



Canadian Internet Policy and Public Interest Clinic
Clinique d'intérêt public et de politique d'internet du Canada

TECHNIQUES OF IDENTITY THEFT

March, 2007

CIPPIC Working Paper No. 2 (ID Theft Series)

www.cippic.ca

CIPPIC Identity Theft Working Paper Series

This series of working papers, researched in 2006, is designed to provide relevant and useful information to public and private sector organizations struggling with the growing problem of identity theft and fraud. It is funded by a grant from the Ontario Research Network on Electronic Commerce (ORNEC), a consortium of private sector organizations, government agencies, and academic institutions. These working papers are part of a broader ORNEC research project on identity theft, involving researchers from multiple disciplines and four post-secondary institutions. For more information on the ORNEC project, see www.ornec.ca.

Senior Researcher: Wendy Parkes
Research Assistant: Thomas Legault
Project Director: Philippa Lawson

Suggested Citation:

CIPPIC (2007), "Techniques of Identity Theft", CIPPIC Working Paper No.2 (ID Theft Series), March 2007, Ottawa: Canadian Internet Policy and Public Interest Clinic.

Working Paper Series:

No.1: Identity Theft: Introduction and Background
No.2: Techniques of Identity Theft
No.3: Legislative Approaches to Identity Theft
No.3A: Canadian Legislation Relevant to Identity Theft: Annotated Review
No.3B: United States Legislation Relevant to Identity Theft: Annotated Review
No.3C: Australian, French, and U.K. Legislation Relevant to Identity Theft: Annotated Review
No.4: Caselaw on Identity Theft
No.5: Enforcement of Identity Theft Laws
No.6: Policy Approaches to Identity Theft
No.7: Identity Theft: Bibliography

CIPPIC

The Canadian Internet Policy and Public Interest Clinic (CIPPIC) was established at the Faculty of Law, University of Ottawa, in 2003. CIPPIC's mission is to fill voids in law and public policy formation on issues arising from the use of new technologies. The clinic provides undergraduate and graduate law students with a hands-on educational experience in public interest research and advocacy, while fulfilling its mission of contributing effectively to the development of law and policy on emerging issues.

Canadian Internet Policy and Public Interest Clinic (CIPPIC)
University of Ottawa, Faculty of Law
57 Louis Pasteur, Ottawa, ON K1N 6N5
tel: 613-562-5800 x2553
fax: 613-562-5417
www.cippic.ca

EXECUTIVE SUMMARY

This paper presents an inventory of the main techniques used by identity thieves. It begins with a review of the types of personal information collected by identity thieves. The paper then describes 23 different techniques employed by identity thieves to acquire personal information.

These techniques are listed under three headings: 1) physical theft; 2) technology-based theft; and, 3) social engineering. Examples of how stolen personal information can be used to commit identity fraud are also identified and the ability of victims in Canada and the U.S. to detect identity theft is briefly reviewed. Appendices A and B contain examples of pharming and phishing techniques, while Appendix C contains a glossary of terms.

This review shows that identity thieves use a wide variety of techniques, ranging from straightforward theft of personal belongings to highly sophisticated computer-based theft. Most thefts are of an off-line nature, with lost or stolen wallets, chequebooks or credit cards a major source of the personal information sought and used by identity thieves. However, use of the internet is becoming more frequent and presents special challenges.

Identity theft techniques are constantly being refined and expanded. This makes it harder to prevent and detect identity theft and for law enforcement agencies to apprehend thieves.

The inventory provides a foundation for further papers in this series, examining legislative, judicial, and policy approaches to the problem and the challenges facing law enforcement agencies.

NOTE RE TERMINOLOGY

The term “identity theft”, as used in this Working Paper series, refers broadly to the combination of unauthorized collection and fraudulent use of someone else’s personal information. It thus encompasses a number of activities, including collection of personal information (which may or may not be undertaken in an illegal manner), creation of false identity documents, and fraudulent use of the personal information. Many commentators have pointed out that the term “identity theft” is commonly used to mean “identity fraud”, and that the concepts of “theft” and “fraud” should be separated. While we have attempted to separate these concepts, we use the term “identity theft” in the broader sense described above. The issue of terminology is discussed further in this first paper of the ID Theft Working Paper series.

TABLE OF CONTENTS

	Page
1. INTRODUCTION.....	1
2. WHAT TYPES OF PERSONAL INFORMATION DO THIEVES STEAL?.....	1
3. HOW DO THIEVES ACQUIRE PERSONAL INFORMATION?.....	3
3.1. TECHNIQUES INVOLVING PHYSICAL THEFT.....	5
3.1.1. <i>Theft of Wallets, Purses, Cell Phones, Computers and other Sources of Personal Information</i>	5
3.1.2. <i>Dumpster Diving</i>	5
3.1.3. <i>Change of address</i>	6
3.1.4. <i>Mail Theft</i>	6
3.1.5. <i>Reshipping</i>	7
3.1.6. <i>Government Records</i>	8
3.1.7. <i>Tombstone Theft</i>	9
3.1.8. <i>Skimming (magnetic strip duplication)</i>	9
3.1.9. <i>Insider Theft</i>	11
3.1.10. <i>Purchasing stolen personal information</i>	13
3.1.11. <i>Identity Consolidation – “Breeding”</i>	13
3.2. TECHNOLOGY-BASED IDENTITY THEFT TECHNIQUES.....	13
3.2.1. <i>Phishing</i>	13
3.2.2. <i>Pharming</i>	15
3.2.3. <i>DNS Cache poisoning</i>	15
3.2.4. <i>Spyware, Malware and viruses</i>	16
3.2.5. <i>Internet Searches and Google Hacking</i>	17
3.2.6. <i>Exploiting computer systems’ security vulnerabilities (cracking)</i>	17
3.2.7. <i>Wardriving (Drive-by Identity Theft)</i>	18
3.2.8. <i>Acquiring used computer equipment</i>	19
3.3. SOCIAL ENGINEERING TECHNIQUES.....	20
3.3.1. <i>Pre-texting</i>	20
3.3.2. <i>Obtaining credit reports</i>	21
3.3.3. <i>Bogus Employment Schemes</i>	21
3.3.4. <i>Contests and Surveys</i>	22
4. HOW DO THIEVES USE STOLEN PERSONAL INFORMATION?.....	22
4.1. SELLING PERSONAL INFORMATION.....	24
4.2. FORGING IDENTITY DOCUMENTS.....	24
4.3. TAKING OVER EXISTING ACCOUNTS.....	24
4.4. OPENING NEW ACCOUNTS.....	25
4.5. ORDERING GOODS ONLINE USING A DROP-SITE.....	25
4.6. SECURING EMPLOYMENT.....	25
4.7. OBTAINING A PASSPORT.....	26
4.8. OBTAINING GOVERNMENT BENEFITS.....	26
4.9. OBTAINING HEALTH SERVICES.....	26
4.10. HIJACKING EMAIL ACCOUNTS.....	27
4.11. MAKING LONG DISTANCE CALLS.....	27
4.12. CONCEALING ONE’S TRUE IDENTITY.....	27
4.13. MORTGAGE FRAUD.....	28
4.14. TAKING OVER INSURANCE POLICIES.....	29
4.15. SUBMITTING FRAUDULENT TAX RETURNS.....	29
4.16. FILING FOR BANKRUPTCY.....	29
4.17. SELLING STOLEN GOODS.....	30

5. DETECTING IDENTITY THEFT	30
5.1. CANADA.....	30
5.2. UNITED-STATES	31
6. CONCLUSION	31
APPENDIX A – EXAMPLES OF PHISHING EMAILS	33
APPENDIX B - PHARMING.....	36
APPENDIX C– GLOSSARY OF TERMS.....	37

1. INTRODUCTION

In order to prevent, detect and deal with the aftermath of identity theft, it helps to have an understanding of how it happens in the first place. Many of the techniques used are relatively straightforward, such as simple theft of wallets, mail and credit cards. Other techniques are quite complex, sophisticated and technology-based. Thieves are constantly developing new and improved ways to acquire personal information to use in a fraudulent manner or to create false identities for the same purpose.

This paper focuses on the techniques used by identity thieves. First, the types of personal information sought by identity thieves are listed. This is followed by an inventory of the actual techniques employed by identity thieves to acquire this personal information. Examples of how stolen personal information can be used to commit identity fraud are identified. The ability of victims in Canada and the U.S. to detect identity theft is briefly reviewed. Appendices A and B contains examples of phishing and pharming techniques. Appendix C contains a glossary of terms.

2. WHAT TYPES OF PERSONAL INFORMATION DO THIEVES STEAL?

Acquiring the personal information of another person is the key to success for identity thieves. There is no standard definition for “personal information”.¹ However, the information needed will usually be more than an address or telephone number. In Canada, the Office of the Information and Privacy Commissioner of British Columbia refers to it as “information forming the biographical core of an individual”.² Date of birth, social insurance number, driver’s licence number, vehicle registration certificate, bank account or credit card number and other unique identifiers are examples of personal information.

Craats has identified twelve types of personal information most sought after by identity thieves:

- (i) Credit card numbers
- (ii) CW2 numbers (found on the back of credit cards)
- (iii) Credit reports
- (iv) Social Security (SIN) numbers
- (v) Driver’s licence numbers
- (vi) ATM numbers
- (vii) Telephone calling cards
- (viii) Mortgage details
- (ix) Date of birth
- (x) Passwords and PINs

¹ Personal information is sometimes referred to as “personally identifiable information”.

² Office of the Information and Privacy Commissioner for British Columbia, Investigation Report F06-01 (31 March 2006) at 13, online: Office of the Information & Privacy Commissioner http://www.oipcbc.org/orders/investigation_reports/InvestigationReportF06-01.pdf.

- (xi) Home address
- (xii) Phone numbers³

According to research conducted at Carnegie-Mellon University, nearly 90% of the U.S. population could be uniquely identified through the use of only three pieces of information: a person's date-of-birth, sex, and postal code.⁴ Clearly, not much personal information needs to be acquired in order for identity thieves to succeed.

The following table provides examples of personally identifiable information identity thieves often try to acquire.

Table 1 – Types of Personal Information Collected by Thieves

Personal information

Name	Gender	Age
Date of birth	Place of birth	Birth certificate
Mother's maiden name	Marital status	Ethnic origin
Address (current and former)	Telephone numbers	Email address
Social insurance number (SIN)	Driver's licence number	Health card number
Passport number	Permanent resident (PR) card	Account credentials (username, password, PIN, etc)
Employment history	Family information	Educational history
Medical history	Number of dependents	Information on your spouse

Property information

Property Addresses	Vehicle plate number	
Vehicle registration number	Information on assets	

Financial information

Credit card numbers	Calling card numbers and personal identification numbers (PIN)	Liabilities
---------------------	--	-------------

³ Rennay Craats, *Identity Theft: the scary new crime that targets all of us* (Altitude Publishing: Toronto, 2005) at 179.

⁴ Information and Privacy Commissioner of Ontario, *Identity Theft Revisited: Security is Not Enough* (September, 2005) at 3, online: IPC - Office of the Information and Privacy Commissioner/Ontario <http://www.ipc.on.ca/index.asp?navid=46&fid1=233&fid2=4>.

Debit card numbers and personal identification numbers (PIN)	Tax payer identification number	Actual or estimated income
Bank account numbers	Mortgage details	Investments information
Outstanding debt		

Biometric information

Fingerprints	Voice print	Retina image
Height	Weight	Eye and hair color

3. HOW DO THIEVES ACQUIRE PERSONAL INFORMATION?

Acquiring personal information is the first step of an identity theft crime. The goal is to obtain sufficient information about the victim to be able to conduct transactions in the victim's name.

Much of this information is readily available, even to the most unsophisticated of thieves. As noted by a fraud investigator for a New York accounting firm:

As long as we live in a free country with ready access to information, and information is important, - and we're not going to control that - criminals out there will find a way to obtain that information and commit identity theft.⁵

Personal information can be collected from a variety of sources and by a variety of methods, some relatively simple and low tech (such as: reading obituaries; stealing mail from homes, businesses and mailboxes; breaking into offices or vehicles to steal files; stealing luggage and briefcases; and rummaging through home and businesses' garbage) and others more sophisticated (such as: stealing or hacking into computers; impersonating clients when calling insurers, credit card companies; using the services of online information brokers; and duplicating magnetic strips on the back of cards). These methods can be exercised either in person or virtually through the internet, phone lines or cell phones.

