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

IDENTITY THEFT: INTRODUCTION AND BACKGROUND

March, 2007

CIPPIC Working Paper No. 1 (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), "Identity Theft: Introduction and Background", CIPPIC Working Paper No.1 (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 Working Paper provides background information on the history, characteristics, causes and extent of identity theft. It discusses the challenges of defining the term "identity theft" and of measuring its size and impacts. It identifies key stakeholders and analyzes the impact of technology, including the widespread use of the internet, on identity theft.

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

INTRODUCTION

Twenty years ago, the term "identity theft" was little used and little known. Today, it is a widely recognized term, one associated with a phenomenon that has captured public, media and government attention and which has become a serious social issue. Often described in alarming terms – "the crime of the new millennium",[1] the "nightmare of identity theft"[2], the "quintessential crime of the information age"[3], identity theft has become one of the most prevalent types of white collar crime. Its impacts can be financially devastating and personally traumatic, its effects long lasting. These can extend not only to individual victims, but also to governments, businesses and society in general.

TERMINOLOGY

What exactly is identity theft? Is it possible to develop an accurate and commonly applicable definition? At first glance, this would seem to be a relatively easy task. In reality, the challenge is formidable. One author has described this problem in the following way:

> Confusion about (the definition of) identity theft is growing at a faster rate than the actual incidence of the crime, clouding the true causes and consequences to individuals and enterprises.[4]

The list of definitions in Appendix A illustrates this point. Although they share many similar features, none of these definitions are identical.

Identity theft occurs when the personal identifying information of an individual is misappropriated and used in order to gain some advantage, usually financial, by deception.[5] It can take many forms.

At one end of the spectrum is fraudulent use of another person's account information (e.g., credit card number) in order to make unauthorized financial transactions, without any additional attempts to impersonate that other person. Such fraud has been addressed with varying degrees of effectiveness by legislators and the private sector. These types of activities are classified by the financial industry as payment card fraud, rather than identity theft. However, they tend to be regarded in the public eye as identity theft (a phenomenon that has been called "definition creep").[6]

---

[1] Sean B. Hoar, "Identity Theft: The Crime of the New Millennium" (2001) 80 Oregon L at 1423.
[2] Joe Vanden Plas, "Managing the nightmare of identity theft", Wisconsin Technology Network (5 September 2006) at 1, online: <http://wistechnology.com/article.php?id=2942>.
[3] Charles M. Kahn & William Roberds, "Credit and Identity Theft" (August 2005) Federal Review Bank of Atlanta Working Paper Series, Working Paper 2005-19 at 1.
[4] Lombardi, Rosie, Myths about identity theft debunked by experts, IT World Canada (22 March 2006).
[5] B.C. Freedom of Information and Privacy Association, *PIPEDA and Identity Theft: Solutions for Protecting Canadians*, (30 April 2005) at 6.
[6] *Lombardi*, *supra* note 4.

It can be difficult to distinguish between ordinary fraud and that which is truly "identity theft". In the case of true "identity theft", the thief misappropriates information relating to the identity of a person - information such as name, address, telephone number, date of birth, mother's maiden name, Social Insurance Number (SIN), driver's licence number, or health card number and then masquerades as the victim, effectively taking over their identity.

The thief may then go on to conduct financial transactions in the name of the often unsuspecting victim, including opening bank, utility and cell phone accounts, securing credit cards, obtaining benefits, securing employment, committing crimes or even beginning a new life, often in other countries.[7] In some instances, blackmail, terrorism, money laundering, people smuggling, immigration scams or drug related crimes may be committed, or the stolen identity may be used by known criminals to hide from law enforcement agencies. The victim's email account may be used to send threatening or defamatory messages. This is different from simply using personal account information, such as a credit card number, to make unauthorized transactions.[8]

A useful definitional model of identity theft has been proposed by Sproule and Archer.[9] Identity theft encompasses the collection of personal information and the development of false identities. Identity fraud refers to the use of a false identity to commit fraud.

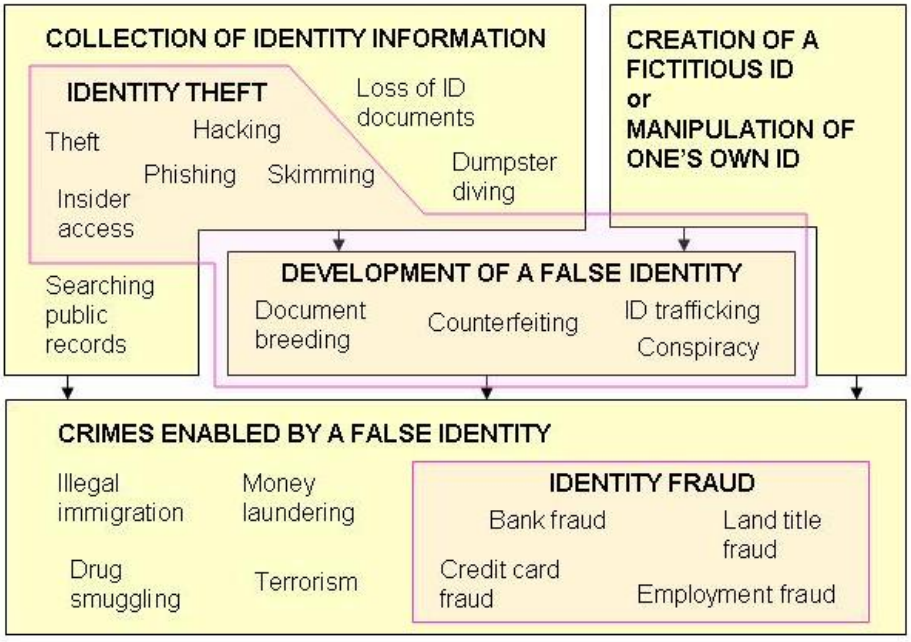

Figure 1 - Definitional Model of Identity Theft

[7] Wenjie Wang, Yufei Yuan & Norm Archer "A Contextual Framework for Combating Identity Theft" (March/April 2006) IEEE Security & Privacy at 25.
[8] *Lombardi, supra* note 4.
[9] Susan Sproule and Norm Archer, *Defining and Measuring Identity Theft*, presentation to the second Ontario Research Network in Electronic Commerce (ORNEC) Identity Theft Workshop, (Ottawa, 13 October 2006).

