Identity Theft:
Who Is Using Your Name?

by

Sean Moran

BCom. (Minor in Law), Carleton University, 2011

Capstone Submitted in Partial Fulfillment of the
Requirements for the Degree of
Master of Public Policy

in the
School of Public Policy
Faculty of Arts and Social Sciences

SIMON FRASER UNIVERSITY

Spring 2014

Approval

Name:	**Sean Moran**
Degree:	**Master of Public Policy**
Title:	***Identity Theft: Who Is Using Your Name?***
Examining Committee:	**Chair:** Nancy Olewiler Director, School of Public Policy, SFU

Maureen Maloney
Senior Supervisor
Professor

Dominique M. Gross
Supervisor
Professor

Rod Quiney
Internal Examiner
Visiting Professor

Date Defended: March 20, 2014

Partial Copyright Licence

Abstract

Technology has advanced at a tremendous pace over the last decade. These advancements have produced immense benefits to the population, but have also increased opportunities for criminal activity. Traditional crimes are being perpetuated in a different environment, with different tools, and targeting different victims. Identity theft is a form of larceny that may destroy a person's reputation and causes emotional and financial havoc, with long-lasting effects. Consequently, while research has progressed, it has been a constant struggle to keep up with the evolution of the crime and the subsequent policy and legislative responses of governments. This study investigates the rise of identity theft in Canada and its implications for individuals, businesses, governments, and other public bodies. The main objective of the research is to recommend ways Canadian legislation and policies can keep up to date with the accelerated growth of identity theft and fraud.

Keywords: identity theft; cybercrime; cyber fraud; Canada; public policy; regulation

Dedication

This research is dedicated to all the victims of identity theft and related crime.

Acknowledgements

Thank you to my supervisor, Maureen Maloney, for providing guidance and support throughout this whole process, to Dr. Richard Frank and Simon Fraser University's International Cybercrime Research Centre for your knowledge and expertise, to my friends for listening to me talk about identity theft and policy day and night, to that one person who changed my entire life, to my family, Jack, Sheila, and Stephanie, for being my rock and an excellent support system, and to my grandmother, Eileen, for showing me the light during the darkest times.

Table of Contents

List of Tables

List of Figures

List of Acronyms

ABM	Automated Banking Machine
CAFC	Canadian Anti-Fraud Centre
CBA	Canadian Bar Association
CIO	Chief Information Officer
CIPPIC	Canadian Internet Policy and Public Interest Clinic
CSIS	Canadian Security Intelligence Service
DLN	Drivers License Number
FBI	Federal Bureau of Investigation
FTC	Federal Trade Commission
GDP	Gross Domestic Product
ICRC	International Cybercrime Research Centre
ICSPA	International Cyber Security Protection Alliance
ID	Identity
IT	Information Technology
MeRC	McMaster eBusiness Research Centre
MLAT	Mutual Legal Assistance Treaties
OECD	Organisation for Economic Cooperation and Development
OPHIPA	Ontario Personal Health Information Protection Act
ORNEC	Ontario Research Network on Electronic Commerce
PIN	Personal Identification Number
PIPEDA	Personal Information Protection and Electronic Documents Act
RCMP	Royal Canadian Mounted Police
RECOL	Reporting Economic Crime Online
SIN	Social Identification Number
SMS	Short Message Service
SSN	Social Security Number
UNODC	United Nations Office on Drugs and Crime

Executive Summary

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. Identity theft, in which criminals use someone else’s personal identity and other relevant information in unauthorized ways, has become a significant and growing problem in Canada and many nations across the world. Combating identity theft and protecting consumers and society as a whole is of urgent importance to maintain a healthy economy and stable social environment. Identity documents, whether counterfeit or genuine, provide criminals with a powerful tool for targeting individuals, companies, and government agencies. The integrity of identity documents and identity information is crucial for maintaining public trust in Canada’s economy.

The impact of identity crime on victims is unlike that of other crimes. Individual identity is the basis of almost every aspect of modern life, and when it is compromised, victims often suffer long-term consequences. Apart from economic losses, there is often damage to reputation, loss of access to credit and other services, and in some cases victims even face criminal prosecution for acts committed by others in their name. Identity crimes are multi-layered offences where the theft of an identity is just the first in a series of crimes that can be national or international in scope. Preventing identity theft is, therefore, a first step toward deterring subsequent crimes. Identity theft is a very complex issue. It is not just a technical issue, but also involves economic, social, and legal issues.