The methods employed keep expanding. As law enforcement agencies get better at detecting favoured techniques, thieves turn to new methods. The electronic environment and constantly evolving technologies provide them with ever-expanding and new windows of opportunity.

Personal information is not only acquired directly by the thief, but may also be purchased from a third party, such as the operator of a phishing site or an employee who has stolen information. Online "carder networks" have emerged, through which identity thieves illegally buy and sell stolen personal information. Also, a small amount of personal

⁵ *Craats, supra* note 3 at 182.

information may be used to acquire yet additional personal information, and copies of identity documents. This process, known as “identity breeding”, is described below.

Figure 3.1 illustrates the frequency and distribution of different personal information acquisition techniques in the United States, based on a survey conducted in 2006.⁶ Identity theft is often regarded as a high-tech crime. Yet, it is telling that acquisition of personal information via the internet accounted for less than 10% of cases reported by respondents to this survey. According to these reports, identity thieves continue to rely largely on low-tech methods to acquire personal information of victims.

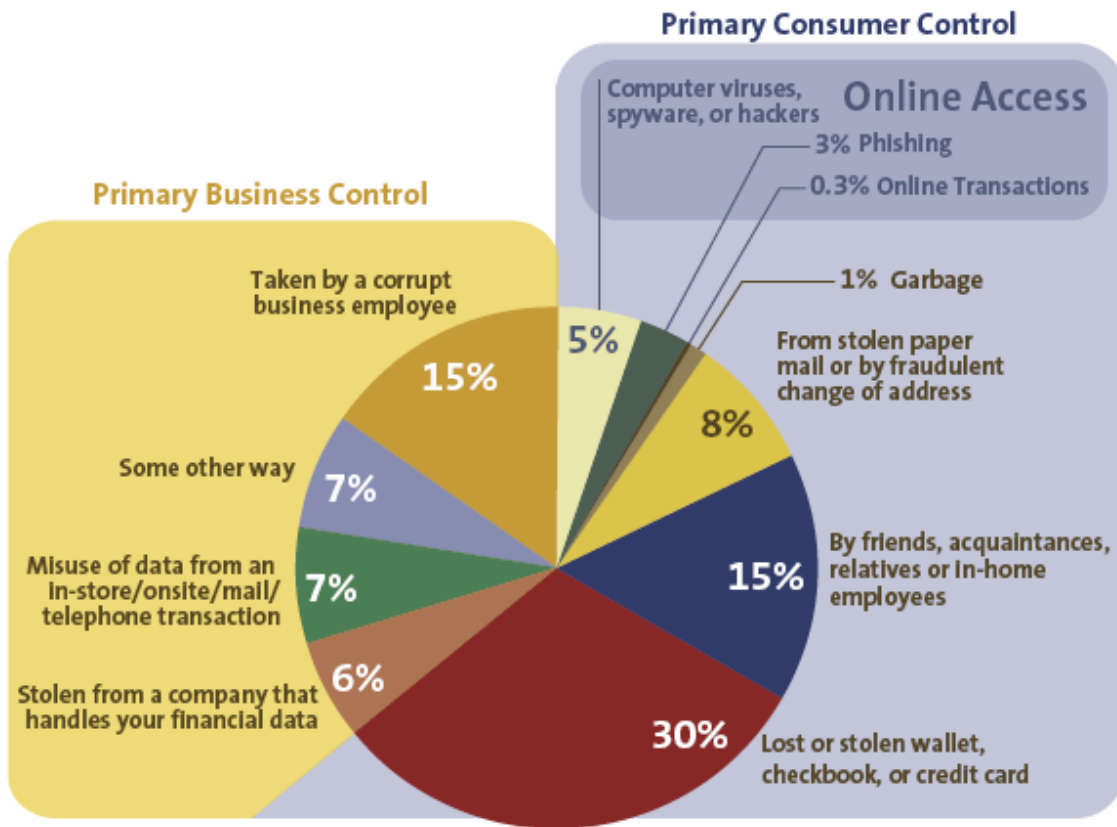


Figure 3.1 - Victims who knew how their information was obtained

The remainder of this section reviews discusses the best known techniques used by thieves to steal or acquire personal information.

⁶ Javelin Strategy and Research, 2006 Identity Fraud Survey Report Brochure (January 2006), online Javelin Strategy and Research <<http://www.javelinstrategy.com/uploads/2006IDFBrochure.pdf>>. 5000 American adults, including 505 victims, representative of the U.S. census demographics distribution were interviewed for this survey.

3.1. Techniques involving Physical Theft

3.1.1. Theft of Wallets, Purses, Cell Phones, Computers and other Sources of Personal Information

Wallets and purses and cell phones can be stolen, or they can be lost or forgotten and then discovered by an unscrupulous person. Computers, especially laptops, and other storage media containing personal information, such as disks or tapes, may also be lost or stolen. Credit cards, debit and calling cards, cheques, drivers licences, account information, Social Insurance Numbers (SINs) – all these and other pieces of key personal information can be in the hands of thieves literally in one swipe. Card receipts can be forgotten at restaurants, at a cashier counter, or at an ATM machine, where they may be picked up by thieves.

Portable computers containing databases of personal information are a particularly rich target for thieves. On Friday, September 26, 2003, two well dressed men walked into the Calgary offices of the Canada Customs and Revenue Agency (CCRA) and stole 15 DELL laptop computers valued in excess of \$60,000.00.⁷ Four computers containing confidential personal information on more than 120,000 Canadians were also stolen from CCRA's Laval offices on September 4, 2003.⁸ The personal information of thousands of Canadians became at risk for identity theft and fraud as a result. At the time of publication, there was no indication that identity theft had occurred as a result of this security breach.

In May 2005, the U.S. Department of Justice reported that a laptop containing information on 80,000 departmental employees was stolen.⁹ A similar situation occurred at the University of California, Berkeley. This time, personal information, including social security numbers (SSN), was stored, unencrypted, on the laptop.¹⁰

3.1.2. Dumpster Diving

Identity thieves may sort through household garbage, searching for pieces of paper containing financial and other personal information. Certain businesses are especially vulnerable to dumpster diving. These include hotels, rental car companies and others that swipe credit cards for reservations and then discard, rather than destroy the copies, once the customer has paid.¹¹ These paper copies then make their way into often readily accessible garbage disposal units, where they may be found by an identity thief.

⁷ City of Calgary, Follow-up to shop breaking at the Canada Customs and Revenue Agency offices (6 October 2003), online: The City of Calgary

<http://www.gov.calgary.ab.ca/citybeat/public/2003/10/release.20031006_193103_7097_0>.

⁸ Robert Fife, "Theft threatens privacy of 120,000" *Canada.com News* (30 September 2003), online: PSSG - Information Risk Management, Privacy + Cyberliability Specialists

<<http://www.projectscope.com/images/RevCanTaxtheft.pdf>>.

⁹ *Identity Theft Revisited*, *supra* note 4 at 6.

¹⁰ *Ibid.* at 7.

¹¹ *Craats*, *supra* note 3 at 39.

3.1.3. Change of address

Thieves redirect mail for two main reasons: 1) Mail is an abundant source of personal information; and 2) Redirecting mail gives a thief more time to engage in fraudulent transactions before the victim detects any suspicious activity.

Thieves can arrange to have a victim's mail redirected, either on a specific account of the victim through the institution that provides that account, or for all of a victim's mail, by using Canada Post's Change of Address Service (Redirection).¹² Very little information about the victim is needed in order to have Canada Post redirect his or her mail. Canada Post requires the following information to complete this process online:

- Old/New address
- Move Date
- Contact information (phone number, email address)
- Credit Card number and expiration
- Required to assist in authentication:
 - o Date of birth
 - o Social Insurance Number (optional)
 - o Driver's License number and Province of issue (optional)
 - o Knowledge of your personal credit history¹³

A man and a woman were arrested for committing this fraud in Ottawa in March 2006.¹⁴ The mail of several victims was redirected using a change of address form. The victims had provided all the necessary personal information to the thieves by replying to an online job offer. According to the article, the police were provided information on the fraud by Canada Post corporate security.

In the United States when a change of address is hand-written, verification notices must be sent to both the current and forwarding addresses. In another example of the use of this technique, the notice sent by the U.S. postal service arrived one week after some of the victim's mail had been forwarded; however, by then the damage was done.¹⁵

3.1.4. Mail Theft

Mail theft is an especially easy way to steal personal information. Mail can be stolen from home and business mailboxes and from garbage and recycling bins. Mail provides

¹² Canada Post, Change of Address Service (Redirection), online: <http://www.canadapost.ca/tools/pg/manual/e01-e.asp>.

¹³ Manage My Mail, online: Canada Post <<https://ssl.postescanada-canadapost.ca/tools/mmm/ssl/bin/GettingStarted.asp?lang=en>>.

¹⁴ Globe and Mail, "Canada Post tip leads to arrests in identity scam" (9 March 2006), online: [globeandmail.com](http://www.theglobeandmail.com/servlet/story/RTGAM.20060309.gtpost09/BNSStory/Technology/home) <<http://www.theglobeandmail.com/servlet/story/RTGAM.20060309.gtpost09/BNSStory/Technology/home>>.

¹⁵ abc7news.com, "'Change Of Address' System Causing ID Theft?" (15 March 2006), online: [abc7news.com](http://abclocal.go.com/kgo/story?section=7on_your_side&id=3996599) <http://abclocal.go.com/kgo/story?section=7on_your_side&id=3996599>.

an excellent source of personal information – such as bank and credit card statements, driver’s licence renewals, pre-approved credit card applications, discarded utility bills and so forth. These may provide key details, such as the name of the victim’s bank, account number, signature (from cancelled cheques, driver’s licence), driver’s licence number and credit card numbers and limits. In CALPIRG’s survey of U.S. law enforcement officials, 68% of officers surveyed cited mail theft as a top concern related to identity theft.¹⁶

The proliferation of unsolicited pre-approved credit card applications with personal information already typed onto them has made discarded mail an especially good target in the United States. Thieves complete these applications, substituting a new address; the credit cards thus obtained can then be used to rack up charges in the name of the victim. In Canada, unsolicited credit card applications do not contain sufficient personal information for a thief to obtain a card in someone else’s name.

The use of mail theft to further identity theft crimes is well documented in Canada. In 2004, a thief was sentenced to four and half years for fraud. Bradley stole credit cards from the postal service and produced other forged documents to further his fraud.¹⁷ Another convicted thief forged postal service mail keys in order to gain access to personal information which he then used to obtain credit cards. McNeil was not charged with mail theft but for possession of a homemade mail key.¹⁸

3.1.5. Reshipping

This scam involves a company engaging the victim in what appears to be a legitimate business, that of repackaging small electronic items such as cameras or laptop computers and reshipping them abroad.¹⁹ Wire transfers for auction goods may also be provided, with a request to forward funds to another account. The proposition is presented as an easy way to make money. The scheme is a mixture of theft of personal information, credit card fraud and auction fraud. It is often set up over the internet, on chat rooms, or on bulletin boards for job postings.

The “employee” is asked to complete payroll application forms, which request personal information such as address, name and SIN number. Bank accounts are then opened and loans taken out in the individual’s name, with or without his or her knowledge?

Eventually cheques are returned and the “employee” is held responsible for them as well as for shipping costs. The goods involved are invariably stolen, often by purchasers using stolen credit cards obtained through phishing sites or “carder networks”. Thus, the

¹⁶ Jennette Gayer, Policing Privacy: Law Enforcement’s Response to Identity Theft (CALPIRG Education Fund, May 2003) at 10, online: CALPIRG <http://www.calpirg.org/reports/policingprivacy2003.pdf>.

¹⁷ *R. v. Bradley*, [2004] A.J. No. 1278 (Alta. C.A.) (Q.L.), 2004 ABCA 362.

¹⁸ *R. v. McNeil*, [2006] B.C.J. No. 187 (B.C.C.A.) (Q.L), 2006 BCPC 32.

¹⁹ *Craats*, *supra* note 3 at 54.

“employee” comes to realize he or she has not only been “scammed” and has had his or her identity stolen, but has also unknowingly committed criminal acts.