Drawing from this model, and for the purposes these Working Papers, identity theft is defined as a process involving two stages: 1) the unauthorized collection of personal information; and 2) the fraudulent use of that personal information to gain advantage at the expense of the individual to which the information belongs:

1) *Unauthorized Collection*: Identity theft starts with the misappropriation of a living or dead individual's personal information, without consent and often without knowledge, or by theft, fraud or deception. The information can be used immediately, stored for later use or transmitted for use by someone else.

2) *Fraudulent Use*: Identity theft continues with the fraudulent use of the personal information, typically for economic gain. The perpetrator impersonates the victim in order to obtain credit or other benefits in their name. A hallmark of identity theft is repeat victimization - the thief will usually engage in a series of fraudulent uses.[10]

We use the term "identity theft" to cover both the initial unauthorized collection of personal information, and the later fraudulent use of that information.

THE SIGNIFICANCE OF IDENTITY THEFT

Why has identity theft become such a gripping issue, compared with other types of crime? Any form of crime has negative financial and other consequences for its victims, but those associated with identity theft can be particularly hard hitting. Someone's identity is unique and highly personal. To have one's identity information misappropriated by another is a privacy violation of the highest order, akin to and even more invasive than the theft of personal property resulting from a home break-in.

The financial cost of identity theft may be significant. Using the misappropriated personal information of an individual, a thief can make financial transactions as that person, emptying bank accounts, making purchases and racking up debts. It may be some time before the victim realizes what has happened.

However, the effects of identity theft may go far beyond financial loss. Victims of traditional theft can usually replace their possessions, but a victim of identity theft may suffer loss of reputation and standing in the community, as well as damage to their credit rating.[11] It may take considerable time and expense to resolve the resulting problems. At worst, the effects of identity theft may linger, haunting victims indefinitely. Long after the event, they may find themselves denied credit, or even arrested for crimes committed by the identity thief.

---

[10] U.S. Department of Justice, *Identity Theft, Problem-Oriented Guides for Police*, Problem-Specific Guides Series, No. 25 (June 2004) at 1, online: http://www.cops.usdoj.gov/mime/open.pdf?Item=1271.

[11] Bill Diedrich, "Chapter 254: Closing the Loopholes on Identity Theft, But at What Cost?" (2005) 34 McGeorge Law Review at 383.

Identity theft is not just a problem in its own right. It also has ramifications for other types of crime. United States and Canadian law enforcement agencies report a growing trend in both countries toward greater use of identity theft as a means of furthering or facilitating other forms of fraud, organized crime (the bulk of identity crime is committed by organized crime) and terrorism.[12] Especially troubling is the now established link between identity theft and national security.

Although rates of identity theft are levelling off, a significant percentage of Canadians feel threatened. A poll conducted in February, 2006 found that 71% of Canadians are very or somewhat concerned about becoming a victim of identity theft in the future. It also found that 4% of Canadians have personally been subject to identity theft and 20% know someone who has been affected. The number of victims increases to 8% when looking only at credit card holders.[13]

Governments in Canada, the U.S. and in other countries have taken action to combat what has become a crime of international dimensions. Public awareness and victim assistance programs have grown. In spite of new laws, policies and practices, however, identity theft continues to challenge the best efforts of governments, law enforcement, the corporate sector and individual citizens.

HOW BIG IS THE PROBLEM?

Until the last few years, occurrences of identity theft were on the rise. Recently, the rate of increase started to level off, in both Canada and the U.S.

In Canada, Equifax and TransUnion (the two largest Canadian credit bureaus), receive approximately 1400 to 1800 complaints of identity theft per month.[14] PhoneBusters, an organization which studies and reports on identity theft, collects data, educates the public, and assists both Canadian and U.S. law enforcement agencies, reported about 11,000 complaints in 2005 (compared with approximately 8,000 in 2002), at a cost of $8.6 million (compared to $11.7 million in 2002).[15] About one third related to credit cards, including false applications, and 10-12 % related to cell phones.[16] In the first ten months of 2006, 6,483 victims reported to Phonebusters, a lower rate than for 2005. However, the

---

[12] Canada, Department of the Solicitor General and U.S. Department of Justice, *Public Advisory: Special Report for Consumers on Identity Theft* (2003). For example, a recent investigation into a case of identity theft uncovered a major drug operation. The drug traffickers had committed identity theft to rent space within which they operated a clandestine drug lab.

[13] Ipsos-Reid, One-Quarter of Canadian Adults (24%) Have Been Touched by Identity Theft (7 March 2006) at 1 - 3.

[14] PIPEDA and Identity Theft, *supra* note 5 at 10.

[15] Phonebusters, *Identity Theft Complaints*, online: <http://www.phonebusters.com/english/statistics_E03.html>.

[16] *PIPEDA and Identity Theft*, *supra* note 5 at 7.

value of losses reported for this period was $14,735,882, a higher figure than in previous years.[17]

The following table illustrates the statistics on the number of Canadian victims and their losses for the year 2005.