This research is intended primarily to be a framework for the Canadian Federal and Provincial Governments to use when considering cyber fraud regulations. It also serves as an analysis tool for countries, provinces/states, and municipalities globally. This research aids the process of formulating and implementing new or updated policies and legislation to address the escalating global issue of cyber fraud, and more specifically, identity theft. The background combines science and statistical knowledge

to describe current gaps in policy in Canada. The research is informed by qualitative document content analysis, secondary research, and a jurisdictional review.

The objective of this research is to combat identity theft, identity fraud, and identity related crime. More generally, this research aims to promote security, combat crime, and protect victim's rights. Both non-legislative and legislative intervention policy options were presented against the status quo. Non-legislative policy options consist of increasing resources dedicated to combat cyber fraud in law enforcement agencies and businesses, establishing a central reporting agency for victims of identity theft and fraud, and improving and establishing more sophisticated information sharing networks involving identity theft and related crime. Legislative policy options consist of implementing credit freeze and security breach disclosure laws, establishing a national and international common standard definition of identity theft, and establishing international cooperation and partnerships. These policy options were evaluated using five criteria: effectiveness, efficiency, stakeholder impact, economic and financial impacts, and feasibility. Using a multi-criteria approach, the policies are scored as having either a small, medium, or large negative impact relative to the status quo or a small, medium, or large positive impact relative to the status quo. The fourth policy option (combined non-legislative and legislative intervention) ranks the highest. The second policy option (non-legislative intervention) ranked second, the third policy option (legislative intervention) ranked third, and the status quo was the least favourable option presented in this study.

In the short term, the study recommends that the Federal Government of Canada increase resources dedicated to combat cyber fraud in law enforcement agencies through re-allocation of the Cyber Security budget (including on-going education and training programs). Also in the short term, the Federal Government should impose mandatory sanctions on businesses to ensure they have proper resources and mechanisms in place to prevent and combat cyber fraud (including on-going education and training programs). In the medium term, the study recommends that the Federal Government of Canada roll-out the establishment of the Canadian Anti-Fraud Centre as being the central reporting and statistical agency for identity theft and fraud. Lastly, in the long term, the study recommends that Canada be continuously improving and

establishing more sophisticated information sharing networks relating to identity theft and fraud.

Without a national and global strategy, this crime will only continue to grow exponentially, as will the possibility of terrorist acts, financial crimes, drug trafficking, weapons smuggling, and human trafficking, all of which have an adverse impact on the global community and commerce. The recommendation offered here is an attempt to manage identity theft and fraud so that its growth will be contained and reduced. The goal is to get the issue identity theft and related crime to the top of national and international political agendas, since the repercussions are severe and detrimental to economic, social, and security stability.

Chapter 1. Introduction

Computers and information systems have become a fundamental part of Canadian life. Canadians' personal and professional lives have gone digital: we live, work, and play in cyberspace. Canadians use the Internet, computers, cell phones, and mobile devices every day as a means of communication with family, friends, and colleagues. Business is now conducted online, for example banking, shopping, and accessing government services. Digital infrastructure makes all of this possible, and also keeps essential services up and running. The associated information technology enables much of our commercial and industrial activity, supports our military and national security operations, and is a great resource for channelling social activities. Technology has advanced at a tremendous pace over the last decade. These advancements have produced immense benefits to the population, but have also increased opportunities for criminal activity. Traditional crimes are being perpetuated in a different environment, with different tools, and targeting different victims.

Cyber fraud, and more specifically, identity theft and fraud, is a common form of cybercrime today. Twenty years ago, the term "cyber fraud" 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 has become a serious social issue. Cyber fraud is a form of larceny that may destroy a person's reputation and causes emotional and financial havoc, with long-lasting effects. It may be devastating for individual victims, and poses many challenges for governments, businesses, and society in general. Many Canadian law enforcement personnel consider identity theft to be among the most difficult forms of theft to investigate. There has been a flurry of activity in Canada and the United States, as regulators and companies struggle to keep up with the rapid growth of this white-collar crime. Consequently, while research has progressed, it has been a constant struggle to keep up with the evolution of the crime and the subsequent policy and legislative responses of governments.

This study investigates the rise of identity theft in Canada and its implications for individuals, businesses, governments, and other public bodies. The main objective of the research is to recommend ways Canadian legislation and policies can keep up to date with the accelerated growth of identity theft and fraud. The research is based on qualitative (document and case study analysis) research methods, which assisted with the identification of the best policy alternatives and recommendations.