3.1.6. Government Records

In an effort to take advantage of the online context in order to reduce costs, improve service delivery, and enhance openness and accountability, governments are making public records accessible online and through other electronic means. While such improved access has significant public benefits, it can also carry enormous costs for individuals whose personal information is accessed and abused by identity thieves.

A good example of this is in Florida, where a slew of records, including marriage and divorce records, property deeds and military discharge papers, were put online in 2002.²⁰ Although no cases of identity theft have been linked to the exposure of this information, the documents contained enough personal information for an identity thief to be highly successful. The Florida Legislature has ordered the masking of data to be completed throughout the state by the beginning of 2006. The Social Security Number of Jeb Bush was uncovered using these online documents.

The risk posed by personal information contained in court records has been recognized as a concern in Canada. The issue was raised in a 2003 discussion paper on open courts and electronic access to court records.²¹ Certain court records, for example family law court records, can contain a wealth of personal information. In a family law case, the court record will contain, among other documents, financial statements and income tax returns for three years.²² The income tax return documents contain sufficient personal information to enable an identity theft to engage in many of the activities described in Section 4. How do Thieves Use Stolen Personal Information?

Some government kiosks located in public places such as malls and government buildings can be a source of information about other citizens for an identity thief “in the know”. Governments in both Canada and the U.S. are trying to reduce costs and improve service delivery through the use of such kiosks.

In Ontario, kiosks offering automobile licensing services have been used by thieves in an elaborate scheme to steal automobiles by pretending to be the owner of the vehicle.

²⁰ Washington Post, “A Matter of Public Record”, online: [washingtonpost.com <http://www.washingtonpost.com/wp-dyn/content/article/2005/05/24/AR2005052401347_pf.html>](http://www.washingtonpost.com/wp-dyn/content/article/2005/05/24/AR2005052401347_pf.html).

²¹ Canadian Judicial Council, Judges Technology Advisory Committee, *Discussion Paper: Open Courts, Electronic Access to Court Records, And Privacy* (May, 2003), online: Canadian Judicial Council <<http://www.cjc-ccm.gc.ca/cmslib/general/OpenCourts-2-EN.pdf>>.

²² *Ibid.* at 31. The privacy risks posed by court records are currently limited by “practical obscurity”. “Practical obscurity” has come to refer to the inaccessibility of individual pieces of information or documents created, filed and stored using traditional paper methods relative to the accessibility of information contained in or documents referred to in a computerized compilation. Practical obscurity creates physical inconvenience by requiring that individuals attend at each courthouse to examine the dockets.

Having made note of a vehicle's licence plate number, the criminals pay \$20 for a Used Vehicle Information Package (UVIP) at a self-serve Ontario Ministry of Transport kiosk. This package included, in at least some cases, the owner's name and address. The thieves then forge a letter from the owner to obtain a copy of the ownership permit, from which a forged driver's licence is made. Again pretending to be the owner, they then obtain a new key for the vehicle, and proceed to steal it.²³

3.1.7. Tombstone Theft

The personal information of deceased persons can be accessed from newspaper obituaries and headstones. Obituaries provide birthdates, full names and frequently, critical family information. Careless funeral homes may provide personal information to thieves posing as the deceased's insurance company. An identity thief can use this information to create accounts and take out loans without repaying them.

For example, in Atlanta, the identities of 80 recently deceased persons were sold for \$600 each; the names and information were used to secure car loans totalling \$1.5 million. A career identity thief, using information obtained from a funeral home, and from the employer and bank of the deceased, was able to withdraw money from the latter's bank account.²⁴

3.1.8. Skimming (magnetic strip duplication)²⁵

Personal information may be stolen from the magnetic strip on debit and credit cards (or other cards), through the use of small electronic devices called "skimmers" or "wedges". By swiping the card through a skimmer (usually concealed under the counter or in an apron), a thief can copy the information stored on the debit or credit card's magnetic strip and use it in the creation of additional cards for fraudulent purposes. Any card with a magnetic strip - even a library card - can be reprogrammed, using a process similar to the one used by hotels issuing room cards instead of keys.²⁶

This can happen in an instant, without the owner of the card being aware of the theft. In 2004, thieves in Calgary duplicated the debit cards of 35 ATM users within an hour.²⁷ Instances of unauthorized skimming have been reported in gas stations, restaurants, and at ATM machines.

²³ Market Place, GTA, CBC, online: CBC.CA
<<http://www.cbc.ca/consumers/market/files/cars/gta/learn.html>>.

²⁴ Craats, *supra* note 3 at 41-42.

²⁵ Financial institutions do not regard debit or credit card fraud as a form of identity theft. However, it is generally regarded as such by the public and media, and it can be an important starting point for identity theft.

²⁶ Nathanson Centre, *Organized Crime in Canada: A Quarterly Summary* (July to September 2003), online: Nathanson Centre for the Study of Organized Crime and Corruption
http://www.yorku.ca/nathanson/CurrentEvents/2003_Q3.htm.

²⁷ Craats, *supra* note 3 at 60.

The skimmer is an electronic device that is sold legally.²⁸ It can read and write the magnetic strip commonly found on the back of credit, debit and calling cards. Skimmers are used in cash terminals to accept card payments. Certain transactions involve many sub-transactions that require the use of software. For example, a transaction can include processing the payment on the card and processing a credit to a rewards program. These complex transactions are handled by specialized software. The software will obtain the card data when the card is swiped in the skimmer. Once the data is obtained, it is used to carry out the different steps of the transaction.

The collection of this information is necessary for many organizations. It includes the account number, expiry date, name of the cardholder, etc.²⁹ It is conceivable that the personal information obtained at cash terminals could be used by identity thieves if not properly secured by the retailer.

Skimmers can be attached to a waiter's apron or be hidden under the counter. The transaction seems normal to the consumer, but in fact the card is swiped a second time, in the hidden skimmer, while the legitimate transaction is being processed by the sales terminal.

More sophisticated thieves attach portable readers onto ATM card slots, which read the card and pull the numbers from it. A small high resolution camera may also be installed in order to film the victim entering his or her personal identification number (PIN). Alternatively, the thieves may simply look over the victim's shoulder in order to record the PIN being entered. This is often referred to as "shoulder surfing". Another form of shoulder surfing is the use of a camera- equipped cell phone or miniaturized digital camera to snatch a picture of the credit card of the person at the front of the checkout line.

Other thieves will create fake ATM machines equipped with a skimmer and camera, and place them in public places. To the unsuspecting user, the ATM machine seems out of order and after a few swipes, the user gives up, leaving his or her personal information behind. Some thieves even have gone as far as installing real, albeit modified, ATM machines to capture card information.³⁰ This occurred recently in Ontario, where a customer was notified by her bank that her debit card was potentially compromised and it was necessary to cancel her card.³¹

The personal information culled from these cards may be used by the thieves themselves, or may be sold to others. The owner's identity can then be used to make unauthorized charges applied to the card. A secondary card can be created, extending the fraud further.

²⁸ Card Swipe Magnetic Card Readers, online: E System Sales
<http://ezcashregister.com/card_readers.htm>.

²⁹ Magnetic stripe card, online: Wikipedia <http://en.wikipedia.org/wiki/Magnetic_stripe_card>.

³⁰ *Nathanson Center*, *supra* note 26.

³¹ The London Free Press, "Identity theft comes close to home" (23 February 2006), online: London Free Press <<http://www.lfpress.ca/newsstand/Business/2006/02/23/1457797-sun.html>>.

Skimming is not limited to debit, credit and calling cards. Many other cards or documents use magnetic strips to store information. For example, airline boarding passes also contain a wealth of information on the individual.³² Hotel key cards can also be used, not to acquire personal information but to create fake debit and credit cards, since they use the same technology.

In August 2003 in Canada, five Russians were arrested for debit card fraud. Their scam involved the purchase and subsequent modification of five ATM machines. The machines were modified to capture all the necessary information to reproduce the card. They also captured the PIN number entered. About 4,000 people fell victim to the scam, all of whom were reimbursed by the banks. This fraud was the biggest debit-card fraud in Canadian history.³³

A smaller occurrence of skimming occurred in Alberta in 2005. The fraud was perpetrated by an employee of two gas stations. When a customer used either a credit or debit card for a purchase, the employee, Imran Safdar Naqvi, swiped the card using the skimmer and then observed the PIN number entered by the purchaser. The fraud was for a total amount of \$117,188.00.³⁴

3.1.9. Insider Theft

Identity theft often originates from within organizations holding personal information. Individuals are vulnerable because large data banks, governments and corporations hold a wealth of personal information over which the former have little or no control. This may include ATM card numbers, PIN codes, credit card numbers and expiry information, passwords, account information, and other personal information of value to thieves.

To a considerable extent, the security of this information is only as good as the integrity of the employees. Identity theft may originate with fraud by a disgruntled or financially strapped employee who sells personal information.

A recent US study revealed that up to 70 % of personal data stolen from companies was taken by internal employees.³⁵ Canadian financial institutions are also victims of insider abuse. Almost half of Canadian companies responding to a survey in DATE reported experiencing an internal security breach in the period between November 2005 and

³² Guardian Unlimited, "Q. What could a boarding pass tell an identity fraudster about you? A. Way too much" (3 May 2006), online: Guardian Unlimited <<http://www.guardian.co.uk/idcards/story/0,,1766266,00.html>>.

³³ *Nathanson Center*, *supra* note 26.

³⁴ *R. v. Naqvi*, [2005] A.J. No. 1593 (Alta. Prov. Ct. (Crim. Div.)) (Q.L.) 2005 A.B.P.C. 339 at 1 & 2, online: Alberta Courts <http://www.albertacourts.ab.ca/jdb/2003-/pc/criminal/2005/2005abpc0339.pdf>.

³⁵ Collins, J.M. and Hoffman, S.K., "Identity Theft: Predator Profiles", submitted to Security Journal (2004). Manuscript available from JudithCollins - judithc@msu.edu.

February 2006.³⁶ The federal Privacy Commissioner has noted that poor information management practices, particularly in data storage and retention, are the biggest problems facing organizations when it comes to identity theft committed by internal employees.³⁷

An Ottawa-based former employee of Clarica financial services was charged in April 2006 with stealing \$650,000 by impersonating company clients. The 105 charges of theft, fraud, impersonation and forgery referred to acts carried out between 1998 and 2004. Money was allegedly stolen in two ways: 1) by telling the company that clients wanted to redeem money from their accounts, and then forging their signature on the cheques, and 2) by stealing money from clients that was supposed to have been reinvested.³⁸

Even the Bank of Canada and its clients are not immune from identity thieves. In 2006, the personal information of 29 individuals was stolen from the Bank's payroll deduction database and counterfeit identity documents were created as part of a scheme to fraudulently redeem Canada Savings Bonds of customers across the country. The information, consisting of names, ages, birthdates, SINs and home addresses, was also used to obtain fraudulent credit cards and open cellular phone accounts. In all, the Bank of Canada was defrauded of more than \$100,000. The pair of thieves, one of whom has been charged with fraud and possession of property obtained by crime, worked for a call centre operated under contract on behalf of the bank.³⁹

In April 2006, the Ottawa RCMP and Ottawa Police Service arrested two individuals in connection with incidents of identity fraud which had victimized eight account holders of the Canada Savings Bond (CSB) Payroll Savings Program, for a total of about \$100,000. The individuals were employed by EDS, one of the bank's contractors.⁴⁰

In 2002 an employee of Teledata Communications Inc. of Long Island, New York, a company offering banks and other companies access to consumer credit information from commercial credit history bureaus, used his access to client codes and passwords to download credit reports. A network of twenty credit card fraudsters used this information to steal the money and identities of the clients concerned. Over the course of three years, the information of more than 30,000 people was stolen, leading to losses estimated to be between \$50 and \$100 million, including the life savings of some victims.⁴¹

³⁶ Neil Sutton, "Canadian financial institutions among global leaders in security", IT Business (13 June 2006), online: IT Business <http://www.itbusiness.ca/it/client/en/home/News.asp?id=39775&cid=7>.

³⁷ *Identity Theft Revisited*, *supra* note 4 at 5.

³⁸ Ottawa Citizen (26 April 2006) at C1.

