average size of a Canadian household is 2.6 people[9]. We assume that when we ask about the respondent's immediate family, they would consider any family members with which they currently reside (i.e. their household) as well as a generation above (parents) and/or a generation below (children) who are not resident in the household. We therefore assume that one's immediate family is larger than one's household. Assuming that the average immediate family is twice the size of the average household is probably not an unreasonable assumption. If this is the case, our incidence rates are not out of line with those reported in the NCVS survey.

Table 11 - Comparison with NCVS survey

IDT or IDF Category	Incidence rate for immediate family/households in the last 6 months	
	ORNEC (immediate family)	NCVS (household)
Existing credit card fraud	2.7%	1.5%
Other (non-credit card) accounts fraud	2.1%	0.8%
New accounts or other fraud	1.8%	0.5%
Multiple types of fraud	n/a	0.4
Total	6.6%	3.1%
Sample size (N)	3,539	42,000

7.5 Estimates of identity fraud costs

We can use the incidence figures from Section 7.3 (Table 10) and fraud costs from Questions 17-19 to arrive at a national estimate of IDF costs. Working from Statistics Canada figures for July 1st, 2006, we estimated the Canadian population over 18 years of age, at 24,841,800.[10]

[8] http://www43.statcan.ca/02/02d/02d_001_e.htmSelf
[9] http://www40.statcan.ca/l01/cst01/famil53a.htm
[10] http://www.statcan.ca/Daily/English/070329/d070329b.htm and http://cansim2.statcan.ca/cgi-win/CNSMCGI.EXE?Lang=E&ArrayId=051-0001&Array_Pick=1&Detail=1&ResultTemplate=CII/CII___&RootDir=CII/

Using the incidence rate for the last 12 months, when the respondent himself or herself was the victim, we arrive at the results shown in Table 12. Note that we are again giving a range of values because we do not know for certain whether the respondent was the victim of the episode being described in Question 4 and Questions 17-19. Costs used in these calculations are the mean costs for cases that were discovered in the last year in each of the subsets (SELF_ONLY and SELF_VICTIM).

Table 12 – Annual costs of identity fraud

		Minimum	Maximum
Number of victims (last 12 months)	Percent of population	4.0%	9.1%
	Projected number of victims in Canada	993,672	2,260,603
Fraud amount	Mean amount per victim	$2947	$3188
	Total	$2,928,351,384	$7,206,802,364
Victim's hours to resolve	Mean hours per victim	18	23
	Total	17,886,096	51,993,869
Out-of-pocket costs	Mean cost per victim	$165	$396
	Total	$163,955,880	$895,198,788

From Table 12 we can see that there are over 1 million victims of IDF each year and the amount that perpetrators gain from IDF in Canada is over $3 billion dollars. Dealing with identity frauds costs Canadian victims $164 million of their own money and they collectively spend over 18 million hours a year to resolve these problems. Note that the fraud amount includes losses borne by credit card companies and individual companies. However, there are many other costs to businesses and governments, including the costs associated with preventing, detecting and responding to identity theft and fraud that are not captured in this analysis.

8. CHARACTERISTICS OF IDENTITY THEFT AND IDENTITY FRAUD (QUESTIONNAIRE PART 3)

8.1 Data analysis

We want to be able to examine the responses to our victim questions along a number of different dimensions. To do this, we have recoded the response from some questions to create new variables. Two of these new variables, fraud types and credit card purchase only, are described below. These two variables are used in the analysis of many of the victim questions. Other new variables, created for analyses within a single question, are described in the corresponding sections. See Appendix A, Table A3, for a list of Questions and the response type and variable name for each of the victim questions (Q4-Q30).

8.1.1 Fraud types

We created five new variables to describe the types of fraud associated with each case. These variables are determined by the answers to Question 14 and pertain to the case/latest episode being described in Questions 4 through 30. The five variables we created are:

- Credit card fraud
- Existing accounts (other than credit card) fraud
- New accounts fraud

- Other fraud
- Identity theft only (no frauds known)

Note that these are non-exclusive categories, so the total percentage is over 100. A table showing the Question 14 responses and the mappings to these fraud types can be found in Appendix A, Table A1. A frequency analysis of the fraud types is shown in Table 13.

Table 13 – Frequency of Fraud Types

	Responses	Percent of Cases
Victim of other types of fraud (from Q14)	147	9.1
Victim of new accounts fraud (from Q14)	170	10.5
Victim of credit card fraud (from Q14)	925	57.4
Victim of theft, but no frauds to date (from Q14)	206	12.8
Victim of existing accounts fraud (from Q14)	566	35.1
Total	2014	124.9

Because these are non-exclusive categories they are handled as "multiple response" in SPSS and certain statistical analyses, such as chi square, cannot be applied when these variables are used in a cross tab with other variables

8.1.2 Credit card purchase only

After discussion with our research partners, we also created a variable to identify cases where the only fraud committed or attempted was a purchase on an existing credit card account. Some Canadian banks do not feel that these cases should be included in more specific discussions about the IDT and IDF problem, as they believe that they have sophisticated and effective systems in place to address this type of crime. This position is supported in that the victims of these crimes pay little in terms of out-of-pocket costs or time spent to resolve the problem. See Section 8.14 and 8.15 for details.

Of the 1710 victim reports, 615 or 36% were cases where the only fraud committed or attempted was a purchase or attempted purchase on an existing credit card. We will call these cases "CC only" and the remaining 1095 cases will be called "Frauds (not CC only)". The Frauds (not CC only) category includes cases where there was an attempt to take over an existing credit card account, as these cases are more serious than cases where the card was simply used to make purchases.

8.1.3 Cross tab analyses

For many of the characteristics of the cases that are described in Questions 4 to 30 we provide three cross tab analyses in Appendix B. The first is a cross tab with the fraud type. The second is a cross tab with the time to detection, as early detection is believed to lead to reduced costs. The third is a cross tab with the fraud costs. These tables correspond to many of the tables listed in the contents of the Javelin survey reports (Javelin 2006).

In the following sections, results are shown in the order in which the questions were asked in the survey.

8.2 Recency of the case

Question 4 - When was the identity theft discovered?

Table 14 shows the recency of the incidents of IDT and IDF that are reported by the survey respondents. Remember that where there were multiple episodes of IDT or IDF (with the same or different victims) respondents were asked to answer this and all following questions with reference to the latest episode only. Over three-quarters of the cases described were discovered in the last 5 years.

Table 14 – Recency of the case

When was the identity theft discovered?	Frequency	Percent	Cumulative Percent
In the past 6 months	261	15.26	15.26
Between 6 months and 1 year ago	290	16.96	32.22
Between 1 and 2 years ago	334	19.53	51.75
2 to 5 years ago	436	25.50	77.25
More than 5 years ago	389	22.75	100.00
Total	1710	100	

8.3 Method of detection

Question 5 - How was the identity theft discovered? (multiple response)

People may discover that they have been a victim of IDT or IDF in a number of different ways. Table 15 shows an ordered list of responses to this question. Appendix B - Table B1 shows these responses cross tabbed with the CC Only/Fraud (not CC only) classification, a summary of which is also shown in Table 15.

Where there was only a fraudulent credit card purchase, notification from a bank or credit card company and monitoring bank or credit card accounts were each mentioned in over 40% of cases. Where there were other more serious frauds, these methods of detection are mentioned in just over 30% of the cases, and methods of detection such as notification by police or creditors and being turned down for a loan or mortgage were more frequently mentioned

An examination of the open-ended comments associated with the 'Other' response shows additional cases that should be shown in the first two categories - notification by bank or credit card companies (7) and monitoring of bank and credit card accounts (8). As well, there were 22 responses where the IDT was discovered by monitoring other accounts, primarily telephone accounts. Other methods of detection specified in open-ended comments attached to the 'Other' response included confessions by the perpetrator (10), renewal credit cards stolen from the mail (3), credit card purchases denied (3), and debit card withdrawals denied (4).

Table B2 in Appendix B shows the method of detection cross-tabbed by the type of frauds attempted or committed (from Question 14).

- In cases where credit card frauds occurred, detection was primarily through monitoring of accounts (42.8%) or notification by the credit card company (43.3%).

- For cases of existing accounts (other than credit card accounts) detection was also primarily through monitoring (47.5%) or notification (37.6%) but 17% indicated that they had been contacted by creditors about unpaid bills.

- For new accounts fraud, the most frequent method of detection was through contact by creditors or collection agencies about unpaid bills (44.1%) followed by notification by a bank or credit card company (29.4%) and monitoring bank or credit card accounts (24.7%). In 21.8% of cases, new accounts fraud was first discovered when the victim was turned down for a loan, mortgage or other credit.

- Other types of fraud (i.e. employment, benefits, etc.) were detected in many different ways.

- In cases where there was identity theft, but no known frauds, the theft was most frequently discovered through notification by a credit card company or bank (27.7%), having belongings stolen (22.89%), and notification of a data breach from a company that had the victim's information (19.4%).

Table 15 – Method of Detection

How was the identity theft discovered?	Responses	Percent of All Cases	Percent of CC Only cases	Percent of Fraud (not CC only) cases
By monitoring bank and credit card accounts	629	36.8	43.9	32.8
Notification received from a bank or credit card company	616	36.0	44.2	31.4
Belongings were stolen	227	13.3	9.6	15.3
Contacted by creditors or a collection agency about unpaid bills	222	13.0	6.2	16.8
Other	190	11.1	5.0	14.5
Notification of a data breach received from a company that had my information	139	8.1	4.2	10.3
By requesting and reviewing a copy of a credit report	110	6.4	4.1	7.8
Notification by police	100	5.9	1.5	8.3
An application for credit, a loan or a mortgage was turned down.	88	5.6	0.7	7.7
Total	2321	135.7		

It is often proposed that proactive monitoring can lessen the time to detection and the costs associated with IDF. Appendix B – Table B3 shows the method of detection cross-tabbed with the interval between the theft and its discovery.

If we examine these results by the interval between the theft and the discovery of the theft (i.e. column percentages) we find that when discovery of the theft occurs within a week, it is most often through notification by a credit card company or bank (43.8%), monitoring accounts (32.0%) and when belongings are stolen (24.5%). The most common method of detection when discovery takes between a week and a month is through monitoring of accounts (50.2%). When discovery takes over six months, it is most likely to be detected when the victim is contacted by creditors or a collection agency.

We can also examine these results by method of detection (i.e. row percentages) and indicate in what percent of the cases discovery happened within a certain time period. For example, when belongings were stolen, people discovered the theft within a week in 55.9% of the cases. The intervals between the theft and its discovery are shown for each method of detection in Figures B1-B8 in Appendix B.

Appendix B - Tables B4 to B6 show the method of detection cross-tabbed with our three measures of costs. The average amount of money obtained by the perpetrator according to the method of detection is shown in Figure 4, below. (Note that respondents could indicate more than one method of detection, so a case may be included in more than one bar in the Figure.) Figures 5 and 6 show the corresponding relationships between method of detection and the average number of hours that victims spent to resolve the problems resulting from the IDT or IDF (Figure 5) and method of detection and the victim's average out-of-pocket costs (Figure 6).

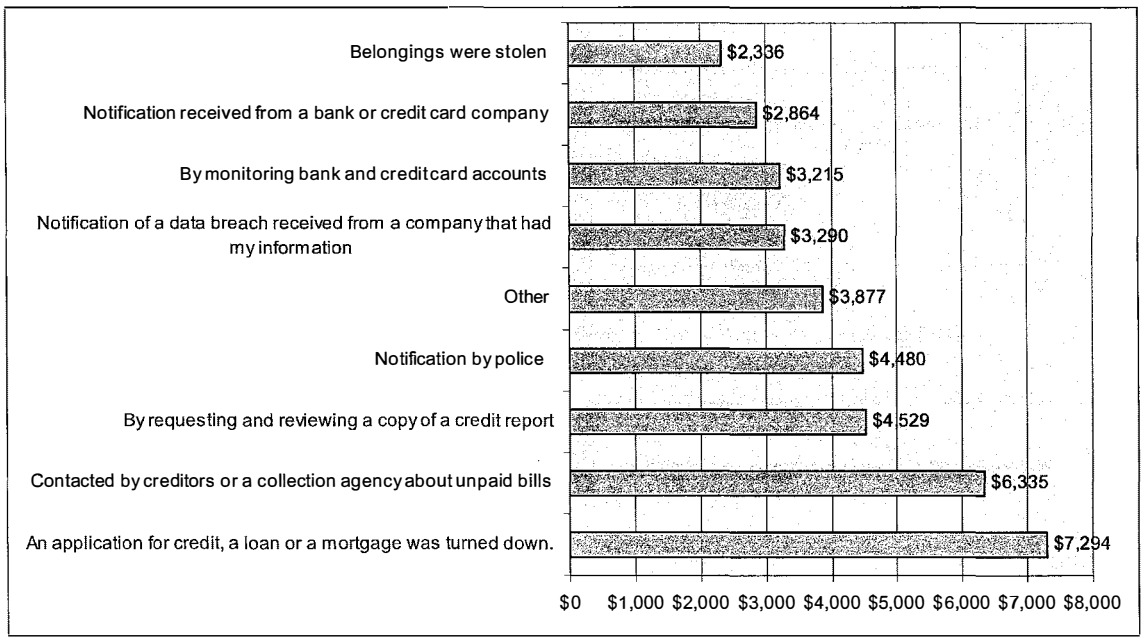


Figure 4 - Average fraud amount, by method of detection

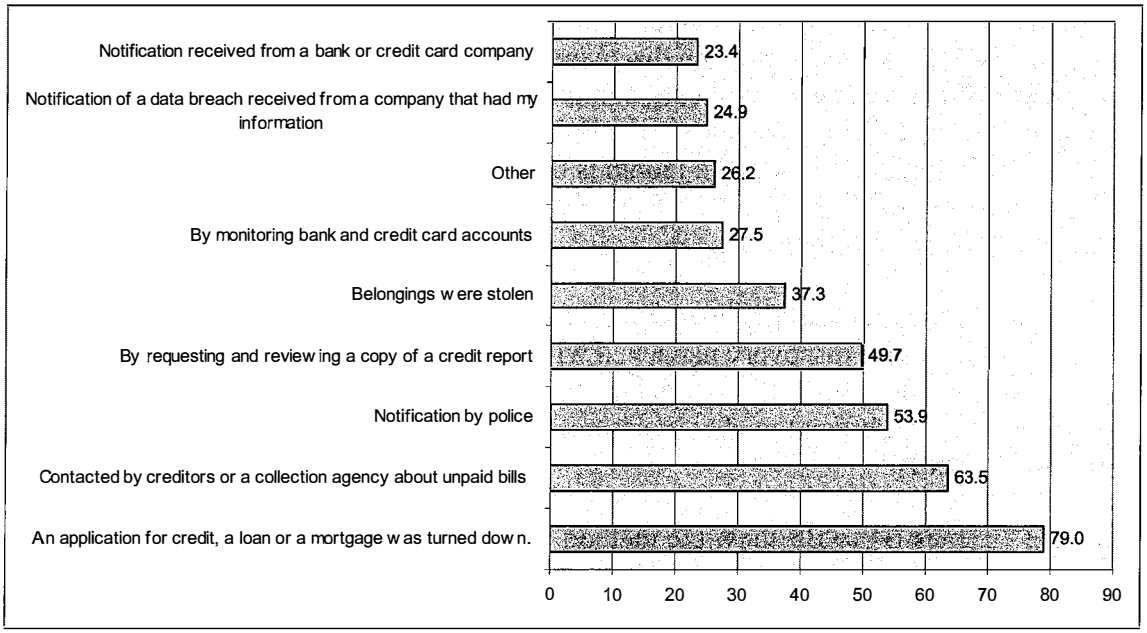


Figure 5 - Average victim hours by method of detection

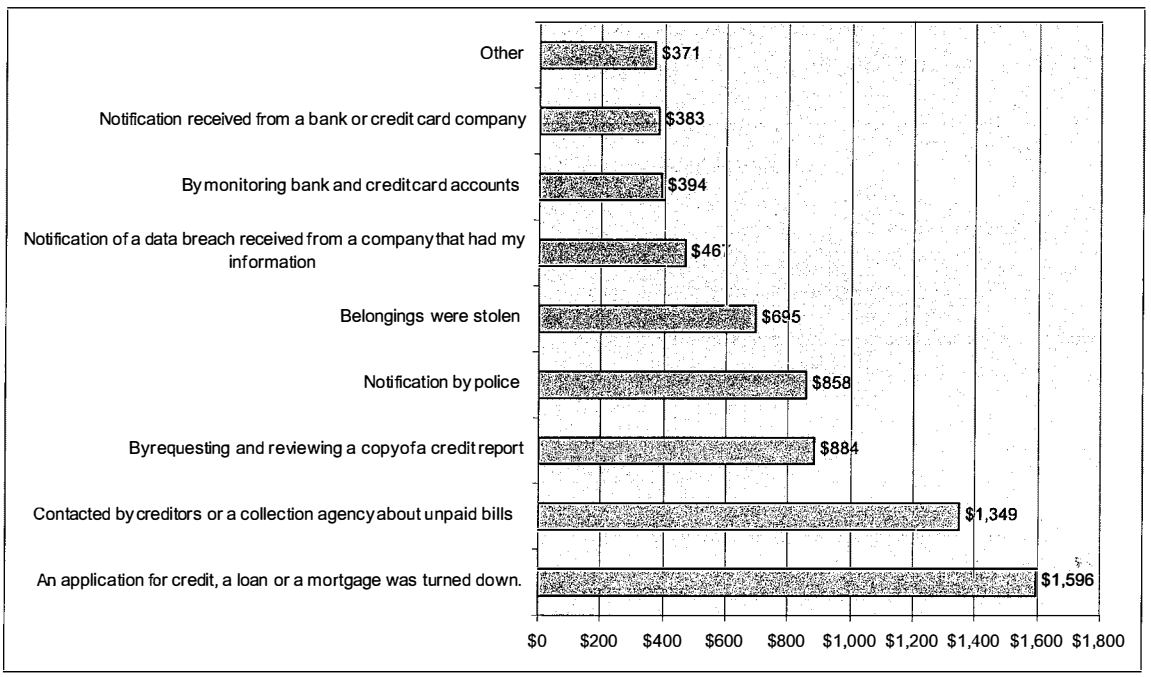


Figure 6 - Average out-of-pocket costs by method of detection

8.4 Awareness of how information was obtained

Question 6 – Do you know how the personal information obtained in the identity theft was accessed or taken? (Check one)

Figure 7 shows the responses to the question of whether the victim knew how their personal information was accessed or taken. In 42% of the cases, the method by which the information was accessed is known. In another 15% the victim may not know for certain, but has a suspicion, of how the information was obtained. There is only a marginal ($p = 0.06$) difference in these percentages across the CC Only and Fraud (not CC only) categories. If we exclude the CC Only cases, the percentage of cases where the victim knows how their information was taken increases to 44%. See Appendix B – Table B10 and Appendix B - Figures B12-B13.