Table 1: 2005 identity Theft Statistics (Canada)

2005		
Province	**Victims**	**$ Loss**
Ontario	4729	$4,450,122.62
Quebec	2614	$1,864,574.23
British-Columbia	2010	$1,376,499.08
Alberta	894	$431,221.89
Manitoba	361	$181,490.32
Nova Scotia	177	$100,036.04
Saskatchewan	157	$87,641.63
New-Brunswick	127	$29,107.52
Unknown	82	$4,350.00
Newfoundland and Labrador	58	$43,358.02
Prince-Edward-Island	18	$5,907.63
Yukon	3	$1,285.00
Northwest Territories	1	$0
Total	**11231**	**$8,575,593.98**

Table 1 - Number of victims in Canada (2005)[18]

Identity theft has been called the "fastest-growing crime in the United States", with approximately nine million victims annually.[19] It has topped the U.S. Federal Trade Commission's (FTC) list of consumer complaints for the last five years. In 2004, the FTC received 246,847 complaints of identity theft, up 52 per cent from 2002. In 2005, 255,565 complaints were received, a modest increase. The FTC currently stores about 815,000 complaints.[20]

[17] Phonebusters, *Monthly Summary Report*, (October 2006), online: <http://www.phonebusters.com>.
[18] PhoneBusters, *Identity Theft Complaints,* online: <http://www.phonebusters.com/english/statistics_E05.html>.
[19] State of California, *Locking up the Evil Twin: a Summit on Identity Theft Solutions*, (1 March 2005) at 1.
[20] U.S. Federal Trade Commission, online: <http://www.ftc.gov>.

In the five years since it was established by the FBI and the National White Collar Crime Center, the Internet Crime Complaint Center (formerly the Internet Fraud Complaint Center) has received more than 100,000 complaints related to identity theft. In 2004, it averaged more than 17,000 consumer complaints monthly.[21]

In January 2006, national researchers noted a levelling off of nationwide victim statistics. However, as in Canada, financial losses have grown, to nearly $US57 billion in 2005, indicating a higher per-crime incidence.[22]

According to the FTC, the most common abuses of stolen personal information occur with credit card, phone or other utility accounts. In 2003, these abuses accounted for 54% of the 214,905 incidents reported. Credit card fraud (33% of all fraud) was the most common form of reported identity theft that year, phone or utility constituted 21%, bank fraud 17% and employment fraud 11%.[23]

What do these statistics mean? How much reliance can be placed on them, given that there is no standard definition of identity theft? There can be no question that statistics are skewed. On the one hand, research has suggested that only about 25 % of victims report the crime to the police or to major credit agencies.[24] Conversely, individuals may consider themselves as victims of identity theft, and report as such to authorities, when in fact they are victims of one-time, "everyday" theft or fraud. This creates real problems for developing accurate and reliable statistics, and for understanding and dealing with the problem.

These methodological challenges are further complicated by the fact that there is generally a lag time between the theft of identifying information and the detection of damage. Many victims discover that their identity information has been stolen only when they apply for credit or try to get a mortgage, notice withdrawals from their bank accounts, or receive bills for goods and services that they did not purchase themselves.[25] On average, there is a one year delay in discovering that identity theft has occurred.[26] This means that occurrences may be reported only some time after the event. It also makes it more difficult to reduce losses and catch and prosecute criminals.

OBJECTIVES OF THE WORKING PAPERS

We need to better understand the nature and impacts of this crime. How can identity theft be prevented and detected? What measures can be taken to assist victims and catch and prosecute criminals?

---

[21] *Ibid.*
[22] State of California, *Teaming up Against Identity Theft*, (23 February 2006) at 4.
[23] *Locking up the Evil Twin*, *supra* note 19 at 25.
[24] *PIPEDA and Identity Theft*, *supra* note 5 at 10.
[25] *Police Guide*, *supra* note 10 at 5 and 9.
[26] Federal Trade Commission, *National and State Trends in Fraud & Identity Theft January - December 2003*, (22 January 2004), online: <http://www.consumer.gov/sentinel/pubs/Top10Fraud2003.pdf>.

With these questions in mind, this series of Working Papers looks at two dimensions of identity theft: law and policy. An effective legal framework, supplemented by well crafted policies and practices, are essential parts of the effort to tackle identity theft. How well is Canada doing in this regard? How do we compare with the U.S. and other countries? To date, it appears that no comprehensive survey of Canadian laws and policies, one which compares and contrasts the situation here with the U.S. experience, has been undertaken. The objective of this series of Working Papers is to help to fill this void.

This first Working Paper provides a foundation for an inventory and analysis of the legal and policy dimensions of identity theft in Canada. The other papers build on this framework, each exploring a different aspect of the problem: identity theft techniques; existing and proposed laws; court decisions and law enforcement and government and corporate sector policies aimed at preventing identity theft. A separate White Paper on "Approaches to Security Breach Notification", released in January 2007, addresses the related issue of data security breaches.

The focus of this paper is on the situation in Canada. However, much of the information and analysis includes consideration of the U.S. scene. This is in part because, while the size of the problem is much greater in the U.S., there are many similarities with Canada in terms of the nature and impacts of identity theft. There is also a wealth of information, from media reports, government documents and surveys, and academic literature, on identity theft that was compiled in U.S. but which reflects, to varying degrees, the situation in Canada. Third, there has been considerably more activity on the legislative front in the U.S., where the federal and state governments have been seized by the issue of identity theft and have taken measures to combat it.

One underlying premise is that Canada can learn from the experiences of the U.S., and to a lesser degree, from other countries such as the United Kingdom, Australia and France. It is in our interest to see how others have, for better or worse, tackled the problem.

IDENTITY THEFT STAKEHOLDERS

While conducting research on identity theft, it is imperative to keep in mind the main stakeholders affected by this type of crime. When identity theft crimes are committed, all the stakeholders identified below are usually involved in some way. The terminology used reflects the model developed by Wang et al.[27]

[27] *Wang, supra* note 7.