³⁹ Ottawa Citizen (8 April 8, 2006) and Ottawa RCMP and Bank of Canada, Press Release (19 April 2006).

⁴⁰ itWorkCanada, "Bank fraud trail leads to former outsourcing help" (28 April 28, 2006), online: itWorkCanada <<http://www.itworldcanada.com/a/Security/3185acb5-1b95-4019-8bf9-a146ecf8446f.html>>.

⁴¹ *Craats*, *supra* note 3 at 92 – 97.

3.1.10. Purchasing stolen personal information

This is one of the easiest ways to acquire personal information about unsuspecting victims. Personal information can be acquired via “carder networks” and other underground networks which specialize in personal information trafficking. The personal information available from these sources will usually be the result of insider abuse or the remote exploitation of computer vulnerabilities to access large client databases.⁴²

In 2003-2004, a large “carder network” was dismantled by the Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice, and other U.S. Attorneys' offices and law enforcement agencies.⁴³

In the Alberta case mentioned above in s. 3.1.8, the thief sold debit and credit card information acquired by skimming to a high school acquaintance. He charged \$100.00 for each skimmed card and realized a total profit of over \$117,000 before he was caught.⁴⁴

3.1.11. Identity Consolidation – “Breeding”

Once an identity thief has obtained a small quantity of information, it is possible to obtain more personal information using the available information. This process is called “identity breeding”. For example, an identity thief who has the driver’s licence and health care card of an individual can use these identification documents to obtain a replacement SIN card for the victim, and then engage in financially-rewarding fraudulent activities in the victim’s name. To obtain a replacement SIN card, a birth certificate must first be obtained. Requirements to obtain a birth certificate depend on the province of birth. In Quebec, the required information is limited to one document bearing their current home address and one piece of photo ID.⁴⁵

3.2. **Technology-Based Identity Theft Techniques**

3.2.1. Phishing

Phishing is a hybrid technique in the sense that it involves both the use of technological means and social engineering by masquerading as a trustworthy organization in an e-mail message. The e-mail message is used to lure victims into providing account and other personal information. . A new and fast growing online scam, “phishing” now accounts for 20 – 25 % of identity theft incidents.⁴⁶

⁴² *Identity Theft Revisited*, *supra* note 4 at 24.

⁴³ U.S Department of Homeland Security, “U.S. Secret Service’s Operation Firewall Nets 28 Arrests” at 1, online: United States Secret Service <<http://www.secretservice.gov/press/pub2304.pdf>>.

⁴⁴ *Navqi*, *supra* note 34 at 1- 2.

⁴⁵ Conditions pour obtenir un certificat de naissance, online: Directeur de l’état civil <<http://www.etatcivil.gouv.qc.ca/English/Conditions.htm>>.

⁴⁶ Rosie Lombardi, “Myths about identity theft debunked by experts”, IT World Canada (22 March 2006), online: Webwereld <<http://www.webwereld.nl/articles/40378/myths-about-identity-theft-debunked-by-experts.html>>.

Phishing messages have become extremely sophisticated, such that consumers cannot easily distinguish them from legitimate messages from the targeted institution. They typically contain an alert that something is wrong with the victim's account, or ask that personal information and passwords be updated, corrected or verified. In an ironic twist, some phishing messages even come in the form of a fraud alert. The message is written in a language similar to that used by the organization; it will also use the same colors and logos - this is known as "spoofing". There is a sense of urgency to the message. The urgent nature of the message may dupe even those who are not customers of the company being impersonated to respond. Phishing messages may also direct the user to a fake web site (see "pharming", below), or to send in the information by fax or phone. Worms and viruses may spread the phishing e-mail further, via victims' address books.

These sites also count on the lack of awareness by the average user of details which distinguish legitimate web sites from unlawful duplicates. For example, the domain name of spoofed sites often use slight variations of the real site's domain name (such as www.amaazon.ca instead of www.amazon.ca).

According to Robert Siciliano, a security consultant, unwitting individuals respond to five of every 100 phishing emails that ask for personal information.⁴⁷ Individuals respond to these emails because they look authentic. In fact, when U.S. adults participating in a study were asked to determine if emails were fraudulent, the error rate was approximately 30%.⁴⁸ It should be noted that some phishing sites and emails look so realistic they have the potential to fool even the most prudent internet users.

Most phishing scams are directed at U.S. consumers. However, the Anti-Phishing Working Group in April 2005 found more than 2,850 active sites, masquerading as almost 80 different legitimate companies, in 68 countries.⁴⁹ It is estimated that in the month of April 2004, three billion phishing e-mails were sent around the world.⁵⁰ Gartner estimated in April 2004 that 1.78 million Americans had responded to phishers.⁵¹

Clients of Canadian financial institutions are also often the targets of phishing scams. A recent poll conducted by Ipsos-Reid found that 24% of Canadians have received emails purporting to be from a financial institution that asked them to verify their input account, password or personal information.⁵² Fourteen percent of Canadian recipients have become victims of these schemes. According to AOL Canada's Phishing Study, almost one out of every three Canadians surveyed have received an email from a company seeking confirmation of their account information. Alarmingly, 12 per cent surveyed

⁴⁷ Journal Sentinel, "Banks must do more to fight identity theft, expert says" (8 February 2006), online: <http://www.jsonline.com/story/index.aspx?id=391823>.

⁴⁸ Rachael Lininger and Russel Dean Vines, *Phishing – Cutting the Identity Theft Line* (Indianapolis, Indiana: Wiley Publishing, 2005) at 1.

⁴⁹ *Ibid* at 51

⁵⁰ *Craats*, *supra* note 3 at 164.

⁵¹ Gartner, About Gartner, online: http://www.gartner.com/it/about_gartner.jsp.

⁵² Ipsos-Reid, Concerns over Identity Theft on the Rise (22 November 2005).

admitted to clicking through an email link or URL to “confirm” their account information.⁵³

The various steps involved in phishing are illustrated in Appendix A.

3.2.2. Pharming

The term “pharming” is derived from the term “phishing”, which is discussed in s.3.3.1. Pharming is also known as “domain spoofing”. It is the use of a spoofed website to entice unwitting individuals into giving up their personal information.⁵⁴

Pharming can be accomplished using two different techniques. In the first technique, the computer host’s file is compromised by entries which map legitimate domain names to illegitimate IP addresses. The second technique is known as Domain Name System (DNS) poisoning. Vulnerabilities in DNS software are exploited in order to gain control over the domain name of an existing website. The numeric address associated with the textual domain name is then changed. The result is that when an unsuspecting user enters the website address that has been changed into their browser, they will automatically be brought to the spoofed site. Their browser’s address bar will show the correct address, but the site displayed will be a fake one. The different steps involved in establishing a pharming scam are outlined in Appendix B.

In both cases, the internet user is fooled into thinking that the site is legitimate.

3.2.3. DNS Cache poisoning

This technique resembles that of pharming, in that unsuspecting internet users are directed to a fake website that looks remarkably like that of a legitimate organization. The main difference is that the tampering of the DNS record is done locally on the computer used to access a website, instead of in a DNS server. The tampering is done in a file called the “hosts file”.⁵⁵

DNS cache poisoning will usually be perpetrated using a Trojan Horse application, a virus or some spyware. The application will add a record for a valid site into the computer’s host file. The IP address placed in the record will redirect the user to the thief’s website instead of to the real website. Users are then asked to enter their personal

⁵³ AOL Canada, Identity Theft Rated Primary Online Security Concern Among Canadians (29 March 2005), online: AOL.ca <http://canada.aol.com/press/press_03_29_05.adp> [AOL].

⁵⁴ The Washington Post, “Citibank Phish Spoofs 2-Factor Authentication” (10 July 2006), online: [washingtonpost.com <http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html>](http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html).

⁵⁵ Hosts file, online: Wikipedia <http://en.wikipedia.org/wiki/Hosts_file>. When a textual internet address needs to be translated into a numeric IP address, the operating system will try to find this association in the hosts file first. If a numeric IP associated with the textual address is not found in the hosts file, a request will be sent to a DNS server.

information. In 2006, clients of more than 100 financial institutions in the United States and Europe were targeted by such an attack.⁵⁶

3.2.4. Spyware, Malware and viruses

Spyware is known for causing system slowdowns or crashes as well as unwanted advertising and interminable pop-up messages. But it can also have more serious consequences, including identity theft. This is because certain forms of spyware enable the activities of computer users to be tracked and the contents of the hard drive to be accessed.⁵⁷

Although firewalls, anti-virus programs and anti-spyware programs can help prevent the installation of spyware onto personal computers, they must be kept up-to-date and are not foolproof in any case. Many users continue to be tricked into installing spyware or malware-laden software onto their computers. According to an Aladdin Knowledge Systems study, spyware is the fastest-growing threat to enterprises, increasing more rapidly than Trojans, viruses and other risks.⁵⁸ A Web@Work survey found that 92% of organizations surveyed reported being infected by some form of spyware. About 17% reported that at least one employee had launched a key logger or other hacking application.⁵⁹

Spyware can be attached to a computer to manipulate what happens on it, and to collect information about an individual or organization. Some spyware and other malware can be used with cell phones, smart phones and PDAs. Some software programs enable criminals to collect résumés, PIN codes, banking information, credit card numbers and other financial information, remotely and without the victim's knowledge.

Thieves keep developing new computerized techniques to acquire personal information. For example, a new type of spyware, called a "banking Trojan", has started to appear. This application integrates into the web browsers installed on a user's computer and monitors the user as he or she is navigating to websites. If the user navigates to the targeted bank's site, the program executes and replaces portions of the bank's website with a replica. The portion of the site replaced in this manner is usually the page where a user can log into his or her account. When the user enters his or her credentials, they are sent to the author of the banking Trojan instead of to the bank's site. As of 2006, these banking Trojans have been used mainly to target South American Banks. The first attack against a North American institution was in 2006 against American Express.⁶⁰

⁵⁶ Ryan Naraine, "Computer Virus 'Hijacks' American Express Web Site" *Fox News* (1 May 2006), online: FOXNews.com <<http://www.foxnews.com/story/0,2933,193784,00.html>>.

⁵⁷ *Craats, supra* note 3 at 71.

⁵⁸ Jason Turcotte, "Spyware threats skyrocket for enterprises", *Application Development Trends* (14 June 2006), online: *Application Development Trends* <<http://www.adtmag.com/article.aspx?id=18724>>.

⁵⁹ "Websense Web@Work Survey: Nearly One in Five Organizations Hit by Keyloggers in 2006" (15 May 2006), online: FRESHNEWS.com <http://www.freshnews.com/cgi-bin/jsj_news/print.cgi?article_ID=31879>.

⁶⁰ *Naraine, supra* note 56.

In a recent case, a Trojan was combined with phishing to target AOL subscribers. The result was the distribution of the Trojan to victims via email. When a person using an infected computer tried to log onto their AOL account the software would prevent them from doing so until the user provided credit card numbers, bank account numbers and other personal information.⁶¹ This type of attack resembles the banking Trojan described above.

3.2.5. Internet Searches and Google Hacking

A considerable amount of personal information can be obtained through searches of legitimate web sites, using search engines such as GoogleTM, locator pages, superpage sites and genealogy sites (which contain death records, birthplaces and sometimes Social Security numbers).⁶² Some sites and data banks also contain court records, registrations and background searches. U.S. sites such as NetDetectivesSoftware and DocuSearch.com contain detailed personal information, which thieves can access for about US\$200.⁶³

Google Hacking consists of using Google's search engine to find "hidden" documents on a website. Many organizations do not realize how much information can be exposed from their website when it is not properly configured and managed. These documents can contain information such as payroll details and employee files, including SINS.

As pointed out by Sullivan, identity thieves who acquire personal information using search engines and carefully crafted search queries are not necessarily computer geniuses.⁶⁴ Tutorials on how to locate specific information using search engines are readily available and can be understood by a large majority of internet users.

There have been no reports of identity theft committed as a result of the use of Google hacking to acquire the personal information of Canadians. However, Google hacking "attacks" are on the rise world wide.⁶⁵

3.2.6. Exploiting computer systems' security vulnerabilities (cracking)

Other types of hacking involve exploiting known security holes or vulnerabilities in software such as Microsoft Windows. Corrupt data and a set of instructions are sent to the software running on a targeted computer. The corrupted data confuses the software and it will start to execute the new instructions sent by the cracker. The goal is usually to install

⁶¹ Robert McMillan, "Six charged in breakup of AOL identity theft ring" *IDG News Service* (29 September 2006), online: Computerworld

<<http://www.computerworld.com.au/index.php/id;1195237489;fp;4;fpid;1398720840>>.