Table 16 shows a comparison between these results and other surveys. The percent of cases where our subjects answered 'Yes' is similar to the results of the Javelin surveys. If we add the number of cases where the subject answered 'Maybe', we get a proportion that is closer, but still much smaller, to that found in the Gartner survey. We do not know the exact wording of the question in the Gartner survey and this could explain the difference between their numbers, the Javelin numbers and our numbers.

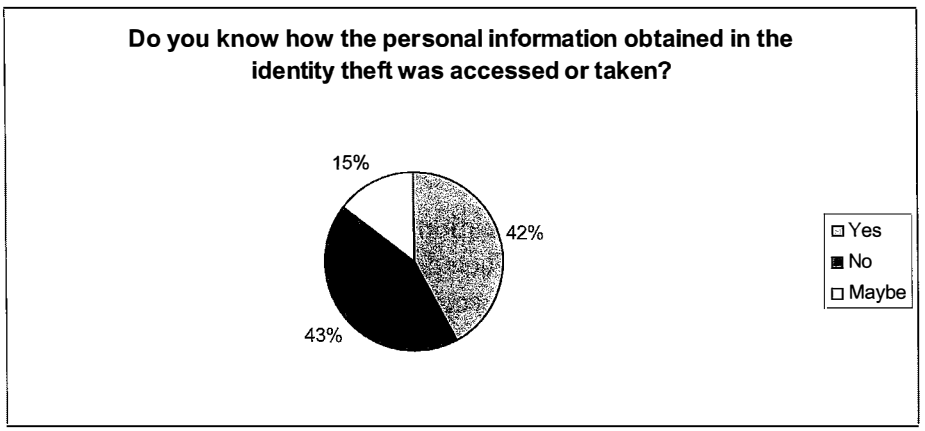


Figure 7 – Awareness of How

Table 16 – Awareness of how (comparison to other surveys)

		Other surveys						ORNEC 2006
		Gartner 2006	FTC 2003	Javelin 2004	Javelin 2005	Javelin 2006	NCVS 2004	
Awareness of how	Yes	78%	n/a	54%	47%	42%	n/a	42%
	Maybe							15%
	Total	78%	n/a	54%	47%	42%	n/a	57%

Appendix B contains cross tabs for Awareness of How the Information was Taken and Fraud Type (Table B7), Interval to Detection (Table B8 and Figures B9-B11) and Fraud Amounts (Table B9).

Table 17summarizes the awareness of how information was obtained by fraud type. We can see that victims of existing accounts fraud and other frauds are more likely to know or suspect how their information was obtained.

Table 17 – Awareness of how by fraud type

	Credit card fraud	Existing accounts fraud (non-credit card)	New accounts fraud	Other frauds	ID theft, but no frauds to date
Yes or Maybe	53.9	60.8	56.5	60.5	53.4
No	46.1	39.2	43.5	39.5	46.6
Number of cases	925	566	170	271	206

8.5 How information was obtained

Question 7 - How do you suspect the information was accessed or taken? (Check one)
or
Question 8 - How was the information accessed or taken? (Check one)

Table 18 shows an ordered list of the known or suspected methods of access to personal information. These cases represent 57% of the 1710 cases of IDT or IDF found in our study. In 43% of the cases, the victim does not know how the information was obtained.

The most common response is that the information was taken from the home (12% of all cases), followed by 'taken during a transaction conducted in person' (11%) and stolen wallets and purses (9%). Transactions conducted in person still account for almost four times as many cases as transactions conducted online, however we must remember that in 43% of the cases the method of information access is unknown. These unknown cases may represent a larger percentage of online threats than the known cases. In 26 or 2% of the total number of cases, the information was given in response to a phishing scam.

An examination of the open-ended comments associated with the 'Other' response shows multiple cases in the following additional categories:

- Known or accessed by friends or family (38 cases)
- Skimming operation or compromised automatic teller machines (ATMs) (20 cases)
- Stolen (other than wallet or purse) (20 cases)
- Online threats (other than transactions - e.g. key loggers, hacking, etc.) (9 cases)
- From credit card receipts or account statements (6 cases)
- Dumpster diving (5 cases)
- Shoulder surfing (4 cases)

Appendix B has tables show how the information was obtained cross tabbed by fraud type (Table B11), interval to detection (Table B12 and Figures B14-B23), and costs (Table B13 and Figures B24-B33).

Table 18 - How information was obtained

	Frequency			Percent of known or suspected cases (N=970)	Percent of total cases (N=1710)
	Suspected	Known	Total		
UNKNOWN			740	n/a	43%
It was taken from the home	43	156	199	21%	12%
It was taken during a business transaction conducted in person	74	122	196	20%	11%
Stolen wallet or purse	20	140	160	16%	9%
Other	37	118	155	16%	9%
Mail was intercepted or redirected	18	50	68	7%	4%
Lost wallet or purse	17	39	56	6%	3%
It was taken during a business transaction conducted online	17	34	51	5%	3%
It was taken from the customer records or employee records of an organization	15	34	49	5%	3%
The information was provided in response to an email or telephone call from what appeared to be a legitimate source	5	21	26	3%	2%
It was taken from public records	4	6	10	1%	1%
Total (not including Unknown)	250	720	970	100%	100%

For frauds involving new accounts and existing (non credit card) accounts, the information was most frequently reported to be taken from the home (30.2% and 32.6% respectively). Where credit card fraud was reported, the information was most frequently taken during an in-person business transaction (22.4% of cases) or from a stolen wallet or purse (20.2% of cases).

The interval to detection is shortest when wallets or purses are stolen or lost and longest when mail is intercepted and when there has been a data breach at an organization.

There is a significant difference between the CC Only cases and the Fraud (not CC) cases. See Appendix B – Table B14. In cases of simple credit card fraud, the most common known or suspected method of obtaining information is during a business transaction conducted in person (19.6%), followed by stolen wallets or purses (16.6%) and taken from customer or employee records of an organization (13.3%). When the frauds were more serious than just credit card fraud, the information was most likely to have been taken from the home (21%), followed by "other" (18.3%) and stolen wallet or purse (13.9%).

8.6 Interval to detection

Question 9 – What was the interval between the time the information was stolen and the victim's discovery of the theft? (Check one)

Figure 8 shows the distribution for the interval between the theft and its discovery. More than half of the cases were detected within a month of the theft. However, there are a substantial group of victims (12.7%) who are not sure when the theft occurred.

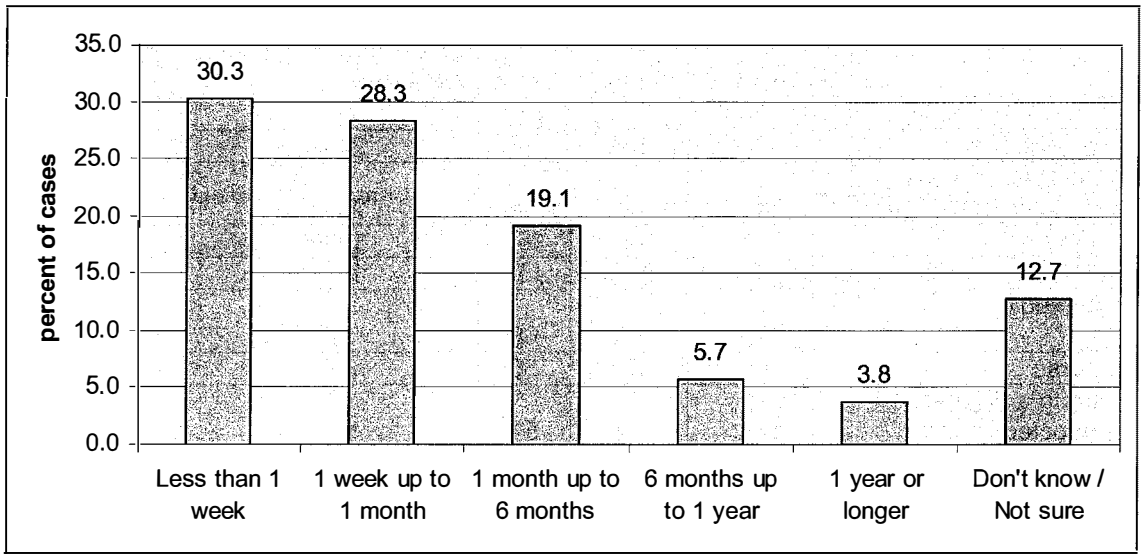


Figure 8 - Interval to detection

There is a significant relationship between the interval to detection and the average fraud amount. The results of an ordinal regression analysis are shown in Appendix B – Figure B34. This relationship is illustrated in Figure 9, below

There is also a significant difference in the interval to detection between CC Only and Fraud (not CC only) cases. Cases where the fraud was limited to credit card purchases are discovered more quickly than cases where the frauds are more extensive. This is shown in Figure 10 below and in Appendix B - Table B19.

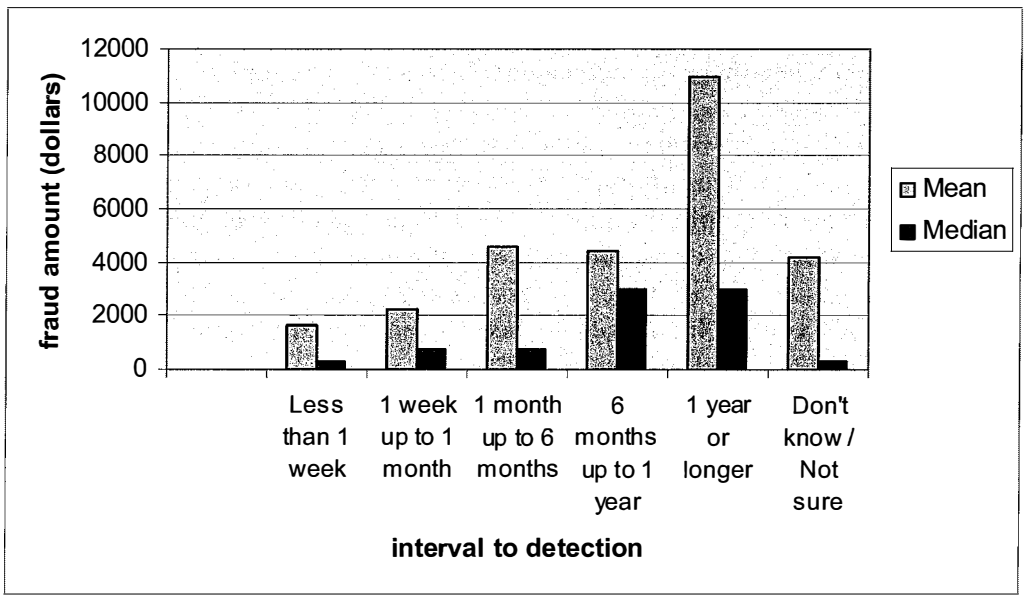


Figure 9 – Interval to detection and average fraud amount

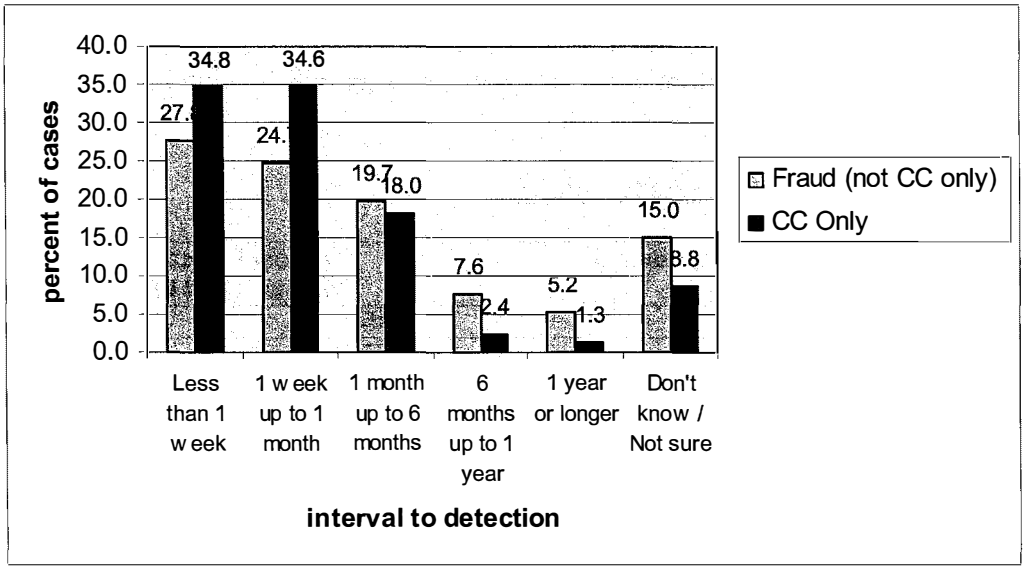


Figure 10 - Interval to detection for CC Only and Fraud (not CC only) cases

8.7 Awareness of what information was taken

Question 10 - Do you know what information or documents were accessed? (Yes/No)

Question 10 asked if the victim knew what information was accessed or taken. As Figure 11 shows, in 1117 or 65% of our 1710 cases the victim knows what information was obtained.

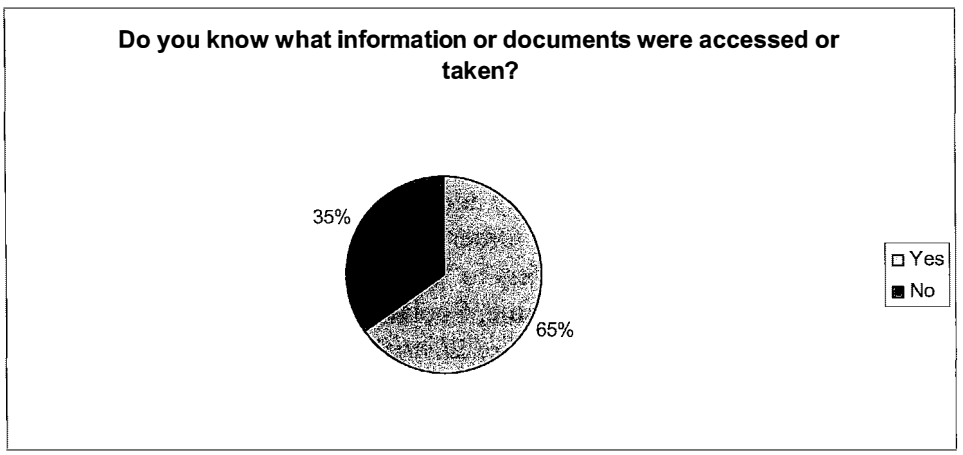


Figure 11 – Awareness of what information was taken

8.8 What information was accessed or taken

Question 11 – What information was accessed or taken? (multiple response)

Table 19 shows the frequencies of responses to Question 11. The most common information accessed was credit card information, reported in 57.7% of the cases where the victim knew what

information was accessed. Name and address were reported in 42.7% and 33.7% of the cases, respectively. Respondents were asked to select all of the responses that applied, so the total number of responses (2910) is more than the number of respondents who knew what information was taken (1117).