The rest of the research is organized in eight parts. Section 2 of the paper discusses the background and evolution of cyber fraud in Canada, identifies the key stakeholders, and will provide some statistical evidence of the seriousness of this form of cyber crime. Then, Section 3 provides a detailed description of the different methodologies and limitations utilized in this capstone. Section 4 presents the analysis and Section 5 the policy objectives and policy options. Section 6 outlines the criteria and measures, while Section 7 details the impact assessment of the policy options. Finally, Section 8 identifies the policy recommendations and provides the conclusion of the research.

Chapter 2. Background

2.1. Cybercrime (Evolution and Definition)

In the 1920's, it was said that the radical change in transportation of persons and goods effected by the introduction of the automobile, the speed with which it moves, and the ease with which evil-minded persons can avoid capture, have greatly encouraged and increased crimes (Clough, 2012). What was said about the automobile in the 1920's is equally applicable to digital technology today. We live in a digital age, and technology has transformed the way in which we socialize and conduct business. As much as this technological shift has had overwhelmingly positive effects, there has also been a dark side to these developments. Crime tends to follow opportunity and in much the same way as states have expanded their operations into cyberspace, so too have organized criminals. In other words, with every advance in technology, there has been a corresponding niche to be exploited for criminal purposes (Clough, 2012). For example, with the development of digital cameras and sharing photos on the Internet, child pornography has increased exponentially. With the convenience of electronic banking and online sales, fraud has escalated. Electronic communication such as email and SMS may be used to stalk and harass. Social media, such as Facebook and Twitter, have been platforms used by criminals to gather personal information for identity theft and fraud purposes (Clough, 2012). These are just a few niches that have been exploited by cyber criminals with the advancement of technology.

As computers became more mainstream, the idea of a separate category of 'computer crime' arose. As early as the 1960's there were reports of computer manipulation, computer sabotage, computer espionage, and the illegal use of computer systems (Clough, 2012). It was not until the 1970's that cybercrime started to accelerate more rapidly, which resulted in specific computer crime laws being enacted. The evolution of such legislation proved successful, reflecting changing concerns

surrounding the misuse of computers. However, rapid technological development continues, and will continue, to present new challenges. In 1982, Parliament passed the Privacy Act, which marked the first time that privacy had been dealt with under separate legislation (Peterson, 2009).

The September 11, 2001 terrorist attacks in the United States led to the passage of the Anti-Terrorism Act in November 2001. Passport Canada, Citizenship and Immigration, and other groups concerned with security became more acutely aware of the need to accurately identify those who entered and left the country. Debate over how to appropriately and safely store information about Canadians arose again (Peterson, 2009). The federal Personal Information Protection and Electronic Documents Act (PIPEDA) was initiated in 2004. PIPEDA has addressed many concerns relating to private companies and disclosure, but critics argue it has not gone far enough. Advocacy groups and individuals are urging the federal government to require leaks of personal information be disclosed, not only to the police and credit bureaus, but also to the affected consumers. Observers are also recommending that a larger budget be made available to law enforcement agencies and that stronger sanctions for cyber fraud be incorporated within the Criminal Code of Canada (Peterson, 2009). In response to these criticisms, the federal government has been developing an integrated, streamlined response to identity theft concerns. However, the Auditor General's report, released February 2007, revealed that, despite repeated warnings about problems with Social Insurance Numbers (SIN) since 1998, little action had been taken. The Auditor General warned that good SIN management was imperative to help prevent cyber fraud (Williams, 2007).

There are almost as many terms to describe cybercrime, as there are cybercrimes. Early descriptions included 'computer crime', 'computer-related crime', 'crime by computer', 'high-technology crime', 'information age crime', or 'digital, electronic, virtual, IT, and technology-enabled crime' (Clough, 2012). The term cybercrime is used because it is widely used in the literature, it has found its way into common usage, it emphasizes the importance of networked computers, and most importantly is the term adopted in the Council of Europe's Convention of Cybercrime (Clough, 2012). The Council of Europe's Convention on Cybercrime of 2001 defines

cybercrime in Articles 2-10 in terms of four substantive categories (Smyth & Carleton, 2011):

1. Offences against the confidentiality, integrity, and availability of computer data and systems;
2. Computer-related offences;
3. Content-related offences; and
4. Offences related to the infringement of copyright and other related rights.