Individuals

Individuals are also known as identity owners.[28] They have the legal right to own and use their identity. They also have the right to obtain identity certificates such as birth certificates, passports, driver's licence and health cards.

They are the victims of identity theft who ultimately carry the burden. As noted, identity theft can be a traumatic experience. Victims suffer financial losses, a loss of reputation, emotional distress, and the often-difficult task of rebuilding their credit rating.[29]

While there are steps individuals can take to protect themselves, the Ontario Privacy Commissioner has noted that consumers are not in the best position to reduce identity theft.[30] In reality, many consumers are not aware of the collection, use and disclosure of their personal information.[31] In these circumstances, it is extremely difficult for them to reduce the risk posed by identity theft.

Governments

Governments play three roles in the context of identity theft. When individuals apply for identity certificates, governments play the role of identity certificate issuers.[32] By using appropriate authentication mechanisms when citizens apply for identity certificates, governments play the role of identity information protectors.[33] When individuals apply for benefits offered by the different governmental programs, governments play the role of identity verifiers, ensuring that the individual is who they say they are.[34]

Businesses and organizations

Banks, credit card issuers, loan companies, credit bureaus and transaction processing firms, when providing financial services such as new accounts, loans and mortgages, play the role of identity checkers. When they provide goods or services or grant credit without conducting an appropriate screening of the individual, businesses may facilitate identity theft. In some instances of identity theft, the perpetrator is an employee of the business that collected the information.

---

[28] *Ibid.* at 26.
[29] Consumer Measures Committee, *Working Together to Prevent Identity Theft*, (6 July 2005) at 2, online: <http://cmcweb.ca/epic/internet/incmccmc.nsf/vwapj/Consultation%20Workbook_IDTheft.pdf/$FILE/Consultation%20Workbook_IDTheft.pdf>.
[30] Information and Privacy Commissioner of Ontario, *Identity Theft Revisited: Security is Not Enough* (September 2005) at 4, online: <http://www.ipc.on.ca/docs/idtheft-revisit.pdf>.
[31] Public Interest Advocacy Centre, *Identity Theft: The Need For Better Consumer Protection* (November 2003) at 30, online: <http://www.piac.ca/files/idtheft.pdf>.
[32] *Wang*, *supra* note 7 at 27.
[33] *Ibid.*
[34] *Ibid.*

Businesses, as well as governments, that collect, hold or transfer personal information, may be subject to security breaches, either internal or external. This is a particular problem for large data storage businesses.

Businesses have a prevention role to play, as identity information protectors. They can fulfill this role by notifying their customers or clients about security breaches and about the risks of identity theft and by offering certain protection packages, such as account monitoring.

Law Enforcement Agencies

Wang has identified law enforcement agencies as also playing a role of identity information protectors.[35] However, because most investigations occur after identity theft has been committed, and because prosecution rates for these offences seem low, law enforcement agencies are better described as "identity information restorers", with police reports and affidavits being used to restore a victim's credit record and reputation. In certain situations, such as when law enforcement officials arrest an individual, they play the role of identity verifiers.

CHARACTERISTICS AND UNDERLYING CAUSES OF IDENTITY THEFT

In some respects, identity theft is not a new phenomenon. For hundreds of years, people have claimed to be someone they are not. They have done this for financial gain, to avoid responsibility for a misdeed, or to gain in social status or an employment position.[36] Perhaps the most notorious example is that of Frank Abagnale Jr., who for five years in the 1960s assumed a series of false identities, backed up by false identification. Abagnale defrauded banks, airlines, hotels and other businesses in 26 countries, for an estimated total of more than $2.5 million.[37]

Although Abagnale apparently created fictitious identities, rather than relying on stolen personal information from real people, his reliance on fake identity documents, forged cheques and social engineering techniques to swindle banks, airlines and other organizations was similar to the *modus operandi* of modern identity thieves. Everyday document fraud, cheque swindling and forgery - all components of today's identity theft phenomenon - have been techniques of choice for criminals for years. Today, however, these crimes have become more complex, often involving many individuals, sophisticated techniques and interjurisdictional activity.

There is often a network of criminals involved with identity theft. Information obtained by one set of criminals may be sold to another operative. For example, online "carder networks" buy and sell stolen personal and financial information, such as personal information obtained electronically or from illegally-made copies of credit or debit cards.

---

[35] *Ibid.*
[36] Craats, Rennay, *Identity Theft: the scary new crime that targets all of us*, (Toronto: Altitude Publishing, October 2005) at 136.
[37] *Ibid.* at 139.

This makes the task of stopping identity theft that much more difficult. Terrorists also use identity theft as a means of achieving their objectives.

It is not just career criminals who are to blame. Insider theft, by corrupt employees with access to personal files, is a major source of identity theft. About nine percent of identity theft cases are carried out by family members.[38] Friends, neighbours and colleagues may also be involved. In some respects, this "friendly fraud" is a more troublesome and perplexing type of identity theft, in terms of the emotional impact on the victim. It is one thing to have one's identity stolen by an unknown thief, but when the perpetrator is a family member or another who is known to the victim, it is especially distressing.