Table 19 – What information was accessed or taken?

What information was accessed or taken?	Frequency	Percent of cases when known (N=1117)
Credit card information	645	57.7
Name	477	42.7
Address	376	33.7
Bank account number(s)	316	28.3
Birth date	266	23.8
Social insurance number	202	18.1
Driver's license number	178	15.9
Personal Identification Number(s)	166	14.9
Other	128	11.5
Password(s)	104	9.3
Mother's maiden name	52	4.7
Total	2910	260.5

8.8.1 Level of information

In their examination of data breaches, ID Analytics makes a distinction between account-level information and identity-level information (ID Analytics 2006). Because accounts can be closed and new accounts created, the damages resulting from a breach or theft involving only account level information are generally smaller than those associated with identity level breaches or thefts. ID Analytics describe account level information as "a consumer name in conjunction with a credit card number, and possibly additional information such as expiration date of the account and CVS (Card Verification System) number" (ID Analytics 2006, p. 7). This is basically the information available on a credit card. Identity level information is described as "a consumer name in connection with an SSN, and possibly address, date-of-birth, or associated phone numbers as well" (ID Analytics 2006, p. 7). Other sources make a similar distinction where the term *personally identifiable information* refers to "any information that can be used to distinguish or trace an individual's identity – such as name, Social Security Number, driver's license number, and mother's maiden name" and *other means of identification* which includes "account information such as credit or debit card numbers" (GAO (General Accountability Office) 2007, p. 2). In the United States, credit and debit cards are legally defined as access devices and not identification documents, whereas identification documents are issued by government agencies (Lyons 2006).

The difference between account level and identity level information is reflected in their 'black market' values. An IBM study found that "2000 credit card records are worth the same as 40 standard identities", where a 'standard identity' included a name, address, phone number and date of birth. Five 'complete identities', which also includes mother's maiden name, bank account number and bank account password are worth as much as 2000 credit card record (Ollman 2007).

We created new variables to classify cases according to the level of information accessed or taken (Question 11). An "account level" flag was created if the respondent indicated that credit card information, bank account number(s), passwords or PINs had been obtained in the IDT. These can all be easily changed to stop the fraudulent activity. An "identity level" flag was created if address, social insurance number, birth date, driver's license number, or mother's maiden name was obtained. These identifiers are not as easily changed as account information. In cases where 'Other' information was indicated, the open-ended descriptions were examined and classified as either account level or identity level where possible. Finally, an "information type" variable was created for each case to indicate whether the information obtained was identity level only, account level only, or both levels. Of the 1710 cases, the victim knows what information was taken in 1117 cases. Of these, our new variables classify 1093 of these cases. In the remaining 24 cases, we cannot determine what information was obtained.

When we look at the 65% of victims who know what information was obtained, we find that in 61% of the cases only account level information was obtained. Figure 12 shows the distribution of cases where the information obtained was account level only, identity level only, or both account and identity level.

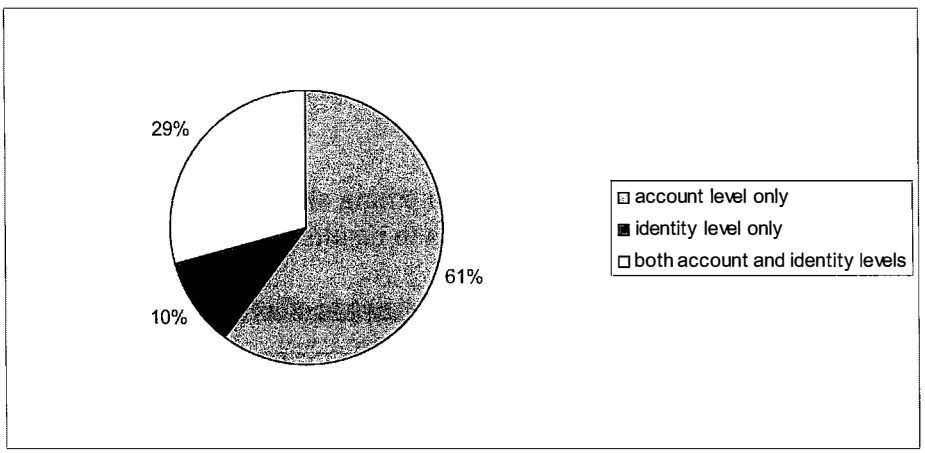


Figure 12 - Level of information accessed or taken (of cases when what information was accessed or taken is known (N=1117)

Our results show that the costs of the IDF are highest when both identity level and account level information is obtained. Table 20 shows the fraud amount, victim's time to resolve, and out-of-pocket (OOP) costs according to the level of information accessed. The difference is most evident when we look at victim costs (both time to resolve and out-of-pocket costs). When both identity and account level information is accessed, the victim's costs in both time and money are more than three times the costs when just account level information is accessed.

In 79.7 % of CC Only cases, only account level information was obtained. In 20.0 % of these cases the perpetrator was reported to have also obtained identity level information, but this information was apparently not used to commit further frauds. See Appendix B - Table B30.

Table 20 - Average costs by level of information accessed

	Count	Mean fraud amount	Mean victim's hours	Mean OOP costs
Account level only	660	$2242	15.5	$236
Identity level only	114	$1970	37.2	$343
Both account level and identity level	319	$5152	48.6	$919
Total	1093	$3063	27.4	$447

8.9 Awareness of the perpetrator's identity

Question 12 - 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.) (yes/no)

Question 12 asked if the victim knows "anything at all about the person who took the information". The pretests for the NCVS survey showed that respondents had a difficult time with similar questions. In some cases, they thought that they must know the person's name in order to give a positive response to the question (Hughes 2004). We therefore provided an example, adding "For example, you may not know their name, but know where they worked or lived" at the end of the question.

In 35% of the reported cases, the victim knew something about the perpetrator of the theft or fraud. Table 21 shows how this result is compares to results found in other surveys.

Table 21 – Awareness of the perpetrator's identity (comparison to other studies

	Other Surveys					ORNEC 2006
	FTC 2003	Javelin 2004	Javelin 2005	Javelin 2006	NCVS 2004	
Awareness of who	26%	unknown	36%	31%	unknown	35%

Appendix B contains tables showing awareness of who committed the theft or fraud cross tabbed by fraud type (Table B31), interval to detection (Table B32) and fraud amount (Table B33).

In general, victims are not as likely to know the identity of the perpetrator when the frauds involve credit cards (only 30.7%) and when a theft only has occurred (26.%). They are more likely to know the identity of the perpetrator when the frauds involve new accounts (47.1 percent of cases), existing accounts (44.2%) and other frauds (41.7%). Victims were also more likely to know the identity of the perpetrator when the interval to detection was longer than 6 months and when the cost of the fraud was over $5000. This indicates that perpetrators close to the victim may be able to hide the crime for a longer period and, perhaps because of this, can gain more in terms of proceeds from the crime.

Victims of credit card fraud only are less likely to know the identity of the perpetrator. Almost 40% of the victims of more serious frauds know the identity of the perpetrator, while only 27% of the victims of credit card fraud only know the perpetrator's identity. See Appendix B, Table B34.

8.10 Identity of the perpetrator

Question 13 - Which of the following best describes the person who took the information? (single response)

Figure 13 shows the result of Question 13, where those who indicated that they knew the identity of the perpetrator were asked to indicate what description best fit the perpetrator. The most common response was that the perpetrator was a relative, accounting for 25.9% of cases where the perpetrator was known, and 9.1% of all cases. Appendix B contains tables showing the results of Question 13, including cross tabs by fraud type (Table B37), interval to detection (Table B38) and fraud amount (Table B39).

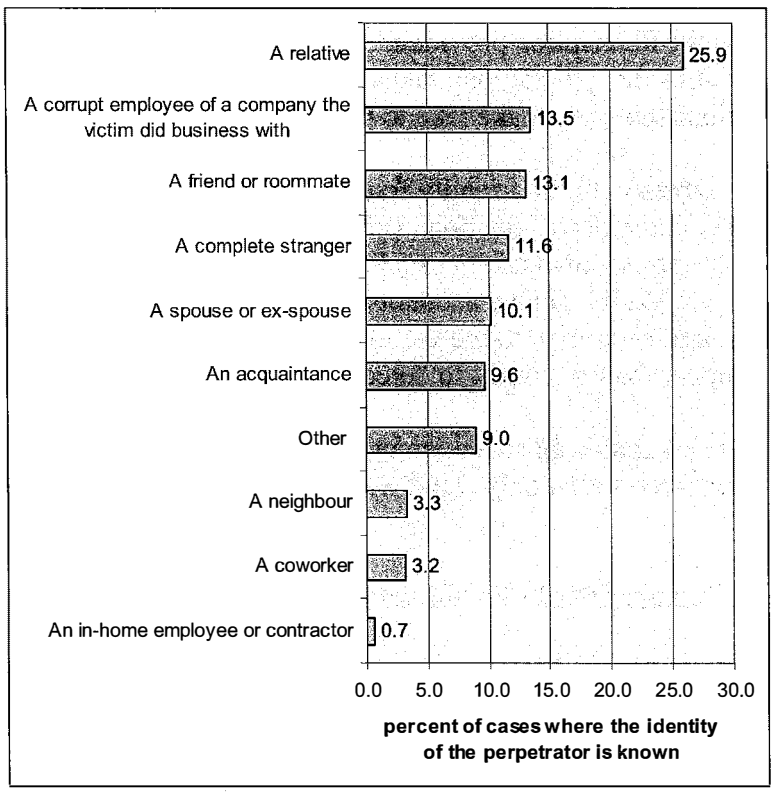


Figure 13 – Identity of the perpetrator

We examined the open-ended comments when we asked people to be specific about their choice of the 'Other" response. Of the 54 'other' responses, ten specified family members if we include in-laws and ex-spouses as family. Twenty-four specified someone else who was known to the victim (friends, relatives of friends, employers, employees, etc.) Fourteen described strangers and in six cases we were unable to determine if the perpetrator was known to the victim prior to the theft.

We find a difference between the victims of CC only and Frauds (not CC only) and the identity of their perpetrators. Victims of credit card fraud only were almost 4 times as likely to report that the perpetrator was an employee of a firm that the victim did business with. In fact, this was the most frequent response for CC only victims (28.5%), followed by a relative (17.6%) and a complete stranger (15.8%). Victims of more serious IDFs were most likely to report that the victim was a relative (29.1%), followed by a friend or roommate (15.8%) and a spouse or ex-spouse (11.9%). See Appendix B - Table B36 for additional details.

8.10.1 Friendly fraud and stranger fraud

Appendix B – Table B40 describes how we mapped the responses to Question 13 into three categories – friendly fraud, stranger fraud and unknown. Remember that in 65% of cases the identity of the perpetrator is not known. Where the identity of the perpetrator is known, in 66% of the cases the perpetrator is someone known to the victim (family, friend, acquaintance, neighbour, etc.). We will use the term friendly fraud to describe these cases. In 25% of the cases the perpetrator is a stranger and in the remaining 10%, although the respondent indicates that they know something about the perpetrator we can not tell whether that person was known to them prior to the theft from the description provided.[11] The friendly fraud/stranger fraud distinction is useful because the actions that people may take to protect themselves from friendly fraud are different than the actions that they make take to protect themselves from stranger fraud.

Appendix B contains tables with the friendly fraud/stranger fraud variable cross tabbed against fraud type (Table B41), interval to detection (Table B42), fraud cost (Table B43), victim's hours to resolve (Table B44) and out-of-pocket costs (Table B45). We can see that when the identity of the perpetrator is known, 82.5% of new accounts frauds and 81.2% of existing accounts frauds were committed by someone known to the victim. Friendly frauds are also associated more with cases where it took longer than 6 months to detect the fraud.

Cases where more serious frauds occurred are more likely to be friendly fraud (72.8% of these cases) than cases where credit card only fraud was committed (47.9%). See Appendix B - Table B46.

Table 22 - Comparison of Costs - Friendly Frauds and Stranger Frauds

	Fraud Cost	Victim's Hours to Resolve	Out-of-pocket cost
Friendly frauds	$5278	41 hours	$770
Stranger frauds	$2698	20 hours	$259

Table 22, above, shows the average costs associated with friendly fraud and stranger fraud when the identity of the perpetrator is known. The average fraud cost for friendly frauds is double the fraud cost for stranger fraud. When we look at victim costs, the average hours that the victim spends to resolve the problem for friendly fraud is double that for stranger fraud and the victim's out-of-pocket costs is three times as much.

[11] After the examination and re-classification of the "other" responses as described previously in this section, the percentages are found to be 72% friendly, 27% stranger and 1% unknown..

8.11 Frauds committed or attempted

Question 14 – Which of the following frauds were committed or attempted using the stolen identity? (multiple response)

Question 14 asked for multiple responses identifying the different types of frauds that were attempted or committed. Table 22 shows the frequencies for each type of fraud that was specified in the responses. Since more than one type of fraud can occur in one episode of IDF, there are more responses (2403) than victim cases (1710) and the total percentage is more than 100%..

Table 22 – Frequencies of Fraud Types

Types of fraud committed or attempted	Number	% of cases
Purchase(s) made on an existing credit card account	832	48.7
Money taken from an existing bank account	416	24.3
No frauds have been discovered to date	206	12.0
Charge(s) to an existing phone or utility account	159	9.3
Other	133	7.8
New credit card account(s) opened in the victim's name	119	7.0
New phone or utility account(s) opened in the victim's name	103	6.0
Crime(s) committed using the victim's name	68	4.0
Loan(s) taken out in the victim's name (e.g. personal, student, auto)	62	3.6
Take over of existing credit card account(s)	51	3.0
Take over of existing phone or utility account(s)	47	2.7
New bank account(s) opened in the victim's name	41	2.4
Take over of existing bank account(s)	39	2.3
Government benefits obtained under the victim's name	32	1.9
Home or apartment rented in the victim's name	30	1.8
Tax fraud committed under the victim's name	28	1.6
Employment gained under the victim's name	24	1.4
Mortgage(s) taken out on the victim's home	9	0.5
The victim's home was sold	4	0.2
Total	**2403**	**140.5**

The most common type of fraud experienced was purchases made on an existing credit card account (48.7% of the cases), followed by money taken from an existing bank account (24% of the cases) and cases where there has been no frauds discovered to date (12% of the cases). The remaining frauds each were experienced in less than 10% of the cases.

A detailed examination was made of the cases where a mortgage was taken out on a home or the victim's home was sold. This report can be found in Appendix B – Figure B42. We believe that only three of the mortgage cases and none of the home sold cases are truly cases of mortgage fraud or land titles fraud. In the remaining 10 cases, we suspect that taking out a mortgages or the sale of a house was a consequence of an IDF and not part of the fraud itself.

We can classify the frauds according to the type of business that was targeted. In Figures 14 to 17 we show the incidence rates of various frauds committed against credit card companies, banks, phone and utility companies and others.

Account-related frauds (against credit card companies, banks and phone and utility companies) are most commonly of the type where an existing account is accessed and charged. The next most common fraud is the opening of a new account in someone's name. The least common type of fraud is the 'take-over' of an existing account, for example, by changing the mailing address or adding additional account holders.