One of the central differences between cybercrime and traditional crime is that traditional crime typically occurs in one space and has an impact on one set of victims, whereas cybercrime can have a global impact (Smyth & Carleton, 2011). Offenders can operate from anywhere in the world, targeting large numbers of people, businesses, governments, or other public bodies across international boundaries. This poses an obvious challenge for law enforcement; and those who commit cybercrime often seek to exploit this challenge, simultaneously undertaking their activities in one country against individuals in many different jurisdictions (Smyth & Carleton, 2011). Most of the time, the criminal activity is deliberately targeted in or through jurisdictions where regulations are known to be weak, or where investigative cooperation is known to be poor. This allows for the minimization of risk that their activities will be discovered, traced, or result in punishment. Despite criticisms that Canadian legislation and policies do not go far enough to address cyber fraud, other critics worry that some organizations are taking advantage of individuals by feeding into paranoia about the problem. For instance, some consumer advocates argue that certain components of identity theft insurance coverage may be superfluous (Peterson, 2009). Consumers can often obtain the same services offered by the insurance providers for free or at a minimal charge. Nevertheless, many Canadians are adding identity theft protection to their home insurance policies.

2.2. Cyber Fraud (Definition)

Cyber fraud can be defined as any act of dishonesty or deception carried out with the use of the Internet, or computer technologies, that defrauds the public or any person or organization out of property, money, valuable security, or service (Smyth & Carleton,

2011). Internet fraud can occur as a result of transmitting misleading or deceitful information online, by failing to honour contractual agreements entered into online, or through misappropriation of funds transmitted electronically (Smyth & Carleton, 2011). Anonymity is the key attribute that motivates online fraud relative to offline fraud. Internet transactions are agreements reached instantaneously and payments are made between anonymous individuals operating anywhere in the world. Online, there are no social cues, such as appearance, facial expression, body language, voice, dress, and demeanor, which may help one avoid fraud. Operating online greatly enhances the ability of individuals to disguise their true identities and intentions, which is an important reason why it is comparatively easy to commit fraud using the Internet, compared to committing fraud offline (Smyth & Carleton, 2011).

2.3. Stakeholders of Cyber Fraud

Individuals, or the general public, are not the only victims of cyber fraud, although they are the primary victims since they typically bear the financial costs through higher insurance premiums, credit card fees, and interest rates. That being said, it is also important to note that secondary victims do exist. A distinction can be made between primary victims and secondary victims of cyber fraud impacts. Primary victims are the individuals, businesses, or public bodies, who initially suffer the harms of fraud. Secondary victims are those who ultimately pay for the economic losses associated with the crime, which include financial institutions, insurance companies, others who, by contract or regulation, agree to reimburse some or all of the costs to primary victims, and finally the general public who pay with increased fees to cover the costs of the crime (Smyth & Carleton, 2011). Primary victims (consumers) do carry the burden of some financial costs, like legal fees, but financial costs ultimately fall on secondary victims. Primary victims predominantly suffer the consequences of social costs, for example, loss of reputation and subsidiary negative health effects. Four main stakeholders help combat cyber fraud through a variety of prevention, detection, and legal protection and theft prosecution activities. These four main stakeholders consist of **identity owners**, **identity issuers**, **identity verifiers**, and **identity protectors** (Wang & Yuan & Archer, 2006).

Individuals are also known as identity owners, and 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 license and health cards, for different purposes related to social activities and financial services throughout the owner's life (CIPPIC, 2007). Individuals are the primary victims of cyber fraud or identity theft since they ultimately carry the burden. Victims suffer financial losses, a loss of reputation, emotional distress, and the often-difficult task of rebuilding their credit rating (CIPPIC, 2007). Even though there are steps individuals can take to reduce the risk of cyber fraud, the Ontario Privacy Commissioner has noted that consumers are not in the best position to reduce cyber fraud. In reality, many consumers are not even aware of the collection, use, and disclosure of their personal information. However, because identities belong to identity owners, it is their responsibility to safeguard them. As such, they should be aware of the risk of cyber fraud and identity theft, and the severe legal and financial damage such theft could cause (Wang & Yuan & Archer, 2006). In addition, identity owners are responsible for using their identity legally and ethically, and not abusing their rights. In this sense, individuals are also identity protectors (Wang & Yuan & Archer, 2006).