⁶² *Craats*, *supra* note 3 at 71.

⁶³ *Ibid.* at 72.

⁶⁴ Bob Sullivan, *Your Evil Twin: Behind the Identity Theft Epidemic* (Hoboken, New Jersey: John Wiley & Sons, 2004) at 209.

⁶⁵ "Google hacking' attacks rising" (19 May 2006), online: Massey University <http://masseynews.massey.ac.nz/2006/Massey_News/issue-08/stories/01-08-06.html>.

a “Trojan Horse” application, which opens a backdoor. The backdoor enables a connection to be made to the computers of an individual or a company without being noticed and allows personal information to be collected surreptitiously.

This technique differs from using spyware, as spyware applications run automatically. In Canada, RCMP statistics show that 120 cases were opened in 1997 and 269 in 2000 which involved "unauthorized use of a computer" and "mischief in relation to data".⁶⁶ In 1999, a resident of Thunder Bay was convicted of hacking, by which he illegally obtained passwords then used to gain free internet access.⁶⁷

Canadian banks are also targets of crackers. According to a study of financial institutions conducted by Deloitte between November 2005 and February 2006, 78 per cent of Canadian respondent companies said they had been subject to some kind of external security breach in the last 12 months.⁶⁸ Security breaches are discussed further in the CIPPIC White Paper entitled “Approaches to Security Breach Notification”.

3.2.7. Wardriving (Drive-by Identity Theft)

In this form of identity theft, thieves take advantage of wireless technology, which allows households to have several computers connected to a network at the same time. The thieves, sometimes referred to as “war drivers”, drive through neighbourhoods, detecting Wi-Fi wireless networks. Wireless equipped laptops and PDAs and software readily available on the internet are used to find unsecured networks. For better detection range, antennas are built or bought, which vary from omni-directional to highly directional.

Once an unsecured network is located, the thief can use it to access the user’s computers. It may be possible to obtain passwords and other personal information, such as bank and credit card information, from files stored in the computers on the network.

Information on unsecured wireless networks is circulated in a magazine called “2600”, which first appeared in 1984.⁶⁹ This publication contains special passwords, codes and information about vulnerable areas for stealing bandwidth. According to Craats, “wardrivers” may assist other wardrivers through markings on buildings, showing vulnerable and protected areas - a form of “underground communication”.⁷⁰

It should be noted that not all wardriving is done with the intent of accessing other computers. For many, this is a hobby similar to bird watching, or just a means of

⁶⁶ RCMP, Criminal Analysis Branch, Criminal Intelligence Program, *Hackers: a Canadian Police Perspective* (30 May 2001), online: Royal Canadian Mounted Police (RCMP) <http://www.rcmp-grc.gc.ca/crimint/hackers_e.htm>.

⁶⁷ Jen Ross, “Canada called 'hacker haven' for criminals” (19 May 1999), online: Electronic Frontier Canada <<http://www.efc.ca/pages/media/globe.17may99b.html>>.

⁶⁸ Sutton, *supra* note 36.

⁶⁹ 2600: The Hacker Quarterly, online: 2600: The Hacker Quarterly <<http://www.2600.com/>>.

⁷⁰ Craats, *supra* note 3 at 59.

obtaining free internet access. Some wardrivers will indeed warn the network owners that their network is unsecured and vulnerable.

However, this was not the intent of Brian Salcedo, who tried to obtain credit card information from the Lowe's chain of home improvement stores in Southfield, Michigan. He and his partner accessed the company's central data centre using an unsecured Wi-Fi connection at one of the stores. From the data centre, they could access all of the other stores' networks. Salcedo modified a program which handled credit card transactions, so that it would store the card information in a location from where he could later retrieve it. For his role in the scheme, he was sentenced to nine years imprisonment.⁷¹ His sentence was affirmed on appeal.

3.2.8. Acquiring used computer equipment

Organizations regularly update their desktop computers and servers. The hard drives in discarded computers can contain the "mother lode" of the former owner's personal information.⁷² This is also true for servers which contained databases on clients or users.

Often, when old equipment is discarded, the hard drives or other old storage equipment are not properly erased, to completely destroy any personally identifiable information they contain.⁷³ Simply deleting files is not enough. When a file is deleted, its name is removed from the list of files on the hard drive but its content is still present on the hard drive. Unless and until old data is over-written multiple times by new data, any deleted information remains retrievable. The process of securely (completely) erasing data is called "white space wiping".

The potential risk posed by computer equipment inappropriately disposed of was highlighted by the actions of two graduate students at the Massachusetts Institute of Technology. They bought used computer hard drives and scanned them for personal information. Medical correspondence and credit card numbers are examples of the type of information they found.⁷⁴

A similar scenario unfolded in British Columbia in March 2006, when 41 computer tape backups containing personal information of British Columbians were auctioned. The tapes contained information about medical conditions, details about applications for social assistance and caseworker entries containing intimate information about peoples' lives.⁷⁵ Although this information is unlikely to have been used by thieves, this example serves to illustrate the ease with which detailed personal information stored in electronic

⁷¹ Kevin Poulsen, "Crazy-Long Hacker Sentence Upheld" (11 July 2006), online: Wired News <<http://www.wired.com/news/technology/0,71358-0.html>>.

⁷² Office of District Attorney John J. Conte, Worcester County, *How to Protect Yourself from Identity Theft*, online: http://www.worcesterda.com/Consumer_Info/identity_theft_protect.html.

⁷³ *Ibid.*

⁷⁴ SecurityFocus, "Discarded computer hard drives prove a trove of personal info" (15 January 2003), online: <http://www.securityfocus.com/news/2055>.

⁷⁵ *Identity Theft Revisited*, *supra* note 4 at 3.

databases can be inadvertently disclosed to unauthorized persons and thus made vulnerable to abuse.

3.3. Social Engineering Techniques

Social engineering involves exploiting the natural tendency of a person to trust others, especially people with whom they have some sort of relationship. This trust can be exploited by thieves, using a variety of techniques, to acquire personal information.

3.3.1. Pre-texting

Pre-texting is a relatively unsophisticated method of obtaining personal information, one which relies on “smooth talking”. Social engineers trick the victim or third parties with whom the victim deals into revealing the victim’s personal information. The key to their success is to win the trust of an individual and to thereby convince the person to go against their instincts or better judgment.

Social engineering can be used to acquire personally identifiable information directly or it can be a component of a more complex acquisition process. Social engineering can be exercised directly against the victim or against a third party with whom the victim has dealings, in order to acquire information about the victim.

Pre-texters attempting to get personal information about the victim from a third party will typically target companies with whom the victim may do business, or close relatives of the victim. They will contact the other party, pretending to be an employee of that company, or of another company with whom the victim does business, and ask for the victim’s account information. They may pretend to conduct telemarketing surveys which require certain personal information to be provided.⁷⁶ They may pretend to call from a “do not call” registry or an anti-fraud organization, requesting personal information on the victim in order to sign up for protection programs. Pretexters also operate in internet chat rooms, where their targets are often children and young adults.

Other targets include employees of companies holding personal information. A “smooth talker” may be able to obtain key details about clients from customer service representatives, by pretending to be the victim or another employee at the company in question. Thieves experienced with this type of “social engineering” are often skilled at duping consumer service agents when telephoning – waiting for young-sounding or inexperienced agents to serve them.⁷⁷ Consumer service agents are often overworked and underpaid, which makes them easy targets for experienced social engineers. It is up to the organization to implement effective authentication procedures before disclosing personal information about customers to individuals purporting to be someone they may not be.

⁷⁶ *Craats*, *supra* note 3 at 63.

⁷⁷ *Ibid.* at 22.

During the early 2000's, a small industry developed around the sale of cell phone records in Canada and the U.S. Although currently targeted by lawmakers, such services are still being advertised on the internet. In exchange for a fee, private investigators offer to obtain cell phone records of specific individuals. They manage to obtain the records, in many cases, by pretending to be the account holder or an employee of the company. This was the case in a highly publicized Canadian incident in which a journalist managed to obtain the Privacy Commissioner's cell phone records from all three Canadian cell phone providers.⁷⁸

In 2000 U.S., Government Accountability Office (GAO) investigators tested security procedures at different institutions. They were able to gain access to secure areas of federal buildings and commercial airports by wearing bogus badges. In 2002, they were also able to obtain various drivers' licences, even when their applications or supporting documentation had plain errors.⁷⁹

One of the most highly publicized cases of social engineering was the breach of the giant U.S. databroker ChoicePoint's authentication mechanism. Some scam artists, using social engineering techniques to pose as a legitimate business, were able to access 150,000 detailed records.⁸⁰ A similar case occurred in Canada in 2004. Individuals gained access to credit files of 1400 Canadians held by Equifax Canada Inc., one of the three major consumer reporting agencies in Canada. The individuals posed as legitimate credit grantors and were able somehow able to satisfy Equifax's authentication procedures.⁸¹

3.3.2. Obtaining credit reports

Thieves may pose as a business with a legitimate interest in getting a victim's credit report⁸². They can pose, for example, as a landlord, a potential employer or a used car seller. As shown by the ChoicePoint breach, the vetting procedures established by data aggregators and consumer reporting agencies are not insurmountable for committed identity thieves.⁸³

3.3.3. Bogus Employment Schemes

Bogus employment advertisements can be used to obtain personal information, by requesting resumes or completed application forms. This happened recently in Ottawa,

⁷⁸ Jonathon Gatehouse, "You are exposed" *MacLeans* (21 November 2005), online: <http://www.macleans.ca/topstories/canada/article.jsp?content=20051121_115779_115779> and "MacLean's Ability to Purchase Jennifer Stoddart's Phone "Records", *NYMITY News* (February 2006), online: <<http://www.nymity.com/privaviews/2006/Elder.asp>>.

⁷⁹ *Sullivan*, *supra* note 64 at 134 – 138.

⁸⁰ *Identity Theft Revisited*, *supra* note 4 at 8.

⁸¹ Mark Hume, "Identity theft feared after credit information stolen" *The Globe and Mail* (16 March 2004), online: [globeandmail.com](http://www.theglobeandmail.com/servlet/story/RTGAM.20040316.wxcredit0316/BNStory/Front) <<http://www.theglobeandmail.com/servlet/story/RTGAM.20040316.wxcredit0316/BNStory/Front>>.

⁸² Graeme R. Newman & Megan M. McNally, *Identity Theft Literature Review* (July 2005) at 43, online: National Criminal Justice Reference Service <<http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf>>.

⁸³ *Identity Theft Revisited*, *supra* note 4 at 11.

where a job listing was posted on a website and people were asked to submit resumes and provide a range of personal information on an application form, including SIN and driver's licence numbers.⁸⁴

A similar scheme occurred in British Columbia, when an identity thief posted construction manager positions in the newspaper. When individuals replied, they were asked to provide personal information. Using his photograph, the perpetrator then forged or applied for new identification using the applicants' personal information. Using the additional identification documents, he opened bank accounts and deposited forged cheques. Through his scheme, he obtained close to \$80,000 before being caught.⁸⁵

3.3.4. Contests and Surveys

Personal information may be provided by individuals under the impression that they are entering a contest or participating in a survey. Their information is, however, then used by thieves. This can happen by means of written submissions to contests or draws for prizes, or through telephone and e-mail soliciting. Surveys and contests can also serve as the basis of phishing emails. Unsuspecting individuals will submit personal information for the chance to win prizes.

In Australia, an actress posing as a pollster conducting a retail survey asked respondents to provide the following information: person's full name, their date of birth, contact number, home address and mother's maiden name, their marital status, nationality, occupation, citizenship status and which bank they used. Of the 30 people stopped, 20 answered every question. Another seven answered every question except one, but only two people refused to answer any of the personal questions.⁸⁶

4. HOW DO THIEVES USE STOLEN PERSONAL INFORMATION?

Once enough personal information has been obtained about an individual, the thief is ready to start the second step of identity theft: unlawful use of the information. The unlawful use usually, but not necessarily, involves fraud.⁸⁷

An important feature of identity theft, when it comes to unlawful uses, is the offender's repeated victimization of a single individual. This may include repeatedly using a stolen credit card, taking over a card account, or using stolen personal information to open new accounts. The main reason why so many frauds can be committed is the fact that it may be a long time before a victim detects that something is wrong. According to the police guide on identity theft, it typically takes 14 months before victims of identity theft realize they have been victimized.