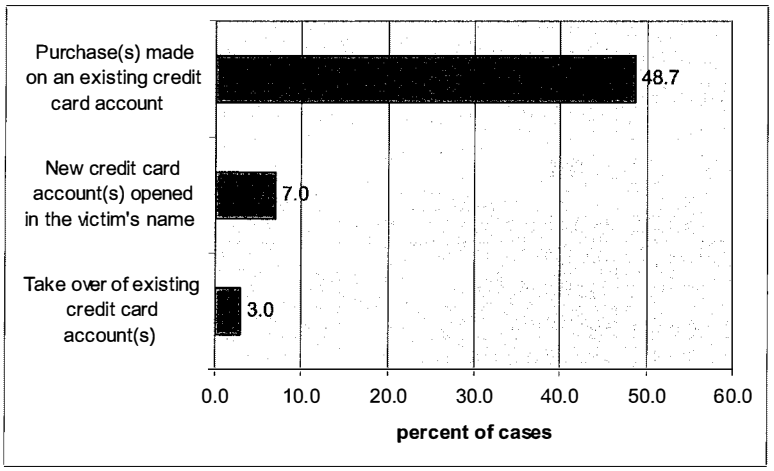


Figure 14 – Types of fraud committed or attempted (credit cards)

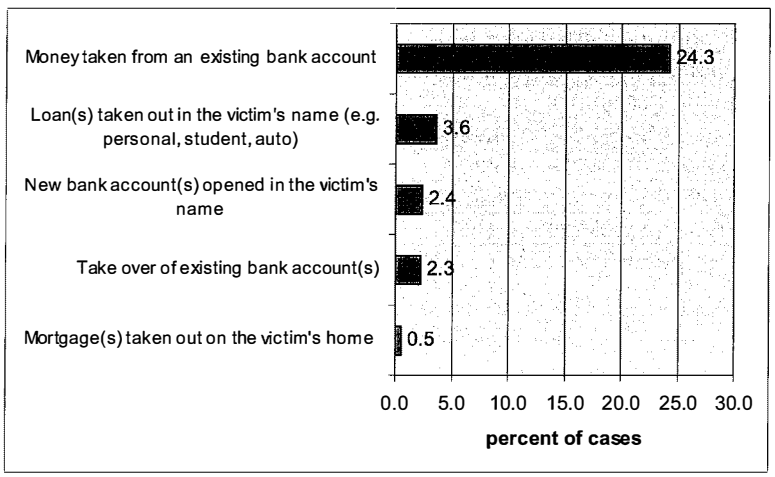


Figure 15 - Types of fraud committed or attempted (banks)

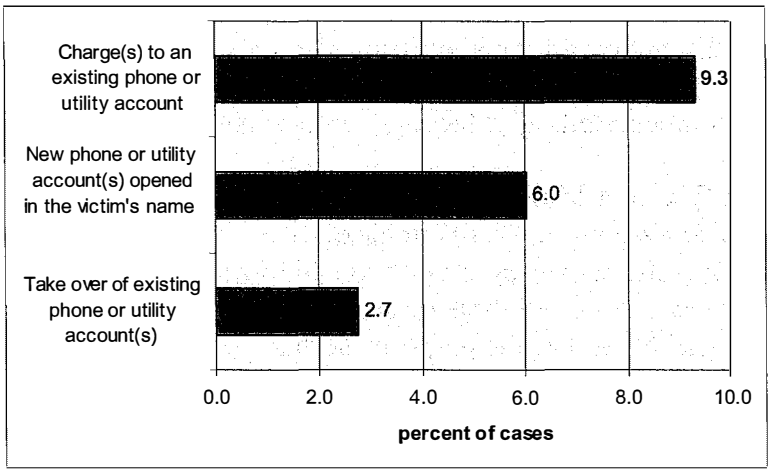


Figure 16 – Types of fraud committed or attempted (phone or utility)

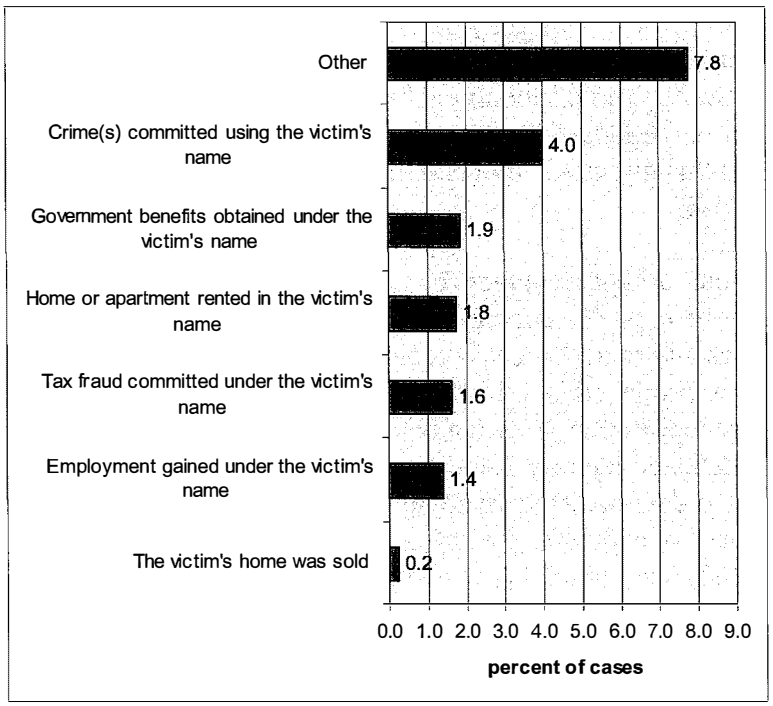


Figure 17 – Types of fraud committed or attempted (other)

8.12 Document breeding

Question 15 – To your knowledge, did the perpetrator use the information to obtain or counterfeit any additional identification documents in the victim's name?

Question 16 – What identification documents did the perpetrator obtain or counterfeit? (multiple response)

Certain identity documents are more valuable to identity thieves than others. Document breeding refers to the practice of using one type of identification document to apply for another type of

document. An example would be to use a birth certificate to obtain a passport. Some of the more valuable documents that are used for breeding are also subject to sophisticated counterfeiting operations. It is usually only after an investigation by police that the victim is notified that document breeding or counterfeiting of these documents has taken place.

The raw results from Question 15 indicate that the victim is aware that document breeding or counterfeiting took place in 83 or 4.9% of our cases. See Appendix B – Table B49. However, when we look at the specific responses in Question 16, twenty- five of these responses are in the 'Other" category. An examination of these responses shows that there was some confusion about what an identity document was. For the purposes of this question, we do not consider credit and debit cards to be 'identity documents' (Lyons 2006). While these cards may be counterfeited as part of an IDF, they are not generally considered useful as breeder documents. If we eliminate the cases where only "Other" was chosen and an 'identity document' was not specified, the number of cases where document breeding occurred is reduced to 60, or 3.5% of our cases.

Eliminating cases where there were only purchases made on existing credit cards increases the percentage of cases where document breeding occurred, but these cases are still just a small percent of the total. Some form of document breeding is known to have occurred in 72 or 6.6% of the cases of more serious frauds. When we again eliminate "other" responses that did not specify an identity document this number is reduced to 54 or 4.9% of the Fraud (not CC) cases. See Appendix B – Table B49.

The specific frequencies and percentages for various breeder documents are shown in Table 23. Driver's licenses are the most common breeder document acquired or counterfeited, appearing in two thirds of the cases where document breeding occurred. Social insurance cards and health cards were acquired or produced in a third of the cases of known document breeding. Multiple false documents were reported in 19 or almost one third of the cases. In two cases, respondents reported that all of the listed identity documents were acquired by the perpetrator and in four cases three of the listed documents were acquired. Since more than oone type of document may have been counterfeited or acquired, the column total (87) is more than the cases of known document breeding (60) and the total percentage is greater than 100%.

Table 23 – Document breeding (frequencies)

Documents counterfeited or acquired	Frequency	% of cases
Passport	5	8.3
Social insurance card	22	36.7
Health card.	20	33.3
Driver's license	40	66.7
Other	0	0.0
Total	**87**	145.0

We would suspect that cases where document breeding occurred would correspond to higher costs. We can see from Appendix B, Figures B51, B52 and B53, that fraud costs, victim's hours to resolve and out-of-pocket costs are all higher when document breeding occurs. Table 24, below, shows the average costs when the victim is and is not aware that document breeding occurred.

Table 24 – Document breeding and average costs

Awareness of document breeding	Fraud amount		Victim's hours to resolve		Out-of-pocket cost	
	Mean	Median	Mean	Median	Mean	Median
Yes	$9,541	$3,000	70	25	$1,741	$75
No	$2,887	$750	25	5.5	$370	$25

8.13 Fraud amount

Question 17 – How much money did the perpetrator obtain through the theft? (Include the value of merchandise, credit, loans, cash, services and anything else the person may have obtained.) (single response)

Fraud amount is the first of three quantitative measures of the cost of IDF. The question asked respondents to choose a categorical 'range', for example $100-$499. To find average costs, variables representing the mid-point of each range were created in SPSS. This is the method used to calculate mean and median in the Javelin studies (Javelin 2006). Response categories and midpoint values are shown in Appendix B, Tables B54-B56.

The cumulative frequencies of fraud amounts are shown in Fig. 18. Two-thirds of the cases of fraud resulted in fraud amounts of less than $1000. Overall the mean fraud amount was $3209, but this includes some extreme cases. Interpolating between the category midpoints, the median fraud amount is $595.

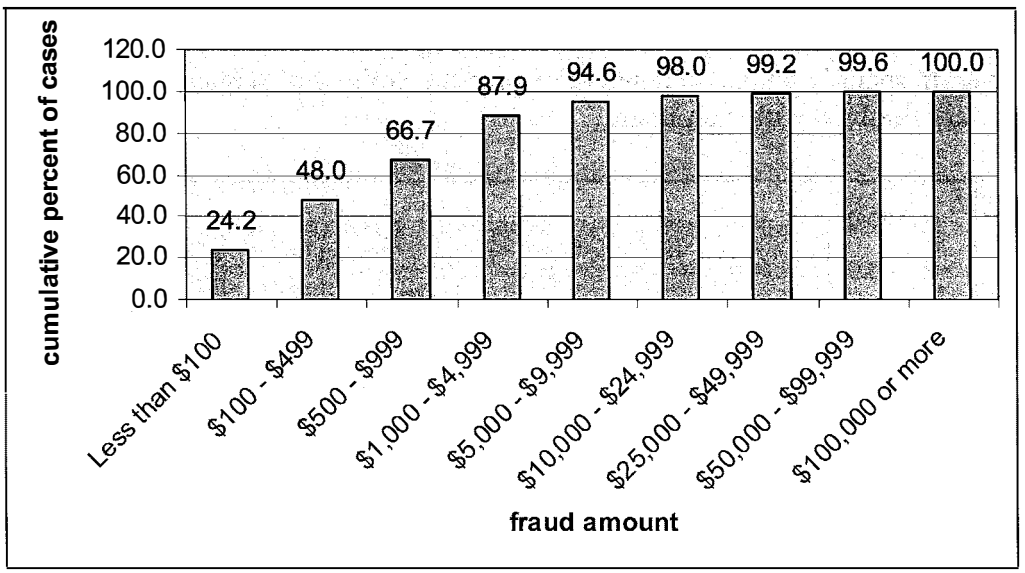


Figure 18 – Cumulative frequency of fraud amounts

While the median fraud amounts for CC Only and Fraud (not CC only) are very similar at $601 and $588 respectively, the average fraud costs are quite different. The average fraud amount when purchases are made on an existing credit card is $1745, whereas the average fraud amount for more serious frauds is $4032. We are therefore seeing more extreme cases in the Fraud (not CC only) category. See Appendix B, Tables B54 and B57 for details.

Cross tabs for fraud amount have been discussed with many of the other variables. A complete list of cross tabs that include fraud amounts is shown in Table 26

Table 26 – Cross references to fraud amount cross tab tables in Appendices

Cross Tab Variable	Location
Method of Detection	Appendix B – Table B4
Awareness of How Information was Obtained	Appendix B – Table B9
How Information was Obtained	Appendix B – Table B13 and Figures B24-B32
Interval to Detection	Appendix B – Table B17 & B18, Figures B34 & B35
Level of Information Accessed	Appendix B – Tables B24 & B25
Awareness of Who	Appendix B – Table B33
Identity of Perpetrator	Appendix B – Table B39
Friendly Fraud/Stranger Fraud	Appendix B – Table B43 and Figure B39
Awareness of Document Breeding	Appendix B – Table B51

Note: Appendices are available on request from archer@mcmaster.ca or sprouls@mcmaster.ca

8.14 Victim's hours to resolve

Question 18 - How many hours of the victim's own personal time have been spent resolving problems associated with this episode of identity theft?

The second qualitative measure of costs is the number of hours that the victim spent to resolve the problems associated with the IDT or IDF. From Figure 19 we can see that in two thirds of the cases the victim spent less than 10 hours to resolve the problems. In one quarter of the cases, the problems were resolved within an hour.

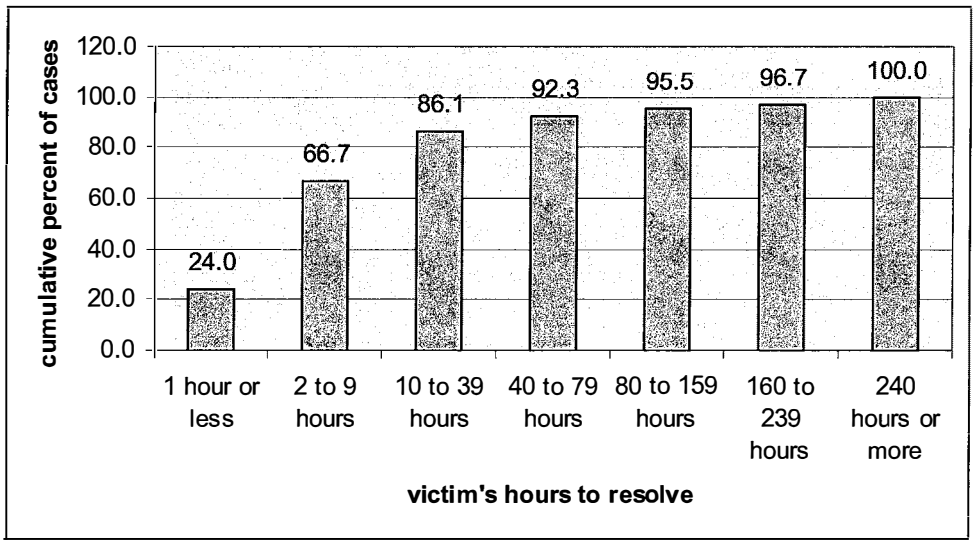


Figure 19 – Cumulative Frequency of Victim's Hours

Overall, the mean number of hours to resolve problems was 27 hours; however this reflects some extreme cases. The median number of hours, obtained by interpolating between category midpoints is 8 hours.

If we look at cases where the only fraud was purchases on an existing credit card, the victim's hours is reduced to a mean of 12 hours and a median of only 5 hours. For more serious frauds, the mean is 36 hours and the median is 12 hours. See Appendix B - Tables B55 and B58 for details.

Cross tabs for victim's hours to resolve have occasionally been discussed with other variables. A complete list of cross tabs that include victim's hours is shown in Table 27

Table 27 – Cross references to victim hours cross tab tables in Appendices

Cross Tab Variable	Location
Method of Detection	Appendix B – Table B5
Level of Information Accessed	Appendix B – Table B26 & B27
Friendly Fraud/Stranger Fraud	Appendix B – Table B44 and Figure B40
Awareness of Document Breeding	Appendix B – Table B52

Note: Appendices are available on request from archer@mcmaster.ca or sprouls@mcmaster.ca.

8.15 Out-of-pocket costs

Question 19 - How much of the victim's own money was spent to resolve problems associated with the identity theft? (Include costs for postage, copying, legal fees, notarized documents, and payment of any fraudulent debts.) *(Check one)*

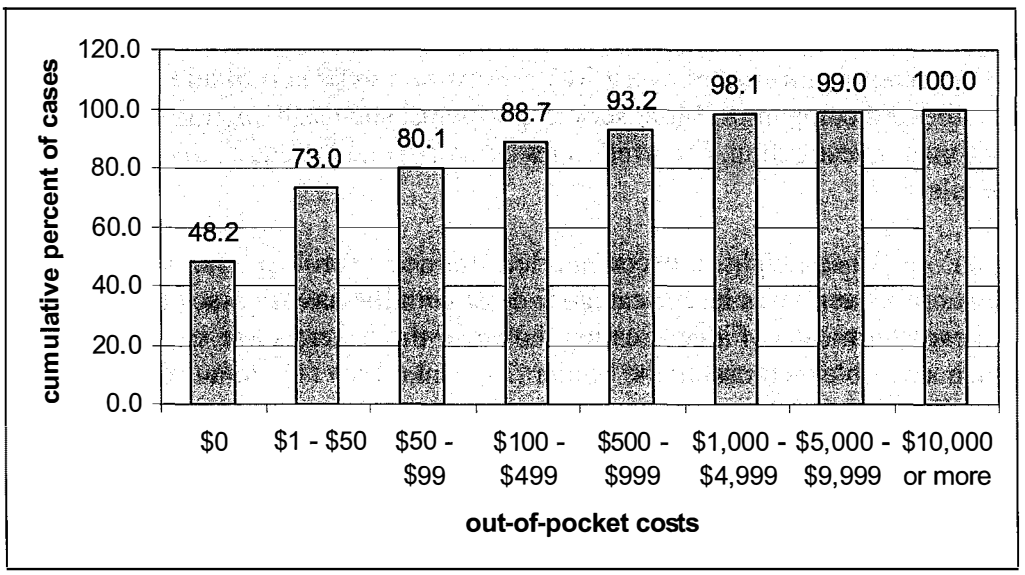


Figure 20 – Cumulative Frequency of OOP Costs

The third quantitative measure of costs is the victim's out-of-pocket (OOP) costs to resolve problems associated with the IDT or IDF. Figure 20 shows the cumulative frequency of the response to this question. In almost half of the cases, victims report that they experienced no

OOP costs. There were some extreme cases, however and as a result the mean reported OOP costs were $436. Using interpolation, from 0 to the midpoint of the first category, the median response is only $4.