Why has identity theft become a crime of choice for criminals? One reason is that it offers thieves the possibility of a very high return combined with a very low risk of getting caught.[39] Few individuals are ever charged with and convicted of identity theft-related crimes.[40] Newman and McNally have noted that identity theft has three main attractions for criminals: 1) anticipated rewards; 2) the advantage of concealment which is intrinsic to the crime[41]; and 3) mild sentences compared with other crimes.[42]

A second key contributing factor to the growth of this crime is the ready access to personal information of individuals, from a variety of sources. Governments, hospitals, credit card companies, cell phone providers and other corporate entities regularly collect and store this information, sometimes without the knowledge and consent of the individuals concerned and not always with appropriate safeguards. Security breaches, especially from large data brokers, are a serious concern, and organizations may fail to notify affected individuals or cooperate with law enforcement agencies to limit the consequent damage.[43]

The North American practice of relying on an identifying number, such as a Social Insurance Number (SIN) or, in the U.S.A., a Social Security Number (SSN) other than for their intended purposes, has facilitated identity theft. These numbers, readily available from payroll accounts and internet sites, are often used to authenticate persons on systems and by credit bureaus to confirm matches when a credit report is requested. This is especially true in the U.S., where SSNs, described as "keys to the kingdom", are used as an identifier, more widely than in Canada.[44] It helps to explain why identity theft is more prevalent in the U.S.

---

[38] *Craats*, *supra* note 36 at 107.
[39] *Ibid.* at 29.
[40] *Ibid.*
[41] Graeme R. Newman & Megan M. McNally, *Identity Theft Literature Review, July 2005* at 46: online http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf.
[42] *Ibid.* at 26.
[43] See, for example, Canadian Internet Policy and Public Interest Clinic (CIPPIC),"Approaches to Security Breach Notification: A White Paper" (9 January, 2007), online: <http://www.cippic.ca/en/bulletin/BreachNotification_9jan07-print.pdf>.
[44] *Canadian Internet Policy and Public Interest Clinic (CIPPIC), Ibid.*

An associated problem is the frequent reliance on "non-identity" documents, such as driver's licences, health cards and birth certificates, by banks and other financial organizations, to authenticate identity. None of these documents is a formal government identification card – a driver's licence is a licence to drive, a health card is issued to provide access to health services and a birth certificate is proof of birth – and all can be forged, may be stolen during delivery and, in the case of driver's licences, are relatively easy for identity thieves to obtain.

Easy access to credit, such as through unsolicited, "pre-approved' cards, and to credit reports, combined with flawed authentication procedures, provides real opportunities for identity thieves.

Practices and omissions of individuals themselves make them vulnerable. The majority of identity theft incidents arise out of "the simple and mundane activities that are part of daily life."[45] Examples include the failure to protect passwords, loss of purses and wallets, ready disclosure of personal information online and to retailers, careless disposal of personal information documents, and so forth.

However, advances in modern technology, especially the widespread use of the internet, have also facilitated the ability of thieves to steal personal information, while also hiding their own identities. This is discussed in the following section.

ADVANCES IN TECHNOLOGY: CONSEQUENCES FOR IDENTITY THEFT

Identity theft provides an excellent illustration of the fact that advances in technology can be both a blessing and a curse. The growth of the crime of identity theft has gone hand in hand with the growth of the internet and associated technology.

Fifteen to twenty years ago, identity theft occurred for the most part as the result of the theft of physical documents, such as mail or hard copy files, containing key information such as credit card receipts, bank statements or government documents. Compared to today, identity theft took place on a smaller scale, required more time and effort to complete and involved smaller losses.[46] Although most identity theft is still carried out by traditional means, the use of the internet and other new technologies has led to new, faster and more widespread types of identity theft.

According to career imposter and fraud artist Frank Abagnale, ""Technology means that what I did 40 years ago is 4,000 times easier to do today."[47] US Senator Charles E. Schumer has stated that "What bank robbery was to the Depression, identity theft is to the Information Age"[48]

---

[45] Jim *Gaston & Paul K. Wing, Protecting Your Money, Privacy & Identity from Theft, Loss and Abuse* ((Toronto: The Canadian Institute of Chartered Accountants, 2003) at 11.
[46] *Craats*, *supra* note 36 at 147-148.
[47] Jeremy Scott-Joynt, "No more Mr Nice Guy?" *BBC News* (10 May 2006), online: BBC News <http://news.bbc.co.uk/2/hi/business/4758501.stm>.
[48] *Craats*, *supra* note 36 at 186.

Advances in technology have also enabled innovations in the detection and prevention of identity theft. However, this works both ways, as criminals can and do master technological advances to steal identity information and commit fraud.

As Wang et al note, "the result is a never-ending race between industry in developing new security features, and criminals, in their attempts to compromise technology and commit fraud".[49] The phenomenon is also described as an "arms race" between offenders and those trying to thwart them. System interventions and improvements in technology can work wonders for prevention (e.g., passwords for credit cards), but in little time, offenders develop techniques to overcome these defences.[50]

An official of the U.S. Federal Trade Commission's Bureau of Consumer Protection has confirmed this point, noting that: "The Commission's experience is that fraud operators are always among the first to appreciate the potential of a new technology to exploit and deceive consumers."[51]

Ultimately this type of race results in costs for businesses. Individuals are also faced with costs, usually in the form of higher prices or higher interest rates. A testimony to the cost of this race is TD Bank's upgrade of its ATM machines to accommodate new chip cards. TD evaluates this cost at $420 million.[52]

Computers

As computer technology has advanced, it has become easier to obtain information about individuals, such as their bank account, SINs and health card numbers. As noted, much personal information is now collected and stored by organizations, much of it electronically, and can be accessed by those in the know. As well, quality fake identification documents, such as driver's licences and diplomas, can be readily purchased on the internet.

Copying Equipment

Innovations such as desktop publishing equipment, colour inkjet printers and colour copiers have enabled the reproduction of most documents. Attempts are made to try to prevent the copying of currency via personal desktop publishing tools. For example, companies like Adobe and Hewlett-Packard use an online service to detect attempts to copy currencies.[53] However, these detection techniques can be countered by simple means.