⁸⁴ Ottawa Citizen (14 March 2006).

⁸⁵ *R. v. Taft*, [2003] B.C.J. No. 444 (B.C.C.A) (Q.L.), 2003 B.C.C.A. 104.

⁸⁶ Rohan Wenn, "Families fooled in privacy scams" *Seven Network (Operations) Ltd.* (23 May 2006), online: Yahoo! 7 News <<http://seven.com.au/todaytonight/story/?id=28500>>.

⁸⁷ Some uses may not be fraudulent. For example, someone could take over another person's email account, and use it to send defamatory or threatening messages. The victim is not actually defrauded of anything.

The repeat victimization of the same individual is evidenced by an Ipsos-Reid poll which shows that many of the victims or those who personally knew a victim of identity theft suffered more than one incident of fraud.⁸⁸ The statistics on the different outcomes from the poll are represented graphically in Figure 4.1. Some possible outcomes are not represented in this figure, probably because none of the participants in the poll were victimized in that particular way.

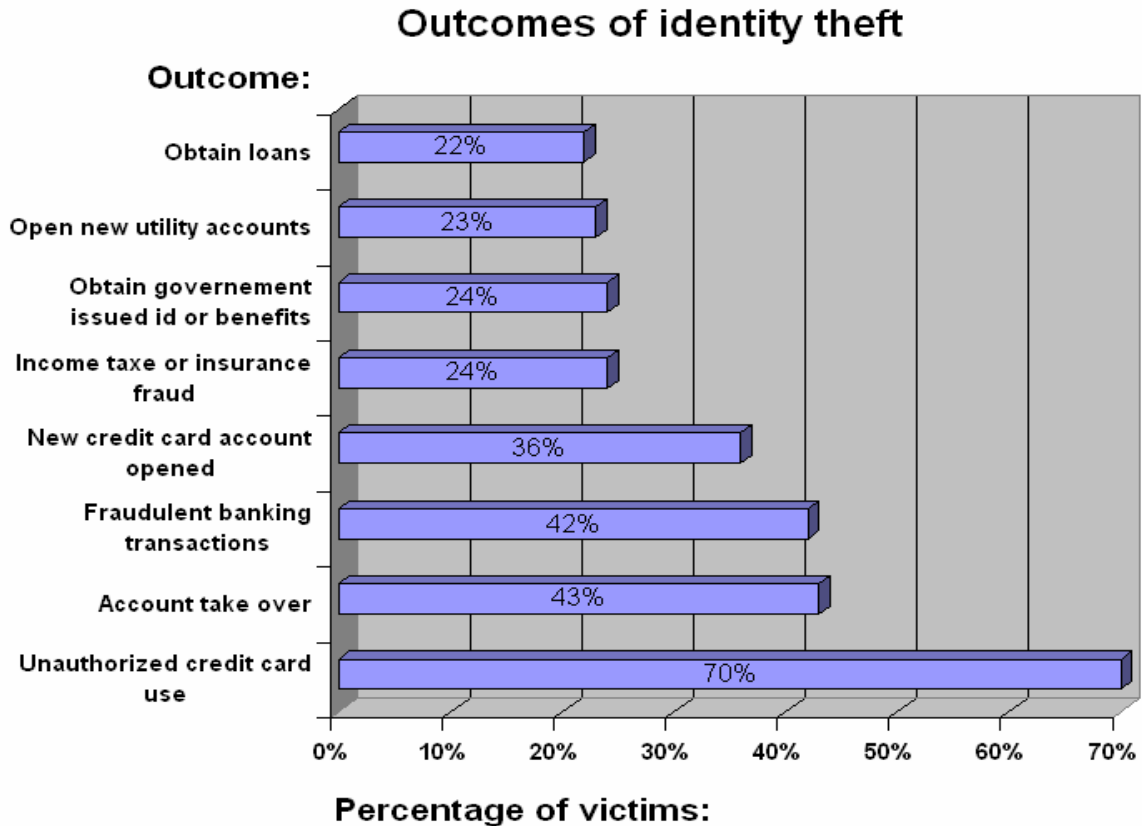


Figure 4.1 - Outcomes of identity theft

The same issues associated with the reporting of identity theft by victims also causes problems when conducting the inventory of unlawful uses. Certain unlawful uses might have occurred, and may still be occurring, without them being reported.

The remainder of this section provides examples of unlawful uses of personal information of victims.

⁸⁸ Ipsos-Reid, Concern about Identity Theft Growing in Canada (28 February 2005). The poll is based on the responses from 1001 adult Canadians.

4.1. Selling personal information

This form of unlawful use will usually be committed by insiders or crackers who have stolen a good amount of personal information. Except under very limited circumstances, selling personal information to another individual is not illegal in Canada. Currently, the *Criminal Code* only makes illegal to sell or transfer credit card data (s. 342) or computer passwords (s. 342.1). Selling driver's licence numbers and social insurance numbers is not prohibited. Personal information sold can come from using any of the acquisition techniques described above.

The economic gain does not come from exploiting the information directly but rather by selling it on the black market to others who will ultimately use it to commit fraud. "Carder networks" are a good example of how thieves derive economic gains from stolen information without committing fraud using the credit card data.

According to Sergeant Jim Hyde of the Florida State Police, drug traffickers are increasingly engaging in identity theft, which is as lucrative as the drug trade but which lacks the harsh sentences of drug trafficking.⁸⁹

According to the Toronto Fraud Squad, a fake health card can be worth \$200, as foundation document, and could fetch up to \$5,000 if used to fraudulently obtain health care.⁹⁰

4.2. Forging identity documents

Thieves often use personal information to create fake credit and debit cards, fake driver's licences or vehicle registration certificates and other identity documents. These forgeries will then be used to commit fraud.

This occurred in the city of Toronto in October 2005. A theft ring created counterfeit health cards, driver's licences, credit cards and other key documents. They then used these as foundation documents to open new bank accounts.⁹¹

4.3. Taking over existing accounts

Once thieves have enough personal information of a particular victim they can contact organizations with whom the victim has existing accounts. When contacting these organizations, they will masquerade as the victim (see "pretexting", at s. 3.3.1 above).

Thieves take control of the accounts by changing the mailing address or the credentials used to access the account. A thief could take over a bank account and empty it out over a short period of time to avoid raising any suspicions.

⁸⁹ Newman & McNally, *supra* note 82 at 26.

⁹⁰ Gordon Atherley, *Identity Theft in Healthcare A White Paper*, Greyhead Associates (January 2006), at 8, online: Teranet Inc. http://www.teranet.ca/corporate/publications/Identity_Theft_In_Healthcare.pdf.

⁹¹ Report F06-01, *supra* note 2 at 7.

4.4. Opening new accounts

With a minimum of personally identifiable information, such as name, address and SIN, an identity thief can open all sorts of accounts, such as bank accounts, credit accounts (either credit cards, credit lines or loans), in-store accounts and cell phone accounts. Some thieves, as discussed below, go as far as obtaining mortgages in a victim's name. In some cases, student loans have been obtained using a series of assumed names.⁹²

Usually, once the account is opened, the thief will change the billing or correspondence address in order to conceal his or her activity from the victim. By changing the address, the thief has a longer window of opportunity to commit fraud using the new accounts. The victim usually will not realize something is wrong until a credit application is refused or a debt collector contacts him or her.

4.5. Ordering goods online using a drop-site

A thief may shop online using stolen personal information, and usually using a computer based in a different jurisdiction from that of the victim. A different country altogether is often used, frequently in Africa. The thief will order some items in the victim's name and using the victim's credit card number. The thief will ask the merchant to deliver them at a "drop site", where a trusted third party or associate will receive them. This associate repackages the items and ships them to the thief. If the authorities check out the drop site, the associate has a defence of plausible deniability.⁹³ Prosecuting the foreign conspirator(s) is almost impossible because of jurisdictional and resource issues.

This type of scheme is described in the 2003 Alberta case of *R. v. Lukian*.⁹⁴ Lukian obtained credit card numbers from the internet and used them to buy merchandise which was shipped to North Dakota. His accomplice would then re-package and re-ship the items back to Lukian in Edmonton.

4.6. Securing employment

An thief who has a criminal record may try to use another person's identity to secure a position which requires a criminal record check as a prerequisite. The thief can also masquerade as the victim in order to apply for positions for which the victim has the appropriate experience and/or education.⁹⁵ Finally, an thief may attempt to obtain employment under another's name to avoid paying income tax.

⁹² *R. v. Thomas*, [2002] B.C.J. No. 734 (B.C. Prov. Ct. (Crim. Div.)) (Q.L.), 2002 B.C.P.C. 113.

⁹³ Michael J. Elston and Scott A. Stein, "International Cooperation in On-Line Identity Theft Investigations: A Hopeful Future but a Frustrating Present", online: International Society for the Reform of Criminal Law <<http://www.isrcl.org/Papers/Elston%20and%20Stein.pdf>>.

⁹⁴ *R. v. Lukian*, [2003] A.J. No. 1495 (Alta. Q.B.) (Q.L.), 2003 A.B.Q.B. 989.

⁹⁵ Office of the Privacy Commissioner of Canada, *Fact Sheet: Identity Theft: What it is and what you can do about it*, online: Privacy Commissioner of Canada <http://www.privcom.gc.ca/fs-fi/02_05_d_10_e.asp>.

4.7. Obtaining a passport

Transnational criminal and terrorist organizations may, as part of their modus operandi, misuse fraudulently obtained travel documents to support their illegal activities.⁹⁶ Although Canadian passport rules have recently been tightened, fraudsters may still be able to obtain passports using stolen personal information.

4.8. Obtaining government benefits

Thieves may be able to obtain various government benefits such as Employment Insurance, welfare and Old Age Pension benefits, by masquerading as another person, using stolen personal information. This technique has been used for many years by Thomas as demonstrated at her sentencing.⁹⁷ Amongst other frauds, Thomas defrauded the Receiver General by obtaining student loans in the name of others, she also defrauded Human Resources Development Canada by obtaining employment insurance in the name of others and finally she defrauded the Province of British Columbia, Ministry of Social Development and Economic Security by obtaining welfare.

4.9. Obtaining health services

A stolen health card can be used to obtain medical services under the victim's name. A thief who sells counterfeit health cards to obtain medical services can fetch up to \$5,000 per card.⁹⁸ An thief who gains access to a victim's health card number could also try to get prescriptions for narcotics.⁹⁹

A potentially serious consequence of individuals fraudulently obtaining medical services under another's name is the addition of erroneous data to the real patient's medical records. This occurs without the real patient's knowledge and consent. The inaccurate information could mislead health providers, ultimately putting the patient's life at risk.¹⁰⁰

According to a study, between 250,000 and 500,000 Americans have been victims of this type of unlawful use of their personal information.¹⁰¹ The World Privacy Forum has found that more than 19,000 complaints of medical identity theft have been filed with the U.S. federal government.¹⁰² Comparable statistics for Canada are not available. However,

⁹⁶ Passport Canada, *Order Amending the Canadian Passport Order (SI/2001-121)* (1 September 2004), online: Passport Canada <http://www.ppt.gc.ca/publications/order_04-113_e.aspx>.

⁹⁷ Thomas, *supra* note 92.

⁹⁸ Atherley, *supra* note 90 at 8.

⁹⁹ Calgary Police Service, "Identity Theft - Do not let it happen to you" (Winter 2004).

¹⁰⁰ Craats, *supra* note 3 at 9.

¹⁰¹ Eileen Ambrose, "Watch out for medical identity theft" (15 May 2006), online: baltimoresun.com <<http://www.baltimoresun.com/business/yourmoney/bal-ambrose0515,0,1144222.column?coll=bal-news-columnists>>.