Where the only fraud committed was purchases on an existing credit card the average OOP cost was $137, and the median cost was $0. In cases with more serious frauds the mean OOP cost was $604 and the median cost was $18. See Appendix B, Tables B56 and B59, for details.

Cross tabs for OOP costs have been occasionally discussed with other variables. A complete list of cross tabs that include OOP costs is shown in Table 29

Table 29 – Cross references to OOP costs cross tab tables in Appendices

Cross Tab Variable	Location
Method of Detection	Appendix B – Table B6
Level of Information Accessed	Appendix B – Table B28 & B29
Friendly Fraud/Stranger Fraud	Appendix B – Table B45 and Figure B41
Awareness of Document Breeding	Appendix B – Table B53

Note: Appendices are available on request from archer@mcmaster.ca or sprouls@mcmaster.ca.

8.16 Other costs

Question 20 - What other (non-monetary) costs resulted from the identity theft? (multiple response)

In question 20, respondents were asked to indicate if there were other consequences or costs to the IDT or IDF. The frequency of responses is shown in Figure 21. In over half of the cases, there were no additional costs to the victim, other than the time and OOP costs reported in questions 18 and 19. Approximately one out of every five victims had some sort of additional problem with banks or credit card companies. More serious problems, such as being turned down for a loan or facing a criminal investigation, occurred in less than 10% of the cases. See Appendix B – Table B60 for details.

Of the "other" responses, eight subjects reported strained or broken relationships with friends and family. Most of the responses in this category dealt with the hassles associated with replacing credit/debit cards or means of identification, however there were some serious consequences reported such as problems crossing the border (3), bankruptcy (1), defaulting on a mortgage (1) and eviction (1).

When we look at the differences between victims of simple credit card fraud and more serious frauds, 70.9% of the victims of simple credit card reported no additional costs while only 42% of more serious frauds reported no additional costs. The victims of more serious frauds were more than 3 times as likely to report being turned down for a loan, being contacted by a debt collector or creditor, having banking problems, or having utilities cut off or being denied new service. See Appendix B – Table B61 for details.

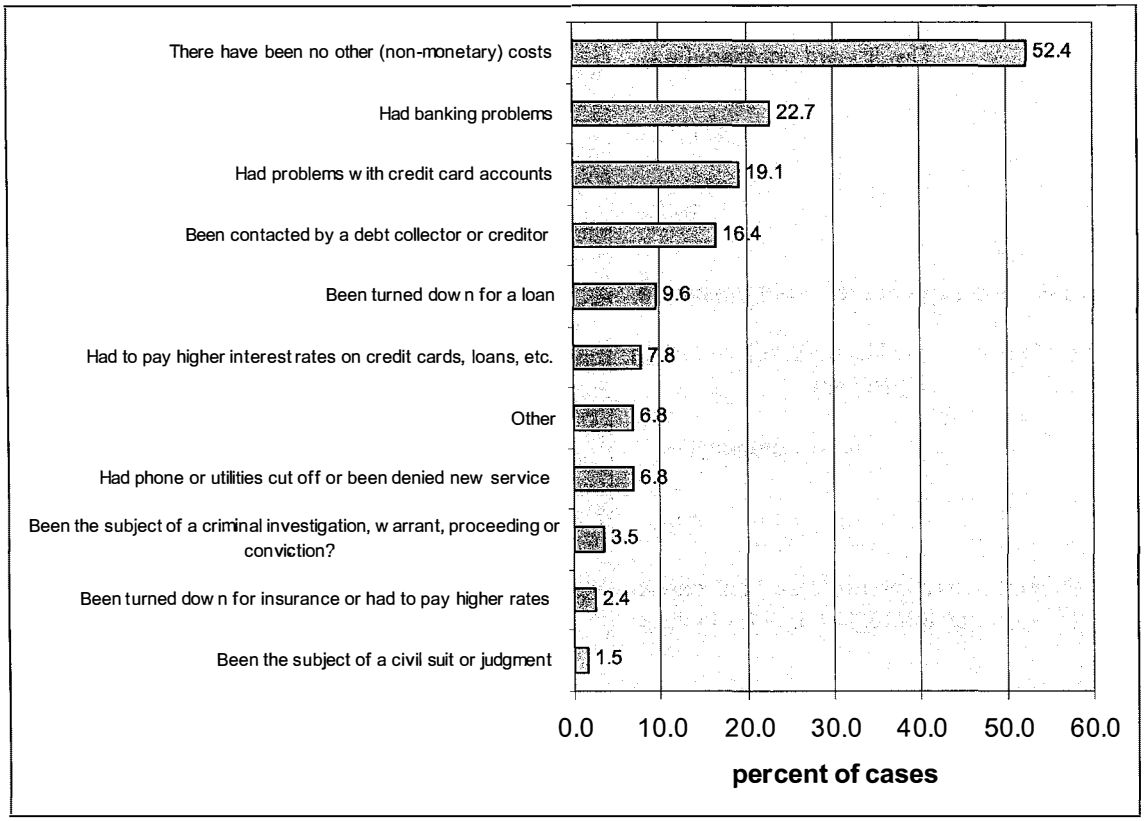


Figure 21 - Frequency of Other Costs

8.17 Reporting

Question 21 – To whom was the identity theft reported? (multiple response)

Frequencies for the responses to question 21 are shown in Figure 22, below and in Tables B62 and B63 in Appendix B. Note that this was a multiple response question, so the percentages in Table 26 and Figure 22 do not equal 100%.

Almost half of the victims reported the fraud to a credit card company and almost 40% reported it to their bank. Surprisingly, while 32% reported to the police, only 2% reported to PhoneBusters (the RCMP and OPP's fraud call centre). This would indicate that either the police departments are not referring people to PhoneBusters or that victims do not make the call even after a referral.

Seventeen of the 117 victims who specified 'other" merely clarified that the bank, credit card company or police first contacted the victim about the fraud and that there was no reason for the victim to notify them. Several of these victims commented that they did not know if the bank or credit card company reported the fraud to other authorities. Eleven subjects reported that they dealt with the perpetrator or the perpetrator's family directly.

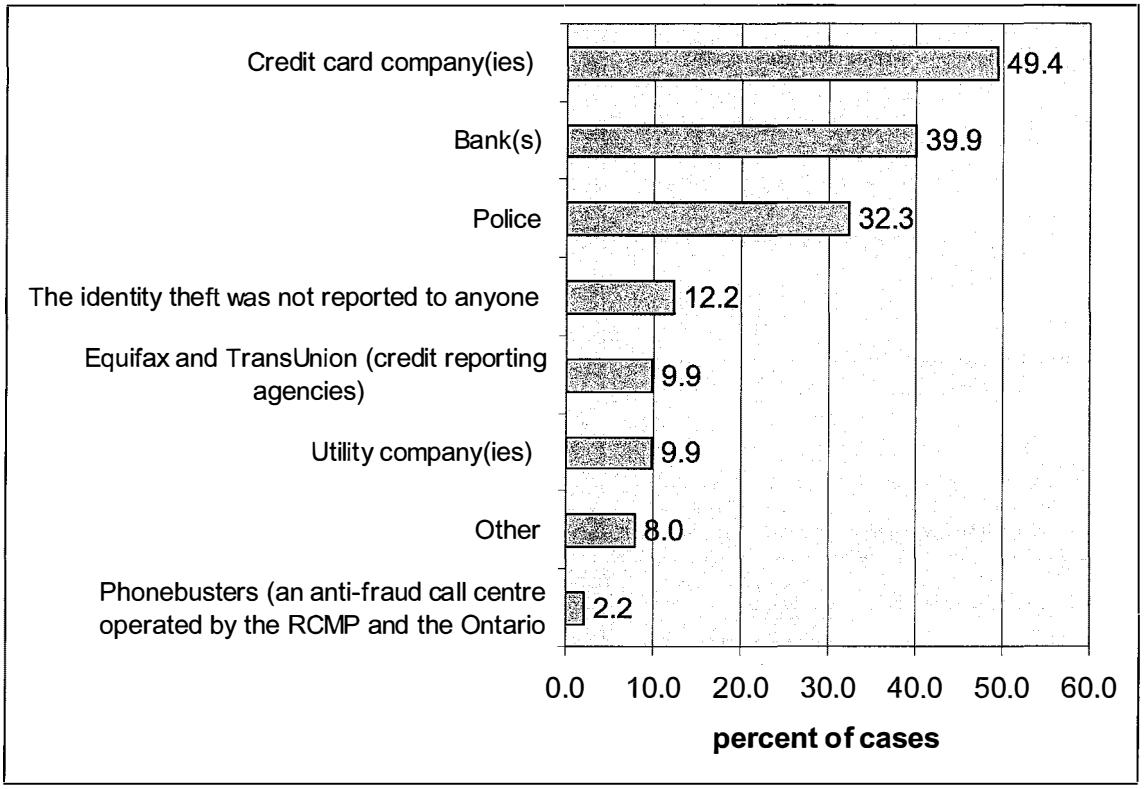


Figure 22 – Frequencies for reporting

Twelve percent of victims did not report the theft or fraud to anyone. We suspect that many of these cases are friendly fraud. If we look at the differences between reporting characteristics of friendly fraud victims and all victims (Table 29) we see that victims of friendly fraud are twice as likely to say that the IDT or IDF was not reported to anyone. Copes, Kerley et al (2001, p.358) reference another study that also found victims were twice as likely to report frauds if the perpetrator was a stranger.

Victims of friendly fraud are also less likely to have reported the fraud to banks and credit card companies. However, they are more likely to have reported the fraud to a utility company. This may be because friendly fraud makes up a higher percentage of utility frauds such as phone frauds.

Seventy-eight percent of the victims of simple credit card fraud reported it to their credit card companies. This compares to 63% reported in a US study (Copes, Kerley et al. 2001). Only 8.3 % of the victims of credit card fraud and 14.4% of the victims of more serious frauds report that they had not reported the IDF to anyone. The larger percentage associated with the more serious frauds is probably related to the fact that more of these frauds are friendly frauds. Other differences in reporting, such as reporting to utilitcompanies and banks, reflect the nature of the non-CC frauds. Details of reporting behaviour cross tabbed by CC Only and Fraud (not CC only) are shown in Appendix B, Table B64.

Table 29 - Reporting and friendly fraud

To whom was the identity fraud reported?	Percent of all cases	Percent of friendly fraud cases	Significance level [1]
Phonebusters (an anti-fraud call centre operated by the RCMP and the Ontario Provincial Police)	2.2	1.0	n/a
Other	8.0	7.3	ns
Utility company(ies)	9.9	14.6	***
Equifax and TransUnion (credit reporting agencies)	9.9	8.3	ns
The identity theft was not reported to anyone	12.2	24.7	***
Police	32.3	31.0	ns
Bank(s)	39.9	33.8	**
Credit card company(ies)	49.4	31.5	***
Total	163.7	152.2	
Number of cases	1710	397	

[1] Difference in proportions test:
Significant at 99% CI ***
Significant at 95% CI **
Significant at 90% CI *
Not significant ns
Cannot be calculated n/a [does not satisfy condition that n*p >= 5 and n(1-p) >= 5]

8.18 Episode status

Question 22 – Do you believe that the misuse of the victim's identity has stopped? (Yes/No/Don't know)

Question 23 – Do you believe that all of the problems associated with this episode of identity theft have been resolved? (Yes/No/Don't know)

Questions 22 and 23 determine the current status of the episode of IDT or IDF that is being described. Question 22 first asks if the subject believes that the misuse of identity has stopped. If the response to question 22 is positive, we then ask if all of the associated problems have been resolved. Tables B65-B66 in Appendix B contain the detailed results. From these two questions we can classify the case into one of three categories:

- misuse ongoing
- misuse stopped but problems not resolved
- resolved

Between 10 percent and 20 percent of respondents were unsure if the misuse had stopped (18.1%) or if all problems had been resolved (10.1%). These results indicate that there is lingering anxiety over the IDF even once it has been detected and initial actions taken. For both questions we include the 'don't know' responses with the negative responses in order to arrive at our status categories

Table 30 shows the distribution of cases within the three categories of status. In 23 percent of cases, the victim believes that the misuse of their identity is ongoing. Fourteen percent believe that the misuse has stopped, but do not believe that they have resolved all of the problems associated with this episode of IDF.

Table 30 – Episode status (frequencies)

Status	frequency	percent of cases
Misuse ongoing	393	23.0
Misuse stopped but problems not resolved	243	14.2
Resolved	1074	62.8
Total	1710	100.0

8.19 Time to resolve

Question 24 – After the identity theft was first detected, how long was it before all of the associated problems were resolved?

When the response to Question 23 was positive, Question 24 tried to determine the interval between when the theft was first discovered and when all of the problems had been resolved. Figure 23 shows how long it took to resolve all of the problems associated with the described episode of IDT or IDF. Two thirds of the cases were resolved within one month of detection. See Table B67 in Appendix B for frequencies. More serious frauds took longer to resolve than simple credit card frauds, although the difference is not as large as we might think. See Appendix B - Table B68 for a cross tabbed table.

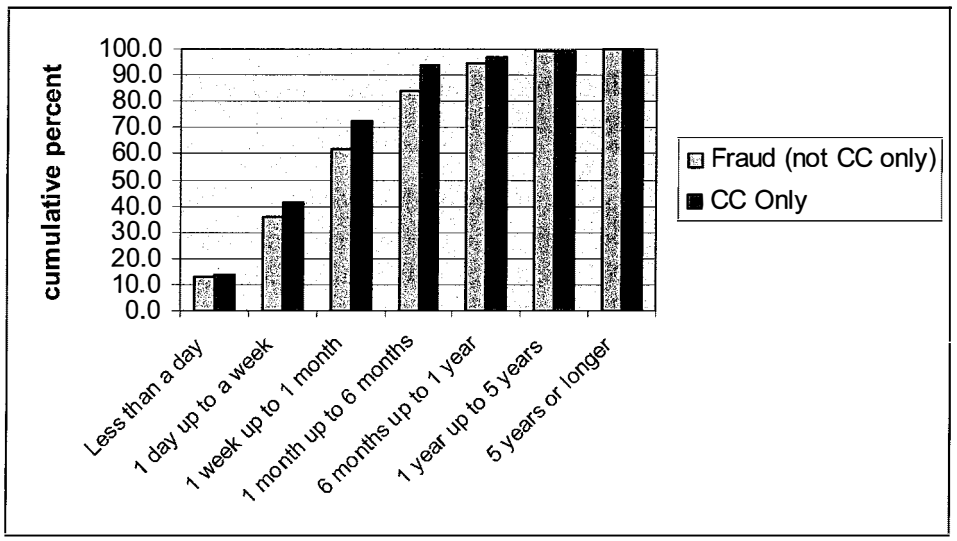


Figure 23 – Time to resolve

8.20 Descriptions

Question 25 – Is there any other information that would help to describe this episode of identity theft? (open-ended response)

A final victim question asked if there was any additional information about the case of IDT or IDF. A total of 631 respondents provided additional information.

Most of these comments describe simple credit card fraud or cheque frauds. Many of them also describe cases of friendly fraud, often with drug addition as a contributing factor. A selection of some of the more serious and saddest cases are as follows:

- It was my Mom that had all her money taken while she was dying in the hospital but since she has passed they said they could do nothing about it since she was unable to tell them her money was taken without permission.

- Mail stolen from mailbox. Credit cards, chequing account, and not sure what else. Had to declare bankruptcy. Lost house.

- It has made my relative's life a living hell. But we believe the perpetrator has been identified and is either being investigated or arrested.

- Someone impersonated my husband and claimed unemployment insurance under his name, received and cashed money from the government. The situation was difficult to resolve and my husband was repeatedly contacted to repay money he had never received.

- Husband is a crackhead

- Because it is the victim's daughter, the victim will not do anything about it

- Things have popped up 6 month or a year after from cell phone company, and other companies looking for my husband, insisting on talking to him…

- The victim continues to have unresolved issues. The perpetrator has never really been punished as these problems continue to manifest themselves. In reality, the victim continues to suffer, the perpetrator enjoys their freedom.

- … money was short for his addiction and stole his mother's identity for his own use This person is addicted to crack and heroine as well as alcohol and she knows that I know what she was doing. As she knows I would cause her problems with the law if she ever tried to use my name she has stopped.