---

[49] *Wang*, *supra* note 7, at 11.
[50] *Newman & McNally*, *supra* note 41 at VII.
[51] *Craats*, *supra* note 36 at 187.
[52] Vivian Moreau, Place hand here (2005), online: Ottawa Insight <http://www.carleton.ca/ottawainsight/2005/pfinance/pf10.html>.
[53] Central Bank Counterfeit Deterrence Group (CBCDG), Banknotes & Counterfeit Deterrence, online: <http://www.rulesforuse.org/pub/index.php?lang=en>.

This type of equipment, along with electronic scanners, has eliminated the need for expensive and specialized equipment and expertise to create the false documents used to perpetuate identity scams. Now, using a laser printer and graphic design software, an inexperienced identity thief can achieve equivalent results to those of hardened criminals.[54] For example, fake identity certificates, even forged digital certificates, can be created, or the images and information on stolen ones altered.

The Internet

No technological advance has carried such profound implications for identity theft as much as the internet. It is not that internet use is the main vehicle for identity theft – as noted, offline activities remain the primary medium for stealing and abusing personal information. However, the internet has made it infinitely easier for criminals to use the identities of other persons. King has noted that "the Web makes it easier for fraudsters to masquerade as the victim facelessly and anonymously".[55]

One consultant in the field has stated that: "The restless tide of e-commerce changes personal identity to a cipher. You stop being a person (and) start becoming pieces of data".[56] Previously, personal information was stored on paper and kept in file cabinets or desk drawers. During the nineties, this changed almost overnight. internet access, e-mail accounts, online shopping, electronic records storage and transmittal all became an integral part of the business world.

Fraud committed online can be distinguished in two important respects: 1) it is far more difficult for law enforcement to identify and apprehend online fraudsters; 2) these offenders can commit crime on a far broader scale than their real-world counterparts.[57]

Data Warehouses

As noted, data warehouses hold extensive dossiers of personal information, generally without the knowledge of the individuals concerned. Files are compiled from public records - court records, property tax files, registration and licensing bureaus, credit bureaus and consumer demographics. Social Security and Social Insurance numbers may also be available. Anyone able to gain access to these data banks has all the information required to steal identities, both night and day.

This is precisely what happened to the largest American data aggregator, Choicepoint, which collects, stores and sells information about most adults. In 2005, a Nigerian fraudster was able to access between 145,000 and 500,000 files, enabling him and his

[54] *Craats*, *supra* note 36 at 151.
[55] *Lombardi*, *supra* note 4.
[56] *Craats*, *supra* note 36 at 183.
[57] Mohamed Chawki and Mohamed S Abdel Wahab, "Identity Theft in Cyberspace : Issues and Solutions (Spring 2006) vol. 11, no. 1 Lex Electronica at 3, online: Lex Electronica <http://www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf>.

associates to obtain birthdates, Social Security Numbers and other vital personal information. More than 750 instances of identity theft or attempted fraud resulted from this breach.[58]

In Canada, criminals were able to obtain 1400 files from Equifax Canada, a major credit reporting company.[59] These files contained bank account numbers, credit histories and addresses.

CONCLUSIONS

It is clear that identity theft is a special type of crime and one that is particularly difficult to prevent and resolve. Its impacts go well beyond financial losses, extending to psychological and emotional distress, inconvenience and expense for the victim, and sometimes having long-term effects.

A generally accepted definition for identity theft is elusive. However, there seems to be general agreement involves a number of activities including, at a minimum, unauthorized collection and fraudulent use of personal information. Ironically, while the public profile of identity theft seems to be increasing, the actual rate of occurrences has levelled off in recent years. However, the dollar volume of losses has increased, in both Canada and the U.S.

Identity theft involves a multiplicity of players: governments; law enforcement agencies; the corporate sector and individuals. All have a role to play in prevention, detection and mitigation.

The underlying causes of identity theft are numerous and complex. The readily available nature of personal information of all kinds, often in electronic form, combined with lax security measures on the part of governments, the corporate sector and individuals themselves, is a major factor. So too are advances in technology, such as the burgeoning use of the internet. As technology becomes more sophisticated, the phenomenon of identity theft has the potential to become an even greater problem.

[58] The Choicepoint issue is discussed in Privacy Journal on Choicepoint (April 2006) and in *Craats, supra* note 36 at 97-102.

[59] CBC News, "Security breach opens 1,400 Canadians to possible identity theft" (17 March 2004),online: CBC.CA <http://www.cbc.ca/story/canada/national/2004/03/16/credittheft040316.html>.

APPENDIX A – DEFINITIONS

Related definitions

There are many definitions of "personal information" and of "fraudulent use". The definitions below reflect the most common definitions of these terms in the literature on identity theft.

"personal information"	means information about an identifiable individual. The information will usually exceed a simple address and phone number to include information such as the person's date of birth, social insurance number (SIN), drivers licence number, vehicle registration certificate or bank account information.
"fraudulent use of personally identifiable information"	means an unlawful use of personally identifiable information of another individual to perform transactions such as open credit card and bank accounts, redirect mail, establish cellular phone service, access email accounts, rent vehicles, equipment, or accommodation, and even secure employment.

Published definitions

Below is a list of various definitions for what is generally known as "Identity Theft". The definitions are classified based on the type organisation which published it.

Government Agencies

"Identity theft is the unauthorized collection and use of your personal information, usually for criminal purposes. Your name, date of birth, address, credit card, Social Insurance Number (SIN) and other personal identification numbers can be used to open credit card and bank accounts, redirect mail, establish cellular phone service, rent vehicles, equipment, or accommodation, and even secure employment."

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

"Identity theft involves the use of a victim's personal information to impersonate them and illegally access their accounts, obtain credit and take out loans in the victim's name, obtain accommodation, or otherwise engage in transactions by masquerading as the victim. Identity theft also includes the acquisition or transfer of personal information as an instrument to commit these crimes in the future."