¹⁰² ABC News, "Medical ID Theft Can Wreck Victims' Health and Finances" (3 May 2006), online: ABC News <<http://www.abcnews.go.com/GMA/Health/story?id=1917165&page=1>>.

the Ontario Ministry of Health and Long-Term Care website makes mention of identity theft as a source of health care fraud in the province.¹⁰³

4.10. Hijacking email accounts

Service account hijacking, a form of computer fraud, involves taking over the victim's email address, domain name, chat account or other computer based identifiers, and sending messages to others in the name of the victim. Usually this type of identity theft is related more to defamation than to fraud for economic gain, although it can be used for the latter. Another common purpose for hijacking internet accounts is to send spam.

4.11. Making long distance calls

This technique involves using an existing calling card or acquiring a new calling card using the personally identifiable information of the victim. The card is then used to make long distance calls. In some cases, the thieves use the cards to sell cheap long distance calls to newly arrived immigrants.

4.12. Concealing one's true identity

When using personal information for concealment, the offender assumes another's name to cover up past crimes and avoid capture, sometimes over many years. The offender can also use another's name and identification to avoid arrest. The September 11 hijackers, for example, all used some form of false identity, which resulted in the subsequent arrest of the identity theft victims.

CALPIRG's research has shown that in 15% of cases, the thief continues to impersonate their victim when arrested, providing the victim's personal information to the police.¹⁰⁴ In St. Louis, a woman was convicted for a drug crime and even served time in prison under a relative's name. The victim only found out about the crime when she discovered she had a felony record.¹⁰⁵ Our review of Canadian caselaw related to identity theft has revealed that in many cases, the identity thief provided a victim's name when arrested.

The personal information of another person may also be used to cover a criminal's tracks when committing other crimes¹⁰⁶. This dramatically increases the difficulties faced by law enforcement in investigating other crimes. As well, this type of concealment can be devastating for victims. A routine traffic check may result in the identity theft victim being handcuffed and taken into custody.

¹⁰³ Ontario Ministry of Health and Long-term Care, *Health Card Fraud*, online: Ontario Ministry of Health and Long-term Care <http://www.health.gov.on.ca/english/public/pub/ohip/card_fraud.html>.

¹⁰⁴ CALPIRG, *supra* note 16 at 8.

¹⁰⁵ Peter Shinkle, "Frequent culprits in ID theft are friends, family" *St. Louis Post* (15 March 2006), online: Operation Restore Trust of Iowa <http://www.stopmedicarescams.org/press_room/?page=releases&view=53>.

¹⁰⁶ CALPIRG, *supra* note 16 at 8.

Once a person's name has been entered into crime databases used by law enforcement agencies, it can be very hard to get it removed. It is certainly the case in the U.S.¹⁰⁷ The problem is so common in California that the state has an identity theft victims registry which police can use to verify if a person claiming "you have the wrong person" is indeed an identity theft victim. In a similar vein, the state of Virginia now issues Identity Theft Passports to victims.¹⁰⁸

4.13. Mortgage Fraud

An unusual and disturbing form of identity theft involves homes and mortgages. There are increasing incidences of mortgage fraudsters taking over homeowners' names in order to sell their houses or take out mortgages in their names. In the U.S., mortgage fraud grew five-fold between 2001 and 2004, from 4000 to 17,000 cases.¹⁰⁹ In Canada, mortgage fraud is estimated to cost up to \$1.5 million annually.¹¹⁰

Generally, mortgage fraud occurs when fraudulent information, such as false employment records, is provided to a lender in order to obtain a mortgage. Title fraud, another variant of real estate fraud, involves an individual falsely assuming the identity of another property owner. This false identity is then used by the criminal to assume the title or sell or obtain other mortgages based on that property, using the identity of the true owner.¹¹¹

In Canada, a criminal registered a lien against a property in connection with a purported debt. He then forged the owner's signature on a document offering the home for sale as payment of the debt. The owner learned this when a "For Sale" sign appeared on his lawn. The criminal was charged with fraud and was ordered to pay restitution. It took considerable time and money for the owner to regain title to his home.¹¹²

Fraud also occurs when thieves file transfer of ownership papers, counting on the land titles office not to cross-reference the signature. The properties of an Ontario resident were sold in this manner. The perpetrators were found to have identity documents bearing the name, date of birth and SIN of the owner, but with a different photograph. They were charged with stealing identity to acquire mortgage money, but the evidence was considered to be insufficient to prove that the thieves had been acting fraudulently by claiming to be the owner.¹¹³

A recent law enforcement investigation uncovered an allegedly elaborate mortgage fraud scheme in British Columbia that involved obtaining mortgages using false employment

¹⁰⁷ *Sullivan, supra* note 64 at 41-42.

¹⁰⁸ *Ibid.*

¹⁰⁹ *Craats, supra* note 3 at 113.

¹¹⁰ CBC News (25 April 2006).

¹¹¹ Criminal Intelligence Service Canada, *Identity Theft* (8 August 2005), online: Criminal Intelligence Service Canada <http://www.cisc.gc.ca/annual_reports/annual_report2005/identity_theft_2005_e.htm>.

¹¹² *Craats, supra* note 3 at 109.

¹¹³ *Ibid.* at 111.

records and banking documents.¹¹⁴ In April 2006, a Surrey B.C. woman pleaded guilty to mortgage fraud after posing as the owner of a vacant lot and taking out a \$170,000 mortgage on the property. The mortgage was arranged through a mortgage broker; fortunately, a different broker identified the scam and alerted police.¹¹⁵

According to the Ottawa Police Service, drug traffickers commit identity theft and mortgage fraud to obtain properties, usually houses, which are converted into indoor marijuana growing operations (grow ops).¹¹⁶ Such grow ops have been discovered in all types of neighbourhoods.

In the 2002, about 10,000 individuals reported to the Federal Trade Commission that some kind of home loan had been taken out in their name. These loans occasioned losses of at least \$300 million. The actual number is probably higher, as some victims likely did not report it.¹¹⁷

4.14. Taking over insurance policies

The identity thief may make a change of address on the car insurance policy of a person whose personal information has been stolen. The thief will then make false claims for “pain and suffering” suffered from auto accidents.

4.15. Submitting fraudulent tax returns

A thief may submit a fraudulent income tax return using the victim’s identity. The thief will invent numbers that result in a tax refund and then collect the refund.

4.16. Filing for bankruptcy

Thieves may file for bankruptcy under a victim’s name to avoid paying debts they have incurred under the victim’s name, or to avoid eviction.¹¹⁸ When a thief files for bankruptcy, this leaves false public records. According to CALPIRG’s data, clarifying these false records is a growing problem for victims.¹¹⁹

¹¹⁴ *Criminal Intelligence Service Canada*, *supra* note 111.

¹¹⁵ Wendy McLellan, “Hot market fuels mortgage fraud” *CanWest News Service* (1 May 2006), online: canada.com <http://www.canada.com/reginaleaderpost/news/business_agriculture/story.html?id=713e4985-0e75-40f4-8bdd-9100fa3155c8>.

¹¹⁶ Thomas Legault, Meeting with fraud investigators from the Ottawa Police Service (25 September 2006) [unpublished, archived at Canadian Internet Policy and Public Interest Clinic].

¹¹⁷ *Sullivan*, *supra* note 64 at 54.

¹¹⁸ University of Oklahoma Police Department, *Identity Theft - Part 1 - Introduction to Identity Theft - The Police Notebook*, online: The University of Oklahoma <<http://www.ou.edu/oupd/idtheft.htm>>.

¹¹⁹ *CALPIRG*, *supra* note 16 at 8.

4.17. Selling stolen goods

Identity thieves can obtain personal information of the owner of a vehicle of the same model as the one they have stolen. They can then obtain replacement vehicle registration documents. Using the replacement documents they can sell the stolen vehicle to unsuspecting victims. This particular situation has occurred in Australia.¹²⁰

5. DETECTING IDENTITY THEFT

Theft of personal information is often very hard to detect and there may be a significant lag time between the theft and detection. The theft will usually not be detected until the victim discovers unauthorized activity in accounts, is contacted by a financial institution or debt collectors, or is denied credit.

Individuals might not be able to do much to prevent identity theft from happening to them, but they can play a significant role in its early detection and mitigation of its consequences, on both themselves and with respect to other stakeholders, such as credit card issuers and banks. The CIPPIC website contains a number of Frequently Asked Questions about identity theft, which provides guidance to individuals for preventing, detecting and mitigating the effects of identity theft.

5.1. Canada

According to an October 2005 Ipsos-Reid poll, many Canadians have discovered that they had been victimized by using self-detection methods. It also seems that account monitoring conducted by banks and credit card issuers is beneficial in the detection of identity theft crimes. The results of the survey are shown graphically in Figure 5.1.¹²¹

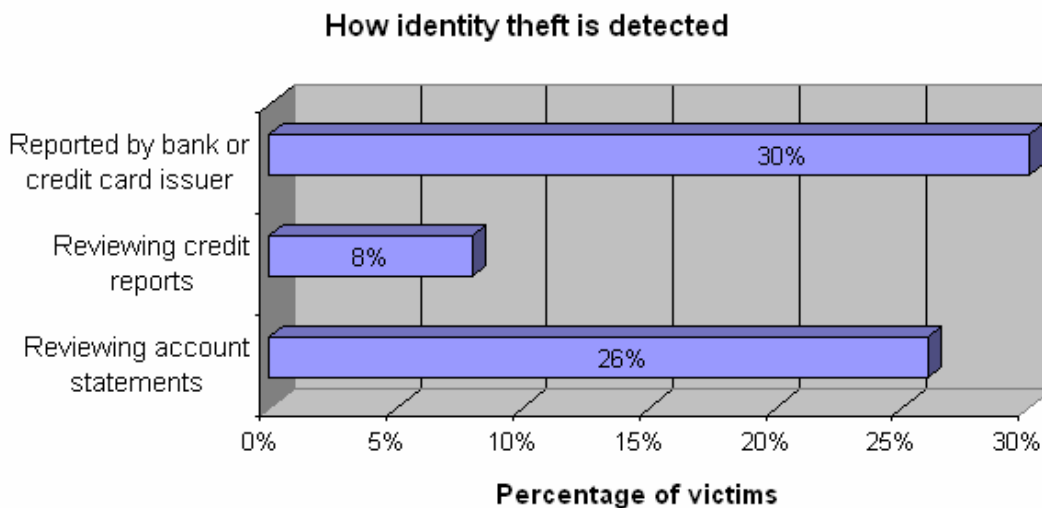


Figure 5.1 - How identity theft is detected in Canada

¹²⁰ Government of South Australia, Office of Consumer and Business Affairs, *Case Studies* (13 June 2006), online: Government of South Australia, Office of Consumer and Business Affairs <<http://www.ocba.sa.gov.au/consumeradvice/protection/idtheft/studies.html>>.

¹²¹ Ipsos-Reid, *Concern over Identity Theft on the Rise* (16 October 2005).

5.2. United-States

In a 2006 survey conducted by the Better Business Bureau shows that American victims seem to have better success in detecting identity theft than Canadian victims, though the percentages are quite low in the U.S. also. Only about 47% of victims could identify the source of the compromise of their personal information and only 36% could identify the person who misused their information.¹²²

The 2005 Javelin Identity Fraud Survey Report found that 47% of victims found out they had been victimized by using self-detection methods, such as the monitoring of statements and credit reports.¹²³ In 2005, 44% of these self-detections occurred through the monitoring of electronic or paper statements.¹²⁴

Another finding was the effect of early detection by the victim. Self detection, particularly using electronic statements, has three main advantages: 1) early detection; 2) smaller fraud amounts; and 3) smaller cost to the individual. Presumably, early detection also reduces the time it takes for victims to repair the damage done to their reputation and credit history.

It took an average of 67 days to detect the crime when victims detected it versus 101 days when someone else detected it.¹²⁵ The Javelin survey also found that self-detection resulted in lower fraud amounts (\$4,431 vs. \$8,466) and reduced costs for individuals (\$347 vs. \$538). It showed that, on average, those who detected the crime using electronic means suffered a fraud of \$550 versus a loss of \$4,500 for those monitoring paper statements.¹²⁶

6. CONCLUSION

Criminals use various techniques to acquire and use personal information. The acquisition techniques used reflect their level of expertise and commitment. The techniques used also vary depending on their motive, which is usually either financial gain or concealment.