- The thief was a drug addict who stole from his mother

- Son using mothers blank checks to get money for drugs

- Person used drivers license number as theirs when arrested for public intoxication, it cost me hours of my time and money to travel over three hours on numerous occasions because the government wouldn't help

- … Did not know that anyone was using my son's identification until he applied for a job in [*name of province*]. Needed to do a Criminal Record check for his new employment….

- It was when I received a bill for maternity services from local hospital for delivery of baby; & wasn't involved with anyone at the time. Was a single person.

- My younger brother took my wallet and obtained identity in my name and then returned the wallet without my knowing it was missing. He used it mainly to get a copy of my drivers license as ID when the police were looking for him.

- This person who did this to me was an in-law and someone I thought that I could trust, i was wrong and it has continued to cost me a lot of money and frustration, it also cost me my house, i will never trust fully anyone again

Many people took this opportunity to describe the impact, including emotional responses, on the victim. Selected examples are as follows:

- It was awful

- … it was a total violation of self.

- Very upsetting

- It is not an experience I wish on any one. You have to prove to all that the charges were not yours.

- It's very frustrating to not only be victimized, but to also have to cover the costs incurred by the perpetrator! That's like being victimized twice!

- It's hard trying to prove that it was someone else accessing information or funds other than the right person

- One of the most time consuming things that can happen to anyone.

- Basically a trust was broken and never regained, without justice being served…

- Very frustrating & helpless feeling

- …lost a lot of sleep & suffered a considerable amount of embarrassment when my employer was contacted

- It really [took] a lot of money and time to get rid of the problem
- It was very scary; I couldn't believe how it happened…
- It was not very easy to get it straightened out and it made me feel like a fraud
- The victim loses credibility with creditors and utility companies…
- A traumatic experience
- Very, very stressful and frustrating
- …. you feel embarrassed and violated
- It was a scary, demeaning experience. I was subject to a visit by police and study by hand writing experts to determine if I had in fact written the cheque that was used
- Only that it was done by a friend and I never trust anyone now. It took a long time for the victim to sort the problem and caused countless amount of stress

Other people described how their data was accessed:

- All mortgages are registered in this province. Unknown to us, that includes every single financial detail about the mortgage - rates, due date, amount and all personal info to obtain the mortgage….
- Paid to have mail forwarded, mail still went to old address, new person cashed cheques, ran up phone bill (after getting it re-installed in my name) ran up credit card, had new cheques printed on my bank account, used them. The post office said oops, sorry…
- A bank branch my brother used closed, and they threw all their paper records into an unlocked dumpster behind the bank. This is how all his information, plus that of probably countless others was stolen.
- My Employment Records with Revenue Canada were left in a cabinet that was sold at an auction. The new owner found mine and about 50 other employees' information

Many respondents offered advice to others, including:

- Changed the way I deal with money Only use money that I have transferred by phone to the account I use on a daily basis and only transfer money I need for that transaction
- Better knowledge in how banks operate, what protection there is for individuals during divorce. What laws are in place to protect consumers? Better educate women of their rights and responsibilities.

- When applying for the credit card ask about the safety precautions against identity theft
- Watch out for girls from Ghana and Nigeria on the Yahoo message network.
- I am more careful now when dealing with banks. I didn't know that someone with the same 'last name' could so easily walk into a branch in another province - get access to and clean out an account without anyone really checking who was standing in front of them.
- …Never have a pin number with a link to you (birth date, phone numbers). That was the only reason my money was returned…
- Don't put your SIN on applications. Give it directly to employer upon hiring.

Other pieces of advice (and the number of respondents who offered it) were:

- Never trust anybody and keep everything under lock and key (12)
- Be careful handing over credit/debit cards and hide your PIN (8)
- Don't keep identification documents in your car and always lock your car (4)
- Be very careful shopping online (4)
- Do a background check on roommates (2)
- Don't leave your purse unattended (2)

Some respondents offered suggestions for reducing either the incidence or impact of IDT and IDF:

- The banks should release more information to the victims.
- Why do banks send renewal credit cards in the mail? I believe as a customer YOU should go to the bank and get a new card.

Other common suggestions were:

- Enact tougher laws (5)
- Enact stricter authentication processes (5)

There were a surprising number of descriptions of debit card skimming, where both a card reader and a camera for recording the PIN are employed. Thirty-five respondents indicated that this had happened to them or someone in their family. This is almost 1% of the sample who volunteered this additional information. Twelve of these 35 descriptions indicated that the skimming had taken place at a gas station and four indicated that it had occurred at a bank. Debit card skimming generally receives prompt attention from both the banks and police, who then notify the victims. This may be why we received these comments, as this is one of only a few identity thefts where victims know exactly what has happened.

9. CONCERNS ABOUT IDENTITY THEFT AND IDENTITY FRAUD (QUESTIONNAIRE PART 4)

The next section of the survey asked questions about all respondents' concerns about IDT and IDF (N=3539).

Question 26 – How concerned are you about becoming a victim of identity theft in the future?

Response to this question was on a 5 point Likert scale. The overall response is shown in Figure 24, below.

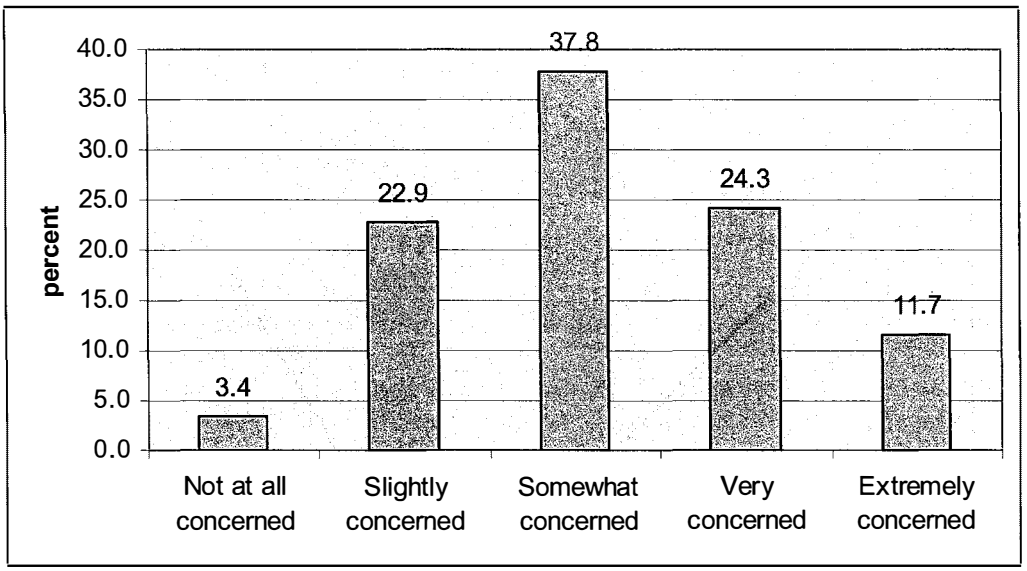


Figure 24 – Concerns about identity theft

Although the scales are not identical, these results are similar to those found in other surveys of Canadians (Ipsos-Reid 2005; Ipsos-Reid 2005; Ipsos-Reid 2005; Saravanamuttoo 2006). See Appendix C, Table C1 and Figure C1 for comparisons to these other surveys.

We looked at differences in concern between non-victims and victims according to the FTC categories. The means for each group are shown in Appendix C – Table C2 and in Figure 25, below.

From Figure 25, we can see that the lowest level of concern is found in the group who had experienced credit card fraud (themselves or through someone in their immediate family). This result probably stems from the fact that these problems were easily resolved and the consequences to the victims were not serious. The perceived risk for a similar occurrence is therefore lower, even than someone who has not had this experience. The level of concern is highest for those who had experienced new accounts or other frauds. As we have seen in previous sections, this group suffered the most serious consequences in terms of costs. Their level of concern for a re-occurrence is therefore higher than others.

In general, the differences between victims and non-victims may seem smaller than expected. An explanation for this may be that the victims or their families have learned from their experiences and changed their behaviours and therefore do not see themselves at as much risk for a reoccurrence.

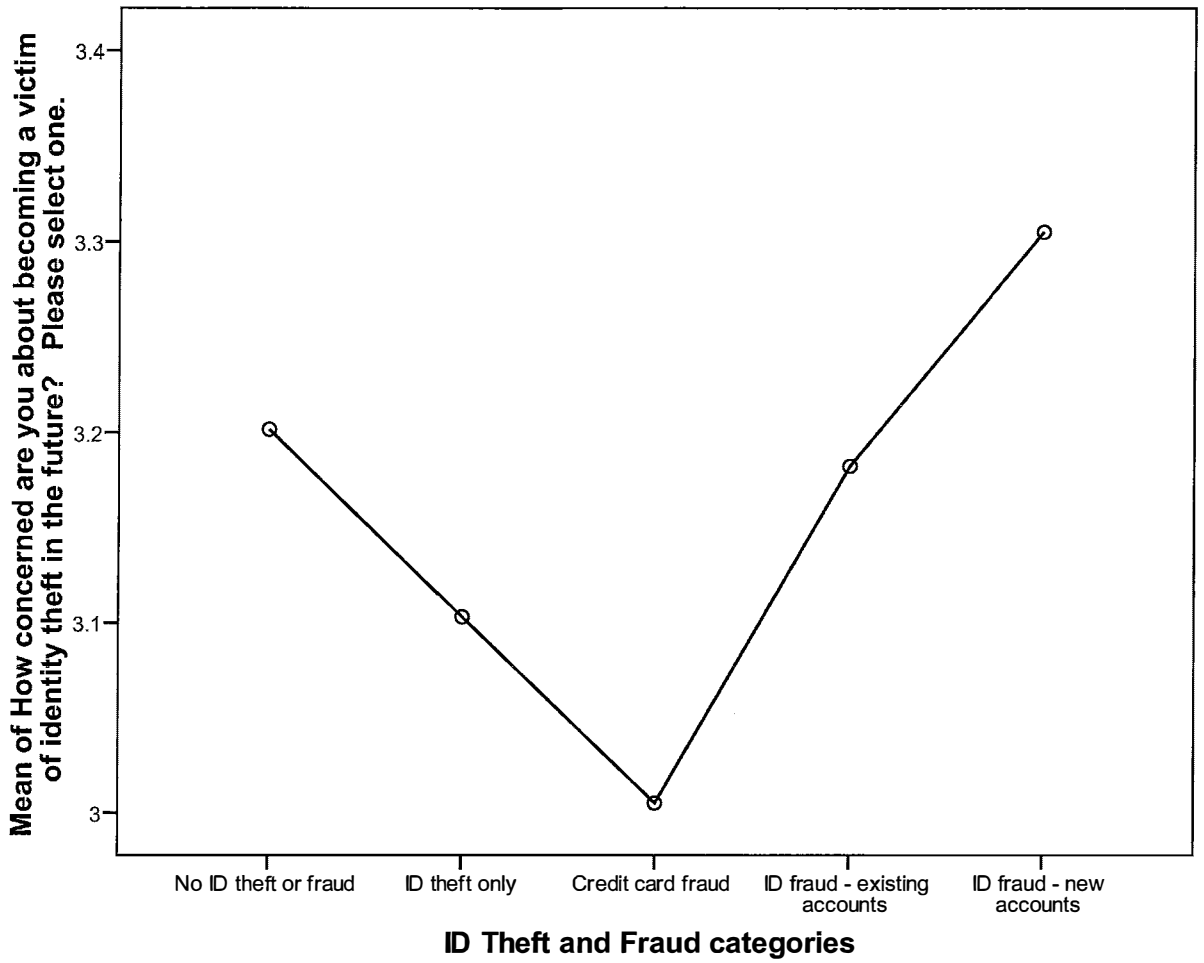


Figure 25 – Level of concern by FTC category

We next looked further at the differences in concern between the following groups:
1. Victims of IDF (self or family) and non-victims
2. Victims of IDF (self) and non-victims
3. Victims of IDF (self or family) excluding credit card fraud, and non-victims
4. Victims of IDT (self or family) and non-victims

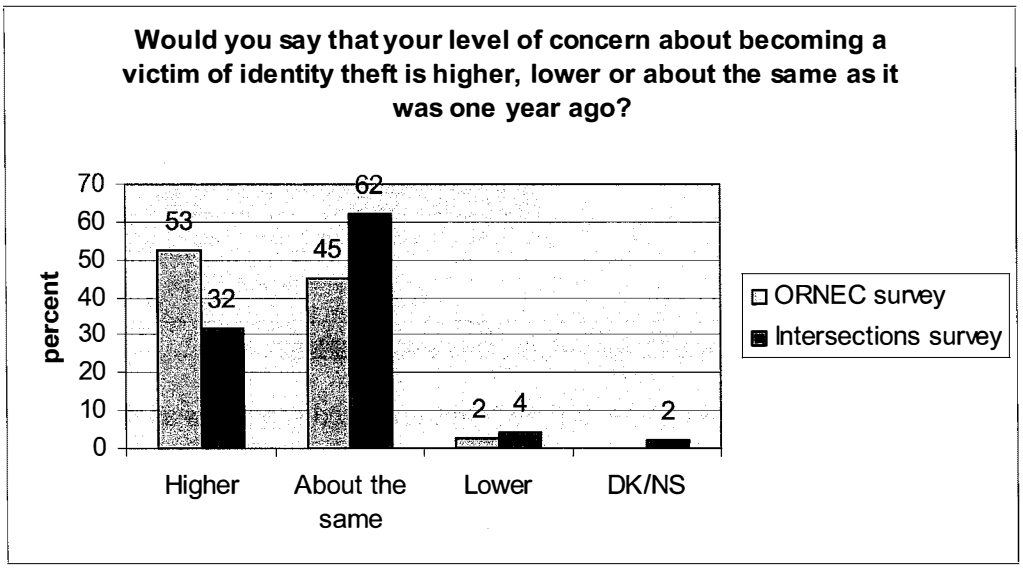
See Tables C4 through C11, in Appendix C.

When we include credit card fraud, there is no significant difference in the level of concern between victims and non-victims (1. and 2. above). When we exclude credit card fraud (3. above), there is a significant difference ($p < .01$). When we look at respondents who had experienced identity theft (4. above), we find that these respondents have a greater level of concern ($p < .05$) than those who had not.

Question 27 – 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 a year ago?

More than half of our respondents said that their level of concern was higher than it was a year ago. Only 2.5% indicated that it was lower. This is probably reflecting an increase in media attention to the problem of IDT and IDF, although it should be noted that the survey was conducted prior to two high profile instances of data breaches in Canada that were announced early in 2007 - TJX Inc. and CIBC's Talvest Mutual funds.

The response frequencies for this question and another Canadian survey can be found in Appendix C – Table C12. Our results and the results of this other survey (Ipsos-Reid 2005) are shown in Figure 25. The other survey, commissioned by Intersection, was conducted by Ipsos Reid, by phone, in January 2005. The higher level of concern reported in our survey, almost 2 years later, may be another indication that increased media attention is heightening consumer concerns.



Note: "Intersections" is a reference to the survey conducted by Ipsos-Reid (2005) titled Canadians and Identity Theft: Concern On The Rise (Ipsos-Reid 2005).

Figure 25 - Level of concern compared to last year

Question 30 – Please indicate the level of concern that you have about the following scenarios happening to you.

Question 30 was intended to allow us to evaluate whether the perceived risks assigned to various scenarios were in keeping with the actual incidence rates of various types of IDT and IDF. Figure 26 shows the scenarios ranked in order of the level of concern assigned by our respondents.

The stolen wallet scenario was ranked as the highest level of concern. In previous sections we saw that stolen wallets or purses accounted for 16% of cases where the method of obtaining the personal information was known or suspected, and 9% of all cases. This was the second most prevalent of known methods of obtaining information, after cases where the information was

taken from the home. (See Question 7.) It would seem appropriate that this scenario be ranked with one of the highest levels of concern.