> **Information and Privacy Commissioner Ontario**, *Identity Theft Revisited: Security is Not Enough*, online: <http://www.ipc.on.ca/docs/idtheft-revisit.pdf>.

"Identity theft occurs when someone uses your personal identity information without your knowledge or consent to commit a crime, such as fraud or theft."

> **Ministry of Consumer and Business Services of Ontario**, *Keep Your Identity Safe: What you need to know to protect yourself*, online: <http://www.cbs.gov.on.ca/mcbs/english/pdf/idtheft_en.pdf#search=%22of%20Consumer%20and%.>.

"Identity theft is when someone uses your name and personal information to commit fraud or theft."

> **Alberta Government**, *Identity theft Participant tip sheet*, Seniors Fraud Awareness Campaign (30 September 2002), online: <htttp://www.seniors.gov.ab.ca/services_resources/fraud_awareness/2001campaign/Identitytheft_tipsheet.pdf#search=%22Alberta%20Government%2C%20Identity%20theft%20Participant%20tip%20sheet%22>.

"Identity theft is the use of your personal information, such as your name, address, driver's licence number, vehicle registration certificate, etc. without your knowledge, by another person."

> **Société de l'assurance automobile du Québec**, *Are You a Victim of Identity Theft*, online: <http://www.saaq.gouv.qc.ca/en/reach_us/identity_theft.html>.

"Identity theft occurs when someone uses your personal information to commit fraud or theft – such as opening accounts or incurring debt in your name, or taking money from your account."

> **Saskatchewan Justice Department**, *Identity Theft – What to do if it happens to you*, online: <http://www.publications.gov.sk.ca/details.cfm?p=9288&cl=1>.

"Identity theft refers to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain."

> **Department of the Solicitor General Canada and United States Department of Justice**, *Public Advisory: Special Report for Consumers on IDENTITY THEFT*, online: <http://ww2.psepc-sppcc.gc.ca/publications/policing/Identity_Theft_Consumers_e.asp>.

"When someone uses personal information such as your name, social insurance number (SIN), credit card number or other identifying information without your knowledge or permission, it is identity theft and it is a crime."

> **Alberta Government Services Consumer Information Centre**, *Consumer Tipsheet - Identity Theft,* online: <www.governmentservices.gov.ab.ca>.

"Personal identity theft is the unauthorized collection and fraudulent use of someone else's personal information."

> **Alberta Motor Association**, *Identity Theft,* online: <http://www.ama.ab.ca/images/images_pdf/IdentityTheftFINAL.pdf>.

"Identity theft occurs when someone steals your name and other personal information with the intention of assuming your identity to gain access to your finances, make purchases and incur debts in your name, or commit other crimes."

> **Canada Post**, *Postal Security,* online: <http://www.canadapost.ca/corporate/about/security/id_theft-e.asp>.

"This crime refers to the illicit gain and use of another person's personal and financial information in order to commit a variety of frauds, including real-estate and payment card fraud amongst others."

> **Criminal Intelligence Service Canada**, *Identity Theft,* online: <http://www.cisc.gc.ca/annual_reports/annualreport2005/identity_theft_2005_e.htm>.

"Identity theft occurs when someone uses your personal information without your knowledge or consent to commit a crime, such as fraud or theft."

> **Ministry of Government Services of Ontario**, *Identity Theft,* online: <http://www.cbs.gov.on.ca/mcbs/english/ID_theft.htm 22/03/2006>.

"Identity theft occurs when someone uses your personal information without your knowledge or consent to commit a crime, such as fraud or theft."

> **Manitoba Finance Consumer and Corporate Affaires**, *Tips for Reducing the Risk of Identity Theft,* online: <http://www.gov.mb.ca/finance/cca/consumb/identity.html>.

Periodicals

"Identity theft is broadly defined as ". . .the unlawful use of another's personal identifying information". Personal identifying information can include the individual's name, address, social security number, date of birth, alien registration number, taxpayer identification number, government passport number, driver's licence information, mother's maiden name, or biometric information such as a fingerprint, voice print, or retina image (U.S. Government Accounting Office, 2002c). Unlawful in this context constitutes the unauthorized use of another's personal information with criminal intent."

> Stuart F.H. Allisona, Amie M. Schuck & Kim Michelle Lerschc, "Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics" (2005) 33 Journal of Criminal Justice 19.

"Identity theft is the assumption of another person's financial identity through the use of the victim's identifying information. This information includes a person's name, address, date of birth, social security number, credit card numbers, and checking account information. With this information, a thief is capable of charging merchandise to the victim's account and changing the billing address for the account so that the unauthorized purchases remain undetected."

> A.J. Elbirt, "Who Are You? How to Protect Against Identity Theft", (Summer 2005) IEEE Technology and Society Magazine.

"Identity theft is an Information Age crime, fuelled by the practice of extending credit or service to people when they identify themselves with information such as Social Security and credit card numbers. Thieves know that if they possess little more information about a victim than, say, name, address and Social Security Number, they can steal credit or valuable services."

> Benjamin Wright, "Identity theft – US: Internet break-ins: new legal liability" (2004) vol. 20, no. 3 Computer Law & Security Report.

Trade Associations

"Identity theft involves securing pieces of an individual's personal information (e.g. birth certificate, social insurance card, driver's licence) and using the information extracted from these forms of identification to impersonate the individual. Once an identity has been "stolen" in this manner, the next step is to use the personal information to commit a forgery or a fraud for financial gain, such as taking over financial accounts or applying for loans and credit to make purchases."

> **Canadian Bankers Association**, Identity Theft: A prevention policy is needed, online: <http://www.cba.ca/en/content/reports/Identity%20Theft%20-%20A%20Prevention%20Policy%20is%20Needed%20ENG.pdf>.