The techniques used by identity thieves cover a wide spectrum of sophistication. Some of them are elaborate schemes, conducted online, which require specialized knowledge of the inner workings of the internet. Some techniques involve tricking unsuspecting and trusting information custodians into releasing personal information. At the other end of

¹²² Better Business Bureau, "New Research Shows Identity Fraud Growth Is Contained and Consumers Have More Control Than They Think" (31 January 2006), online: Better Business Bureau <<http://www.bbb.org/alerts/article.asp?ID=651>>.

¹²³ BBBOOnline, Special Report - BBB/Javelin Strategy 2005 Identity Fraud Survey (January 2005) vol.5 no. 1, online: BBBOOnline <<http://www.bbbonline.org/update/issue.asp?ID=48>>.

¹²⁴ *Ibid.*

¹²⁵ *Ibid.*

¹²⁶ *Ibid.*

the spectrum, identity theft can be as simple as sifting through an organization's or an individual's trash to find discarded documents containing valuable personal information.

An important aspect of identity theft techniques is that they almost always provide anonymity to the thief. That is one of the main reasons why the crime is so popular and often so rewarding to the perpetrator.

Identity thieves are always discovering new techniques.. In the future, as it gets tougher to commit fraud in the classic sense, we can expect to see a migration towards new forms of computerized identity theft. Identity thieves have been quick to realize the benefits of operating in this fashion. This creates further exposure for individuals and a real challenge for law enforcement officials and legislators.

APPENDIX A – EXAMPLES OF PHISHING EMAILS

To: "John Doe"
From: <support@visa.com>
Subject: VISA Billing Dept team
Date: Sun, 06 Nov 2005 21:00:29 -0700


Dear Visa Cardholder.

It has come to our attention that your Visa billing information records are out of date. This requires an update of your billing information. Please take several minutes out of your online experience and update your billing records. You will not run into future problems with our services. Please update your records carefully.

Please click here to update your billing records

Thank you for your time and we appreciate your business.

VISA Billing Dept team.



Visa phishing e-mail¹²⁷

¹²⁷ CBC Marketplace, "What is 'phishing'?", online: CBC.CA
<<http://www.cbc.ca/consumers/market/files/scams/phishing/phishingdefined.html>>.

To: "John Doe"
From: security@scotiabank.com
Subject: Secure Server Update
Date: Sun, 06 Nov 2005 14:54:07 -0700

The simplicity of one mutual fund...

Dear Valued Customer,

- Our new security system will help you to avoid frequently fraud transactions and to keep your investments in safety.
- Due to technical update we recommend you to reactivate your account.

Click on the link below to login and begin using your updated scotiabank account.

To log into your account, please visit the scotiabank website at <http://www.scotiabank.com>

To review your statement, log into your scotiabank account and click the eStatements & eNotices button in the left navigation of your Account Summary page.

Your new statement is listed in the left navigation of the page.

If you have questions about your online statement, please send us a Bank Mail or call us at 1300 651 656, International dial +61-3-8641-9886, 8:00am - 12:00am (EST), 7 days a week.

We appreciate your business. It's truly our pleasure to serve you.

Sincerely,
 Scotiabank Customer Care

This email is for notification only. To contact us, please log into your account and send a Bank Mail.

Scotiabank phishing email¹²⁸

Step by step phishing

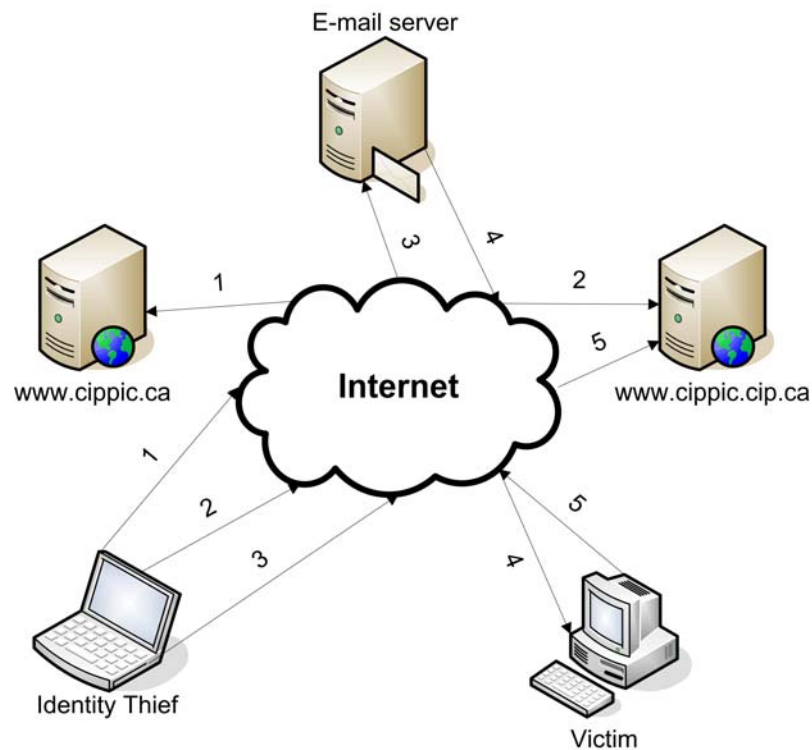
The identity thief downloads a copy of the organization's site;

1. The identity thief registers a domain name very similar to the one being spoofed and sets up a fake website using the copy acquired in step 1. The site will be modified to add a section where the users can enter the requested information;

¹²⁸ CBC Marketplace, "Sc@mmed: Inside the world of online identity theft" (6 November 2005), online: CBC.CA <http://www.cbc.ca/consumers/market/files/scams/phishing/quiz/example_scotiabank.html>.

2. The identity thief sends an e-mail to the potential victims;
3. The e-mail is sent to the victim;
4. The victim follows the link provided in the fake e-mail and accesses the spoofed website to provide the information;
5. Using the information, the identity thief accesses the victim's bank accounts and transfers money to a mule's account or unlawfully uses the victim's personal information.

Steps 4 to 6 are repeated for each victim.

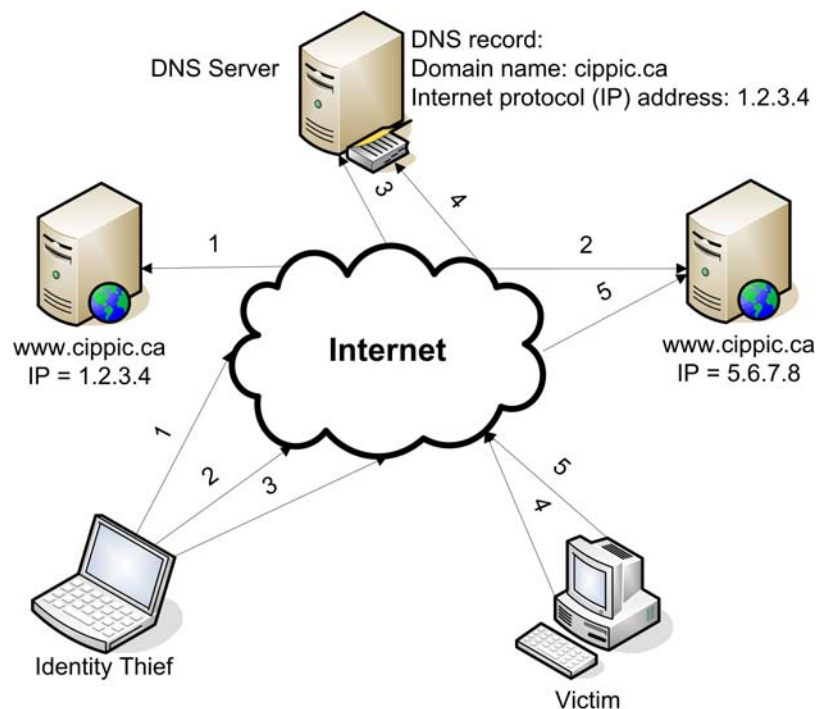


APPENDIX B - PHARMING

The following figure illustrates the different steps involved in establishing a pharming scam using DNS poisoning.

1. The identity thief downloads a copy of the organization's site;
2. The identity thief obtains an internet protocol (IP) address and sets up a fake website using the copy acquired in step 1. The site will be modified to add a section where the users can enter the requested information;
3. The identity thief poisons the DNS record by modifying the IP address associated with the targeted domain name. In this example, the IP address for the cippic.ca domain name is changed from 1.2.3.4 to 5.6.7.8;
4. The victim enters www.cippic.ca in his browser. The browser will contact the DNS server to get the IP address associated with the cippic.ca domain name;
5. The victim is transparently sent to the fake website with the IP 5.6.7.8. The address appearing in the browser window will be exactly the one entered, i.e. www.cippic.ca.

Steps 4 and 5 are repeated for each victim.



APPENDIX C– GLOSSARY OF TERMS

Term	Definition
personal identification number (PIN)	A number usually composed of three or more digits which is required to complete transactions using a debit or calling card.
Spoofing	<p>The act of portraying a fake electronic communication as an official communication. Spoofing will usually consist of replicating the visual aspect and “tone” of official electronic communications. Spoofing can occur in all sorts of electronic communications.</p> <p>Spoofed emails For example, in emails, the originating address will usually be faked to make the email look like it comes from an official source.</p> <p>Spoofed websites An identity thief could setup a website with the domain name www.td-server.ca and make a copy of the TD Canada Trust website, which is normally found at www.tdcanadatrust.com. The distinction between both sites is virtually impossible to distinguish. The only apparent difference is the websites address displayed in the browser.</p> <p>Spoofed instant messages Spoofing can also occur in instant messaging or other chat rooms. A thief would masquerade as an agent of the service provider.</p>
domain name	A textual identifier (such as xyz.com) used to resolve the numerical address of a specific website.
social engineering	<p>Social engineering involves exploiting the natural tendency of a person to trust others, especially people with whom they have some sort of relationship. This trust can be exploited by identity thieves, using a variety of techniques, to acquire personal information.</p> <p>It is generally agreed upon that “users are the weak link” in security and this principle is what makes social engineering possible.</p>
WHOIS database	WHOIS is a TCP-based query/response protocol which is widely used for querying a database in order to determine

Term	Definition
	the owner of a domain name, an IP address, or an autonomous system number on the internet.
DNS Server	DNS servers are the machines responsible for resolving internet domain names into their real addresses — the "signposts" of the internet.
spyware	In the field of computing, the term spyware refers to a broad category of malicious software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party. See also "Malware".
SIN	The Social Insurance Number (SIN) is a nine-digit number used in the administration of various Canadian government programs. It's required to work in Canada or to receive government benefits.
Trojan Horse application	In the context of computer software, a Trojan horse is a malicious program that is disguised as legitimate software. The term is derived from the classical myth of the Trojan Horse. They may look useful or interesting (or at the very least harmless) to an unsuspecting user, but are actually harmful when executed. They are programs that masquerade as something else, like a game or image file, in order to trick the user into some misdirected complicity that is needed to carry out the program's objectives. Trojan Horse programs cannot operate autonomously, in contrast to some other types of malware, like viruses or worms.
malware	Malware is software designed to infiltrate or damage a computer system, without the owner's consent. See also "Spyware".
shoulder surfing	Shoulder surfing can be accomplished in two ways, either by standing in a particular position where it is possible to see someone enter their PIN number in a terminal or by placing a camera in such a position.
cracker	A cracker is a malicious or criminal hacker.
hacker	Hackers are able to exploit systems and/or gain unauthorized access through skills, tactics and detailed knowledge.
backdoor	A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication or securing remote access to a computer, while attempting

Term	Definition
	to remain hidden from casual inspection. The backdoor may take the form of an installed program (e.g., Back Orifice) or could be a modification to a legitimate program.
spam	Spam is also known as unsolicited commercial email. Most spam is a form of commercial advertising, which is economically viable because email is a very cost-effective medium for the sender.
hosts file	In computing, a hosts file, stored on the computer's file system , is used to look up the internet protocol address of a device connected to a computer network , such as a home computer connected to the Internet. The hosts file describes a many-to-one mapping of device names to IP addresses . When accessing a device by name, the networking system will attempt to locate the name within the hosts file if it exists. Typically, this is used as a first means of locating the address of a system, before accessing the internet domain name system .