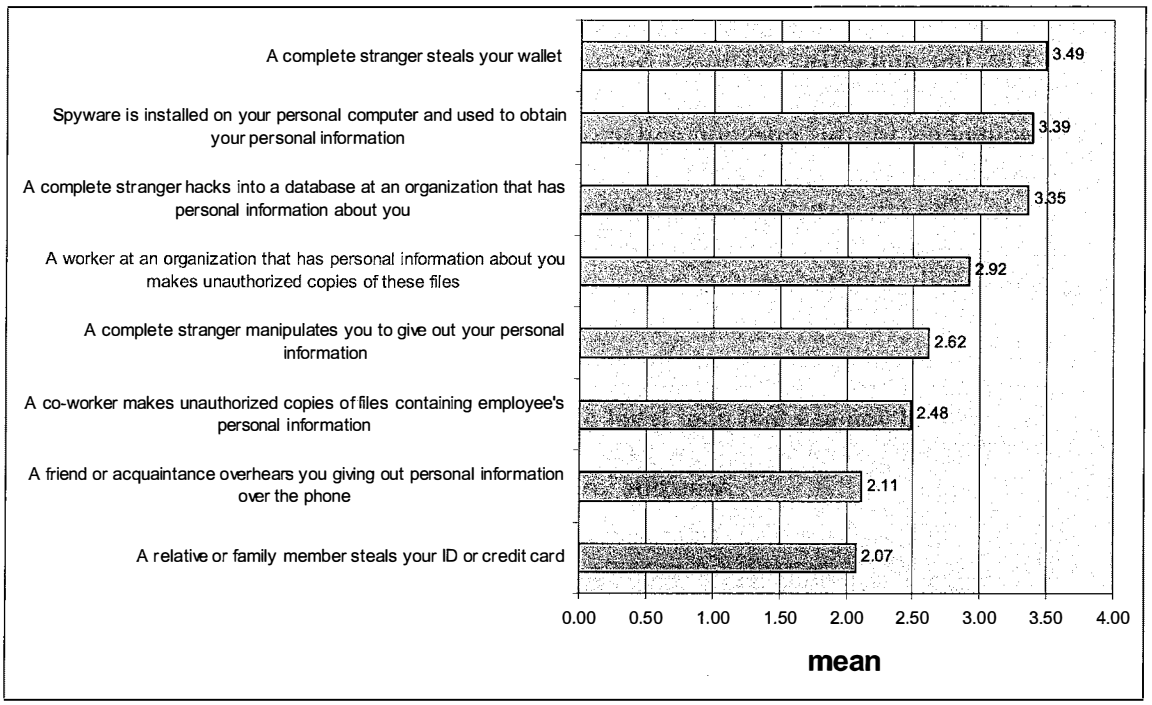


Figure 26 - Scenarios of concern (rank order)

Spyware and hacking were the second and third highest ranked scenarios as far as level of concern. This ranking is high compared to the known methods of obtaining information. In Question 7, spyware and hacking accounted for only 9 cases (specified as 'other') where the method was known or suspected. This is less than 1% of the cases where the method was known or suspected, and only 0.5% of all cases.

Insider access to personal information kept by an organization ranked fourth in level of concern. In Question 7, "taken from customer records or employee records of an organization" was the choice in only 3% of cases where the method of access was known or suspected and 2% of all cases. Canada has no current legislation requiring companies to notify consumers of data breaches. We might expect to see this scenario ranked higher in the US where such legislation is common.

The first through fourth ranked scenarios, described above, are all cases of stranger fraud, as defined in Section 8.10.1. As you may recall, stranger fraud accounted for only 25% of case where the identity of the perpetrator was known. Friendly fraud accounted for two thirds of these cases. The three friendly fraud scenarios in Question 30 obtained the lowest rankings (six through eight) as far as level of concern.

Surprisingly, people were moderately concerned about being subjected to social engineering or pretexting practices, where they would be tricked into disclosing personal information to an

identity thief. This was ranked fifth, lower than the scenarios of stranger fraud and higher than any of the scenarios of friendly fraud.

9.1 Phishing

We also included two questions that would let us estimate the prevalence of phishing.

Question 28 – Have you received emails from a bank or other company asking you to verify or update your account information?

Just under 40% of our respondents indicated that they had received potential phishing emails. (See Appendix C – Table C14 for the actual frequencies.) In 2005, an Ipsos Reid telephone survey (Ipsos-Reid 2005) asked if respondents had received 'phishing' emails. Only 24% of their respondents reported receiving such messages. The term 'phishing' was not defined or explained in the available script of the Ipsos-Reid survey. Anecdotal experience would also indicate that the prevalence of phishing increased dramatically in the time between these two surveys.

In Question 29, subjects who answered Yes to Question 28 were asked if they had responded to such emails.

Question 29 – Have you responded to any of these emails by providing account information?

Fortunately, just over 95% of respondents indicated that they had not responded to phishing emails. Unfortunately, 3.4% said that they had and 1.5% did not know whether or not they had responded. This is a worrisome proportion, as phishing continues to be a pervasive problem and phishing techniques continue to become even more sophisticated.

Other surveys have found similar results. In September 2006, APACS, the UK Payment Association, reported that 3.8% of online banking customers would respond to an unsolicited email, click on a link and provide security and account details[12]. Similarly, a report of the Bi-national Working Group concluded that 5% of recipients of phishing emails would hand over personal details (Binational Working Group 2006).

10. ATTITUDES TOWARDS PREVENTATIVE MEASURES (QUESTIONNAIRE PART 5)

The data in this section is summarized from a presentation given to the ORNEC research partners by Ken Deal, a member of our research group, on June 7, 2007. Further analysis of data from Part 5 will appear in future publications.

In Part 5 we presented 43 measures that individuals, financial institutions and governments might take to prevent IDT or to minimize the impact of IDF. The Max-Diff analysis ranks these potential measures according to the respondent's willingness-to-act. The four highest ranking measures, indicating the respondent's willingness to take these measures and shown in red in Figure 27, are:

[12] http://www.apacs.org.uk/media_centre/press/22.09.06.html (accessed April 18, 2007)

- Refuse to give personal information over the phone to people that claim to do surveys, or people offering products or services at special prices.
- Use anti-virus, anti-spyware and firewall software that is updated on a regular basis on your computer
- Shred financial or important documents before discarding them
- Monitor your account balances and activity online on a regular basis

Figure 27 shows the overall rankings. (The full-text list of measures can be found in the Questionnaire, page 70.)

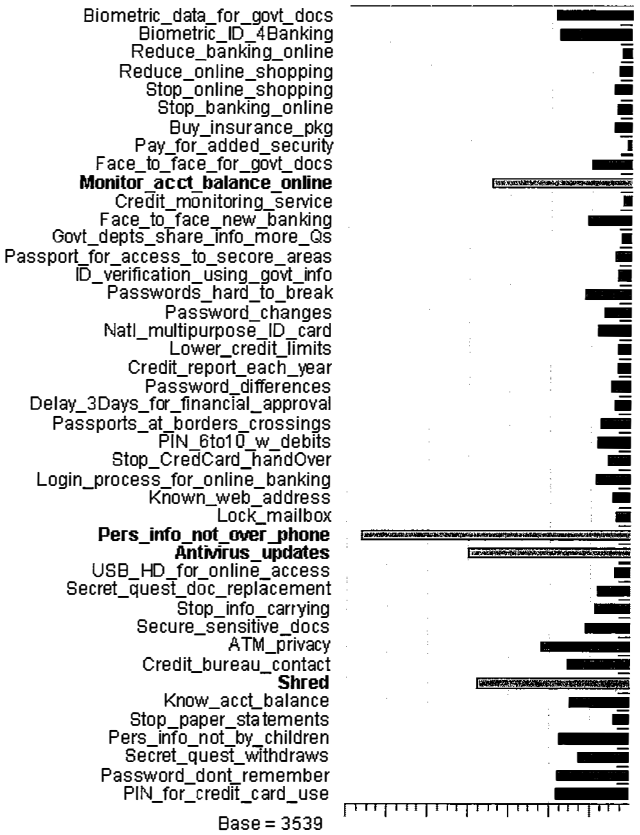


Figure 27 – Willingness-to-act rankings

Data from the Max-Diff analysis were also used to segment the respondents according to similarities in their preferences. The preliminary segmentation analysis identified 8 segments of approximately equal size, ranging from 9% to 15% of the sample. These segments and the measures that contributed to their differences are shown in Figure 28. A description of each segment and the defining characteristics of its members are as follows:

Segment 1 - Don't Give it Away

Members of Segment 1 prefer to protect themselves through increased attention to personal guardianship of information. They are most likely to instruct their children not to reveal personal information, to stop carrying extraneous pieces of identification, refuse to give personal information over the phone, shred documents and watch that no one is observing transactions at an ATM or other debit card machines. Fifteen percent of our respondents are in Segment 1.

Segment 2 – Electronic Vigilance
Members of Segment 2 are more likely to use electronic measures to protect themselves, ensuring that their anti-virus software is up-to-date, monitoring account balances online, and not choosing to let their computer 'remember passwords". Segment 2 also accounts for 15% of our sample.

Segment 3 – Personal Contact is Best
Members of Segment 3 are characterized by a preference for face-to-face or personal contacts when important information is exchanged or important transactions occur. They indicated a willingness to meet in-person with bank personnel for any new accounts and with government personnel for new or renewal documents. They support the use of passports at border crossing and proposals for multi-purpose government-issued identification documents. Segment 3 accounts for 14% of our sample.

Segment 4 – Passwords and PINs
Members of Segment 4 are vigilant about choosing strong passwords and PINs and protecting their passwords and PINS, and would be willing to support stronger methods of authentication based on passwords and PINs. Fourteen percent of our respondents are in Segment 4.

Segment 5 – Biometrics
Members of Segment 5 are characterized by their support for the use of biometrics as authentication factors. A willingness to accept the use of biometrics by governments and financial institutions were the two most discriminating measures of the 43 measures tested. Members of Segment 3 were also somewhat willing to accept biometric authentications. Segments 1, 2, 4, 6, and 8 ranked biometrics very low in their preferences. Segment 5 accounts for 13% of our sample.

Segment 6 – Secret Paper Documentation
Members of Segment 6 believe in the power of 'shared secrets' as an authentication factor. They are willing to share the answers to 'secret questions' with banks and governments as a way of implementing multi-factor authentication. They are also willing to let governments shared their personal information with other government departments or financial institutions as another measure of authentication. They are also wary of the security of paper documents, showing a willingness to stop receiving paper account statements and using locked mailboxes. Segment 6 accounts for 11% of our sample.

Segment 7 – Credit Protection
Members of Segment 7 are seem concerned with their credit rating. They are the most willing to purchase identity theft insurance, to check their credit report yearly, and to subscribe to a credit monitoring service. They would accept lower credit limits as a protective measure. Segment 7 accounts for 10% of our sample.

Segment 8 – Online Reduction
Members of Segment 8 are defined by their willingness to stop or reduce shopping and banking online as a way to reduce their risk of identity theft. They also indicated that they were most willing to stop handing over credit cards to waiters and gas station attendants. Nine percent of our respondents are in Segment 8.

The relative rankings of the measures that contributed to the segment identification, overall, are shown in Figure 28. The highest ranking, or most discriminatory, measures are associated with biometric authentication and the least discriminatory measure was the use of a PIN with a credit card.

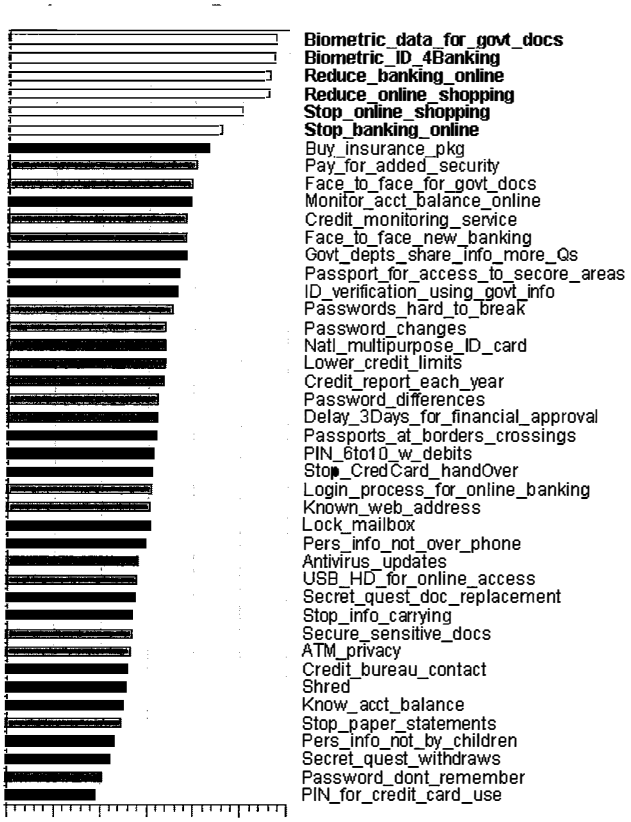


Figure 28 – Ranking of measures important to segment identification

Initial implications from this analysis are that different measures will have different degrees of acceptability within each of these segments, implying that cautions in introducing preventative measures will vary among the different population segments.

11. FUTURE ANALYSIS

We plan to conduct detailed analysis of the results of this survey in a number of different areas. Some of these include:

- A detailed examination of the effect of demographics on victimization. This would be along the lines of Anderson's analysis of the original 2003 FTC survey data (Anderson 2006) and

would provide a Canadian perspective on the problem.

- A detailed analysis of reporting behaviour, examining what types of fraud are most likely to be reported, the characteristics of the fraud that affect reporting behaviour and demographic influences on reporting.

- An examination of the characteristics of cases as we narrow the definition of identity fraud. This could include eliminating cases of credit card fraud only and eliminating cases of friendly fraud.

There are also two major studies that have just been released. One is a follow-up survey by the FTC (FTC 2006). The second is a study by the Economic Crime Institute of Utica College that examined Secret Service files of closed identity fraud cases (Gordon, Rebovich et al. 2007). The results of these studies will be compared to our results.

12. THE 2008 CONSUMER SURVEY

Plans are currently underway to complete a second survey so that we can start to collect longitudinal data on the problem of IDT and IDF in Canada. This could eventually lead to an annual publication of an index on this problem, making it possible to identity related trends, and whether legal, commercial, and governmental policy changes are required and/or have been effective in combating these problems.

By using the immediate family as the level of analysis, the original survey produced a large number of victim cases (1710). As a result, we have a lot of data that describes the long-term characteristics of IDT and IDF. As shown in this paper, we can use this data to compare the Canadian experience to that in the United States.

However, using the immediate family as the level of analysis introduced some problems in the analysis of this data, as we did not know if the cases being described had happened to the respondent or to someone in his or her family. This was particularly problematic in calculating incidence rates for a time frame such as 'in the last year' or 'in the last 5 years'.

For an IDT and IDF index, we need to be able to compare incidence rates on a year over year basis. The 2008 survey will therefore use self as the level of analysis. For our index, we also want to be able to see if the characteristics of IDT and IDF cases are changing. We therefore need to restrict the questions about the characteristics of cases to those that have happened in the last year.

This means that the focus of the 2008 survey will change from a broad look at the historical characteristics of IDT and IDF in Canada to a focus on the incidence and characteristics of cases in the past year. With another sample of 3000 to 4000, the expected number of victim cases will drop from 1710 to somewhere between 150 and 200.

Results from the original survey have also been used to fine-tune some of the questions for the next survey. We will eliminate infrequently used responses to questions and add some responses that were frequently found in the 'Other" category. We will also collect additional information

about the respondents, including income, Internet use, and number and the number and type of accounts held by the respondent.

The Max-Diff section of the survey that measured attitudes toward preventative measures will be replaced by a series of questions about behaviours that are believed to affect the risk of IDT and the ability of a victim to detect it.

QUESTIONNAIRE

1. In your opinion, which of the following scenarios describes a case of identity theft? (Check all that apply)

- You find out that someone who worked in your home used your personal information to get a replacement Health Card and obtain health care services under your name.
- You find out that a friend has received threatening emails that appear to come from you, but you did not send them.
- An underage person borrows another person's identification in order to obtain alcohol or cigarettes
- A family member takes your cheque-book and forges your name on a number of cheques.
- 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.
- While ordering a service, you give your credit card number to a company representative over the phone. You later learn that the company has fired one of their representatives for selling customers' names and credit card numbers to a fraud ring.
- You have an eBay account and a roommate uses your computer to list fraudulent items for auction under your name and account.
- You receive an email from your bank, asking you to respond and confirm your account information. You do this and then later find out that the email was not sent by the bank.
- Your insurance company advises you that they have lost a computer disk that had unencrypted customer information on it including names, addresses, birth dates, and drivers' license numbers.
- Your boss promotes an idea you had to improve how your group works, and takes credit for the result.
- You receive a notice from the Canada Revenue Agency that you owe income tax from a job that you never held.
- You give your credit card to the attendant at a gas station who swipes the card through an illicit machine that reads the information on the card's magnetic strip. The attendant then sells the information to criminals who manufacture counterfeit credit cards.
- Someone steals your wallet and uses your credit card to make purchases at a store

2. Assume that the following general scenarios describe different types of identity theft or fraud. Have any of them EVER happened to you or to anyone in your immediate family? (Check all that apply)

MATRIX COLUMNS

- This has happened to me
- This has happened to someone in my immediate family

- This has happened to both me and someone in my immediate family
- This has not happened to anyone in my immediate family, including myself

MATRIX ROWS

- Someone used a credit card and put charges on the account without the account holder's permission
- Someone gained access to an existing account other than a credit card account – for example, a bank account or a telephone or utility account – without the account holder's permission to run up charges or to take money from the account.
- Someone used personal information to impersonate you (or your family member) to obtain new credit cards or loans in your (or your family member's) name, run up debts, open other accounts, or otherwise commit theft or financial fraud.
- Someone used personal information to impersonate you (or your family member) to gain employment, receive benefits, avoid criminal prosecution or otherwise commit fraud or some other crime.
- Someone has accessed your (or your family member's) personal information without permission, although that information has not yet been used to commit frauds or other crimes.