"Identity theft (or identity fraud) includes criminal activity in which a person wrongfully obtains and subsequently uses someone else's personal information with a view to committing a forgery or a fraud for financial gain. An individual's personal information includes the person's name, address, telephone number, birth date, family information, social insurance number and financial account information including personal information numbers."

> **The Canadian Chamber of Commerce**, 2004 Policy Resolutions Industry, online: <http://www.chamber.ca/cmslib/general/I045.pdf#search=%22Canadian

%20Chamber%20Commerce%2C%202004%20Policy%20Resolutions%20Industry%22>.

"Identity thieves steal key pieces of personal information and use it to impersonate the victim and commit crimes in their name."

> **Business Practices & Consumer Protection Authority of British-Colombia**, Consumer Help - Identity Theft - How to Keep Your Self Safe, online: <http://www.bpcpa.ca/Consumers/help/consumers-help-identity-theft.htm>.

Consumer Associations

"The use of someone else's personal information, without his or her knowledge or consent, to commit a crime, such as fraud, theft or forgery. Identity theft also includes the acquisition or transfer of personal information as an instrument to commit these crimes in the future."

> **Consumer Measures Committee**, *Working Together to Prevent Identity Theft,*: online: <http://cmcweb.ca/epic/internet/incmc-cmc.nsf/vwapj/Consultation%20Workbook_IDTheft.pdf/$FILE/Consultation%20Workbook_IDTheft.pdf>.

"Identity theft is the misappropriation and unauthorized use of an individual's identity in order to gain some advantage (usually financial) by deception."

> **BC Freedom of Information and Privacy Association**, **PIPEDA and Identity Theft: Solutions for Protecting Canadians**, online: <http://fipa.bc.ca/library/Reports_and_Submissions/PIPEDA_and_Identity_Theft.pdf>.

"Identity theft occurs when someone wrongfully obtains and uses another person's personal identification data in a way that involves fraud or deception. Such data include name and date of birth or death and a range of closely related applications such as Social Insurance Number, passport, driver's licence and credit card numbers."

> **Public Policy Forum (PPF)**, Roundtable On Identity Theft And Identity Fraud **(**26 June, 2003), online: <http://ppforum.ca/common/assets/publications/en/identity_theft_fraud.pdf>.

"Identity theft is described as "acquiring key pieces of someone's identifying information in order to impersonate them and commit various crimes in that person's name.""

> **Consumer Association of Canada of Manitoba**, Identity Theft - Don't Be A Victim, online: <http://www.consumermanitoba.ca/scam/ID_theft.html>.

Law Enforcement agencies

Canada

"Maybe you never opened that account, or ordered an additional card, but someone else did....someone who used your name and personal information to commit fraud. When an impostor co-opts your name, your Social Insurance Number (SIN), your credit card number, or some other piece of your personal information for their use - short when someone appropriates your personal information without your knowledge - it's a crime, pure and simple."

> **Phone Busters** (operated by the Ontario Provincial Police and the Royal Canadian Mounted Police), *Recognize Identity Theft*, online: <http://www.phonebusters.com/english/recognizeit_identitythe.html>.

"Identity theft is a crime whereby the perpetrator acquires key pieces of personal information about an individual in order to impersonate them. The victim may be dead or living."

> **Calgary Police Services** - *A New Frontier in Crime*, online: <http://www.gov.calgary.ab.ca/police/crimeprev/ident_theft.html>.

"Identity theft is the wrongful use of another persons' identifying information – such as credit card, SIN, or driver's licence number to commit financial or other crimes. Identity Theft is generally a means for committing other offences such as fraudulently obtaining financial credit or loans, narcotics, terrorism, among other crimes."

> **Calgary Police Services**, *Identity Theft: Don't let it happen to you*, (January 2002) IACP National Law Enforcement Policy Centre, online: <http://www.calgarypolice.ca/crimeprev/pdf/identity_theft_2004.pdf>.

"When an impostor co-opts your name, your Social Insurance number (SIN), your credit card number, or some other piece of your personal information for their use - short when someone appropriates your personal information without your knowledge - it's a crime, pure and simple."

> **Ontario Provincial Police**, *Anti-Rackets Alerts: Identity Theft: Could it Happen to You*, online: <http://www.opp.ca/antirackets/english/identity.htm>.

"Identity theft occurs when someone appropriates some of your personal information without your knowledge and uses it to commit fraud. For example, your name and SIN number are used to fraudulently open a credit card account."

> **Waterloo Regional Police Service**, *Preventing Identity Theft*, online: <http://www.wrps.on.ca/fraud_identitytheft.html>.

"When an impostor co-opts your name, your Social Insurance number (SIN), your credit card number, or some other piece of your personal information for their use - short when someone appropriates your personal information without your knowledge - it's a crime, pure and simple."

> **Winnipeg Police Service**, *Crime Prevention: Identity Theft*, online: <http://www.winnipeg.ca/police/TakeAction/identity_theft.stm>.

United States

"Theft or misuse of personal or financial identifiers to gain value and/or facilitate criminal activity."

> **Federal Bureau of Investigation** (FBI), online: <http://www.fbi.gov/>.

Definitions from other organisations

"The act of impersonating another, by means of using the person's information, such as birth date, Social Security number, address, name, and bank account information."

> **HTG Solutions**, Identity Theft In E-Commerce, online: <http://www.technologyexecutivesclub.com/Articles/security/identifytheft.php>.

"Identity theft is the theft and fraudulent use of another person's identity or personal information."

> **Fasken Martineau**, Privacy and Information Protection Bulletin, online: <http://www.fasken.com/WEB/FMDWEBSITEFRENCH.NSF/0/DC49B870A45B9C4385256FB60061A73C/$File/BULLETIN_PRIVACY_FEB2005.PDF>.