If
All responses are "This has not happened to anyone in my immediate family, including myself"
Go to Question 26

If
The answer to more than one row is either:
"This has happened to me" or "This has happened to someone in my immediate family"
OR
The answer to any row is:
This has happened to both me and someone in my immediate family
,
Go to NOTICE 1

3. Was there more than one episode of this type of identity theft or fraud? (Check one)

- Yes
- No
- Don't know / Not sure

If
No,

Go to NOTICE 2.

NOTICE 1
You have indicated that there have been (or may have been) multiple episodes of identity theft experienced by you or someone in your immediate family. Please answer the following questions only with respect to the LATEST EPISODE of identity theft.

Go to Question 4

NOTICE 2
You have been a victim of identity theft. Please answer the following questions about this experience.

4. When was the identity theft discovered? (Check one)

- In the past 6 months
- Between 6 months and 1 year ago
- Between 1 and 2 years ago
- 2 to 5 years ago
- More than 5 years ago

5. How was the identity theft discovered? (Check all that apply)

- Belongings were stolen
- Notification of a data breach received from a company that had my information
- By requesting and reviewing a copy of a credit report
- An application for credit, a loan or a mortgage was turned down.
- Notification received from a bank or credit card company
- By monitoring bank and credit card accounts
- Notification by police
- Contacted by creditors or a collection agency about unpaid bills
- Other (please specify)

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

- Yes
- No
- Maybe

If
Yes

Go to question 8

If
No
Go to question 9

7. How do you suspect that the information was accessed or taken? (Check one)

- Lost wallet or purse
- Stolen wallet or purse
- 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 or over the phone
- It was taken during a business transaction conducted in person
- It was taken from the customer records or employee records of an organization
- It was taken from the home
- Other (please specify)

Go to Question 9

8. How was the information accessed or taken? (Check one)

- Mail was intercepted or redirected
- It was taken from the home
- It was taken from public records
- Stolen wallet or purse
- The information was provided in response to an email or telephone call from what appeared to be a legitimate source
- Lost wallet or purse
- It was taken from the customer records or employee records of an organization
- It was taken during a business transaction conducted in person
- It was taken during a business transaction conducted online or over the phone
- Other (please specify)

9. What was the interval between the time the information was stolen and the victim's 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

10. Do you know what information or documents were accessed or taken? (Check one)

- Yes
- No

If
No
Go to Question 12

11. What information was accessed or taken? (Check all that apply)

- Name
- Address
- Credit card information
- Bank account number(s)
- Social insurance number
- Birth date
- Driver's license number
- Mother's maiden name
- Password(s)
- Personal Identification Number(s)
- Other (please specify)

12. 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
- No

If
No
Go to Question 14

13. 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 the victim did business with
- A coworker
- Other (please specify)

14. Which of the following frauds were committed or attempted using the stolen identity? (Check all that apply)

- Purchase(s) made on an existing credit card account
- Charge(s) to an existing phone or utility account
- Money taken from an existing bank account
- Take over of existing credit card account(s) (For example, the account holder's billing address was changed or additional users were added to the account)
- Take over of existing phone or utility account(s) (For example, the account holder's billing address was changed)
- Take over of existing bank account(s) (For example, the account holder's address was changed or additional users were authorized on the account)
- New credit card account(s) opened in the victim's name
- New phone or utility account(s) opened in the victim's name
- New bank account(s) opened in the victim's name
- Home or apartment rented in the victim's name
- Loan(s) taken out in the victim's name (e.g. personal, student, auto)
- Mortgage(s) taken out on the victim's home
- The victim's home was sold
- Employment gained under the victim's name
- Tax fraud committed under the victim's name
- Government benefits obtained under the victim's name
- Crime(s) committed using the victim's name
- No frauds have been discovered to date
- Other (please specify)

15. To your knowledge, did the perpetrator use the information to obtain or counterfeit any additional identification documents in the victim's name? (Check one)

- Yes
- No

If
No
Go to Question 17

16. What identification documents did the perpetrator obtain or counterfeit? (Check all that apply)

- Passport

- Social insurance card
- Driver's license
- Health card
- Other (please specify)

17. How much money did the perpetrator obtain through the theft? (Include the value of merchandise, credit, 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

18. How many hours of the victim's own personal time have been spent resolving problems associated with this episode of identity theft? (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

19. How much of the victim's own money was spent to resolve problems associated with the identity theft? (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

20. What other (non-monetary) costs resulted from the identity theft? (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)

21. To whom was the identity theft reported? (Check all that apply)

- Credit card company(ies)
- Bank(s)
- Utility company(ies)
- 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)

22. Do you believe that misuse of the victim's identity has stopped? (Check one)

- Yes
- No
- Don't know / Not sure

If
No or Don't know / Not sure
Go to Question 25

23. Do you believe that all problems associated with this episode of identity theft have been resolved? (Check one)

- Yes
- No
- Don't know / Not sure

If
No or Don't know / Not sure

Go to Question 25

24. After the identity theft was first detected, how long was it before all of the associated problems were resolved? (Check one)

- Less than a day
- Less than a week
- Less than 1 month
- 1 month to 6 months
- 6 months to 1 year
- 1 year to 5 years
- More than 5 years

25. Is there any other information that would help to describe this episode of identity theft?

26. 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

27. 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
- Lower
- About the same
- Don't know / Not sure

28. Have you received emails from a bank or other company asking you to verify or update your account information? (Check one)

- Yes
- No

If
No
Go to Question 30

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

- Yes
- No
- Don't know / Not sure

30. Please indicate the level of concern that you have about the following scenarios happening to you.

MATRIX COLUMNS

- Extremely concerned
- Very concerned
- Somewhat concerned
- Slightly concerned
- Not at all concerned
- N/A

MATRIX ROWS

- A worker at an organization that has personal information about you makes unauthorized copies of these files
- A complete stranger manipulates you to give out your personal information
- A co-worker makes unauthorized copies of files containing employee's personal information
- Spyware is installed on your personal computer and used to obtain your personal information
- A complete stranger hacks into a database at an organization that has personal information about you
- A friend or acquaintance overhears you giving out personal information over the phone
- A complete stranger steals your wallet
- A relative or family member steals your ID or credit card

31. [Max Diff Question]

Please consider various measures that you might take to prevent the theft of your identity.

Considering only these 5 preventative measures, which one would you be Most Likely to Do and which one would you be Least Likely to Do?

LIST OF ITEMS:

- Use a locked mailbox for incoming mail

- Shred financial or important documents before discarding them
- Keep highly sensitive financial information in a secure location
- Make sure no one is watching when using an automated teller machine or debit machine at a checkout counter.
- Use anti-virus, anti-spyware and firewall software that is updated on a regular basis on your computer
- When banking or shopping online, do not select "remember my card number" or "remember my password"
- Have different passwords for different applications or services
- 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.)
- Refuse to give personal information over the phone to people that claim to do surveys, or people offering products or services at special prices.
- Educate children not to disclose personal information in Internet chat rooms or even to family friends without parents' approval.
- Never respond to a business by clicking on a link in an email.
- Know the approximate balance of your account to compare to the balance shown when withdrawing cash at an ABM
- Stop shopping online
- Reduce the amount of shopping that you do online
- Stop receiving paper statements from banks, utilities, and other sources
- Stop handing your credit card over to waiters or gas station attendants
- Stop carrying unnecessary information or documents in your purse or wallet
- Stop banking online
- Reduce the amount of banking that you do online
- Monitor your account balances and activity online on a regular basis
- Request a copy of your credit report at least once a year
- Check Land Registry Office records to ensure validity of home ownership
- Change your important passwords (i.e. for online banking, email accounts, etc.) on a regular basis
- Subscribe to a credit monitoring service that is promoted and offered through your bank
- Allow banks and other trusted parties to use information from government sources (such as license numbers, previous addresses, etc.) to verify your identity when applying for new accounts.
- Use a USB flash drive, provided by your bank, as well as a password, in order to get access to account information and conduct transactions online.
- Accept lower limits on amounts available through credit and debit card transactions.
- Provide biometric data such as fingerprints, voice samples, or retina scans that would be used by your bank to authenticate your identity when using a 'smart' debit or credit card or when banking online.
- Provide an answer to a secret question, whenever you need to identify yourself over the phone or online or when withdrawing large amounts from existing accounts.
- Accept a requirement for a face-to-face interview before new accounts are opened or new credit is extended (e.g. loans or mortgages).

- Require the credit bureaus to contact you before they release information for any new credit account applications
- Accept a three day delay for additional identity verification before approval of you application for a mortgages, a loan, or new credit or utility accounts.
- Pay additional service charges for enhanced security when banking online
- Use a 6 to 10 digit PIN with your debit card.
- Purchase an insurance package that would help restore financial and credit records and cover reasonable expenses if you become a victim of identity theft
- Accept a requirement to use a personal identification number (PIN) every time you use your credit card.
- Support a requirement for a face-to-face interview whenever it is necessary to renew or replace a government-issued document such as a passport, health card or drivers license
- Allow government departments to share information so that additional identification steps, such as responses to challenge questions, could be posed when you apply for a government-issued identification document such as a passport or driver's license
- Apply for and carry a new national multipurpose identity document that many organizations (both public and private) would accept to verify a person's identity
- Support a requirement to show a passport for access to secure areas in airports and other public places
- Answer a "secret question", whenever you need to replace or renew a government-issued document such as a driver's license or passport
- Support a requirement to show a passport to enter the country at a border crossing.
- Provide biometric data such as fingerprints, voice samples, or retina scans that would be used to verify your identity in association with government-issued identification documents such as passports, or driver's licenses
- Accept a change in the log-in process for online banking that would prove to you that the web site that you are connected to is actually your bank's web site.

36. Are you employed by any of the following types of companies or institutions? (Check one)

- A bank or other financial institution
- A law enforcement agency
- A criminal law firm
- A government office that deals with consumer affairs or privacy issues
- None of the above

The market research firm also added demographic questions as follows:

Marital status
Number and age of persons in the household
Level of education
Principle occupation

GLOSSARY

account-hijacking
"the assumption of a customer's identity on a valid existing account" (FDIC (Federal Deposit Insurance Corporation) 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 (Federal Deposit Insurance Corporation) 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." [13]
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"

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

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:

- 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."[14]
See also "credit freeze"

[14] 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 (Australasian Centre for Policing Research) 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 (Australasian Centre for Policing Research) 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." [15]
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."[16]
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"[17]
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."[18]
See also "pharming", "DNS poisoning"

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

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).

[19] 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."[20]

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 a genuine identification document blank into being" (Lyons 2007)

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

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

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 2007)

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

(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

Anderson, K. B. (2006). "Who are the Victims of Identity Theft? The Effect of Demographics." *Journal of Public Policy and Marketing* Vol. 25(2): pp. 160-171.

Baum, K. (2006). Identity Theft, 2004: First Estimates from the National Crime Victimization Survey. Bureau of Justice Statistics, U. S. Department of Justice. http://www.ojp.usdoj.gov/bjs/pub/pdf/it04.pdf

Berrens, R. P., A. K. Bohara, et al. (2003). "The Advent of Internet Surveys for Political Research: A Comparison of Telephone and Internet Samples." *Political Analysis* Vol. 11(1): pp. 1-22.

Best, S. J., B. Krueger, et al. (2001). "An Assessment of the Generalizability of Internet Surveys." *Social Science Computer Review* Vol. 19(2): pp. 131-145.

Binational Working Group (2006). Report on Phishing - A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, Bi-National Working Group on Cross-Border Mass-Marketing Fraud. http://www.usdoj.gov/opa/report_on_phishing.pdf

Braunsberger, K., H. Wybenga, et al. (2007). "A comparison of reliability between telephone and web-based surveys." *Journal of Business Research* Vol. 60: pp. 758-764.

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

Coderre, F., A. Mathieu, et al. (2004). "Comparison of the quality of qualitative data obtained through telephone, postal and email surveys." *International Journal of Market Research* Vol. 46(Q3): pp. 347-356.

Copes, H., K. R. Kerley, et al. (2001). "Reporting behaviour of fraud victims and black's theory of law: An empirical assessment." *Justice Quarterly* Vol. 18(2): pp. 343-363.

Couper, M. P. (2000). "Web Surveys: A Review of Issues and Approaches." *The Public Opinion Quarterly* Vol. 64(4): pp. 464-494.

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.

Dennis, J. M. (2001). "Are Internet Panels Creating Professional Respondents?" *Marketing research* Vol. Summer: pp. 34-38.

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

Finch, H. (2005). "Comparison of Distance Measures in Cluster Analysis with Dichotomous Data." *Journal of Data Science* Vol. 3: pp. 85-100.

Finch, H. and H. Huynh (2000). Comparison of Similarity Measures in Cluster Analysis with Binary Data. Annual Meeting of the American Educational Research Association, New Orleans.

Fricker, S., M. Galesic, et al. (2005). "An Experimental Comparison of Web and Telephone Surveys." *Public Opinion Quarterly* Vol. 69(3): pp. 370-392.

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

FTC (2003). Overview of the Identity Theft Program. Federal Trade Commission. www.consumer.gov/idtheft/pdf/ftc_overview_id_theft.pdf

FTC (2006). 2006 Identity Theft Survey Report, Federal Trade Commission and Synovate. http://ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf

GAO (General Accountability Office) (2007). Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, United States Government Accountability Office. GAO-07-737: 1-50. http://www.gao.gov/new.items/d07737.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

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

Hughes, K. (2004). Final Report of Cognitive Research on the New Identity Theft Questions for the 2004 National Crime Victimization Survey. Survey Methodology #2004-02. Study Series. Washington, DC, Statistical Research Division U.S. Bureau of the Census. http://www.census.gov/srd/papers/pdf/ssm2004-02.pdf

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

Ipsos-Reid (2005). Canadians And Identity Theft: Concern On The Rise, Ipsos-Reid. http://www.ipsos-na.com/news/ (by subscription only)

Ipsos-Reid (2005). Concern About Identity Theft Growing in Canada, Ipsos-Reid on behalf of Intersections Inc and Carlson Marketing Group Canada. http://www.ipsos-na.com/news/ (by subscription only)

Ipsos-Reid (2005). Concern Over Identity Theft on the Rise, Ipsos-Reid on behalf of Capital One Canada. http://www.ipsos-na.com/news/ (by subscription only)

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 (2007). Living the low life on your identity: From groceries to toilet paper, criminals now rely on ID theft for basic needs. 2007. http://www.javelinstrategy.com/2007/02/12/living-the-low-life-on-your-identity-from-groceries-to-toilet-paper-criminals-now-rely-on-id-theft-for-basic-needs/

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

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

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

Lyons, J. (2007). Personal correspondence with. S. Sproule: 28 year career with the RCMP. Principal of "AlterNation".

Ollman, G. (2007). "IDs sell for much more than credit card numbers in underground." *Computer Fraud and Security* Vol. December: pp. 2.

Poynter, R. The power of conjoint analysis and choice modeling in online surveys, Virtual Surveys. 2007. http://www.virtualsurveys.com/news/papers/paper_23.doc

Privacy and American Business (2003). Privacy and American Business Survey Finds 33.4 Million Americans Victims of ID Theft; Consumer Out-Of-Pocket Expenses Total $1.5 Billion a Year. Hackensack, NJ, Privacy and American Business and Harris Interactive. http://www.pandab.org/id_theftpr.html

Roster, C. A., R. D. Rogers, et al. (2004). "A comparison of response characteristics from web and telephone surveys." *International Journal of Market Research* Vol. 46(3): pp.

Saravanamuttoo, M. (2006). Identity Theft & Identity Management: Looking through the eyes of the Canadian public. 7th Annual Privacy and Security Workshop, Toronto, ON, Eckos Research Associates.

Smith, T. W. (2001). Are Representative Internet Surveys Possible? Statistics Canada Symposium - Achieving Data Quality in a Statistical Agency: A Methodological Perspective. http://www.statcan.ca/english/freepub/11-522-XIE/2001001/session18/s18d.pdf

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

Zuriek, E. and L. L. Harling-Stalker (2006). Globalization of Personal Data (GDP) International Survey Research Workshop. Kingston, The Surveillance Project, Queen's University.

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