Governments play three roles in the context of cyber fraud and identity theft, which consist of (1) issuers, (2) protectors, and (3) verifiers. Firstly, governments play the role of identity certificate issuers when individuals apply for identity certificates, which grant certain social or financial rights to the identity owner. Such certificates are valid for a person's (or organization's) identification for a specific purpose over a finite time period. They usually consist of six information components: certificate identifier (such as a passport number), certificate receiver (the owner's name), certificate purpose (citizenship), certificate issuer (the government), validation time period, and the issuer's signature or certification (Wang & Yuan & Archer, 2006). Governments issue identity certificates such as birth certificates, Social Security Numbers (SSN) in the United States or Social Identification Numbers (SIN) in Canada, drivers' licenses, and passports to eligible individuals. Secondly, governments play the role of identity information protectors by using appropriate authentication mechanisms when citizens apply for identity certificates. Government also enacts laws to protect victims of cyber fraud and punish perpetrators. Lastly, governments play the role of identity verifiers when

individuals apply for benefits offered by the different governmental programs. They ensure that the individual is who they say they are (CIPPIC, 2007). When authenticating identities, the checker must establish and use strict authentication processes and execution mechanisms.

Businesses and organizations are also vital stakeholders. 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 verifiers (CIPPIC, 2007). Credit-card checkers, such as merchants, normally verify credit-card validity through electronic communication with the issuer or the holder's bank. The cardholder's signature, however, usually isn't carefully verified. Cyber fraud may be facilitated when these organizations provide goods or services, or grant credit without conducting an appropriate screening of the individual. Businesses, as well as governments, that collect, hold, or transfer personal information, may be subject to security breaches, either internal or external. Businesses are identity information protectors, and therefore have a prevention role to play. They can fulfill this role by notifying their customers or clients about security breaches and about the risks of cyber fraud, and by offering certain protection packages, such as account monitoring (CIPPIC, 2007).

Law enforcement agencies also play a role of identity information protectors. However, because most investigations occur after cyber fraud has been committed, and prosecution rates for these offences are low, law enforcement agencies are better described as identity information restorers (CIPPIC, 2007). Police reports and affidavits can be used to restore a victim's credit record and reputation. Law enforcement agencies, such as the Royal Canadian Mounted Police (RCMP) and the United States Federal Bureau of Investigation (FBI), enforce laws to detect and prosecute violators and give victims legal protection (Wang & Yuan & Archer, 2006). Finally, law enforcement agencies can also play the role of identity verifiers when they make an arrest.

The contextual framework for combating identity theft is presented in the figure below. The nodes represent the major stakeholders, and arrows indicate their interactions and information flows. Red lines indicate the activities taken by identity

thieves/abusers. Green arrows indicate activities by other stakeholders (Wang, Yuan & Archer, 2006).

Figure 2-1. Contextual Framework for Combating Identity Theft

Source: Wang, Yuan & Archer, 2006

2.4. Common Types of Cyber Fraud That Lead To Identity Theft

Cyber fraud involves purposely obtaining the property of another through deception, and its popularity as a crime of opportunity is growing. This is largely due to the fundamental shift in the methods by which many forms of property are owned and stored, owing to rapid developments in technology, communications, and globalization (Smyth & Carleton, 2011). For example, in Canadian society, credit and debit card transactions are overtaking cash transactions in value, and the rise and growth of the Internet, which facilitates wireless transactions, has made theft, as well as the conversion of stolen property into cash, relatively effortless (Smyth & Carleton, 2011). Today, identity theft is the most common form of cyber fraud. The most common types of

cyber fraud that directly and indirectly lead to identity theft include: scareware, phishing scams, phony website fraud, online dating fraud, credit card fraud, insider fraud, and social media fraud.

Scareware:

Scareware remains a common form of cyber fraud because it manipulates the psychology of victims. Scareware takes place when misleading pop-ups suggest that a user's computer is infected with a virus, and prompts them to purchase fake antivirus software to fix the problem. When the victim agrees to the purchase, they provide credit card details to the persons behind the scam (Smyth & Carleton, 2011). The perpetrator can make use of the collected information for other harmful purposes such as identity theft and other methods of fraud.

Phishing Scams:

Phishing is as widespread as robbery and is an act of illegally acquiring sensitive information from an unsuspecting user. Phishing uses trustworthy websites, emails, and online messengers to try to bait and catch unaware users and get sensitive information from them. There are three steps to phishing: the lure, the hook, and the catch. The lure involves social engineering. Examples can include network or account security upgrades, financial incentives and rewards, or a threat of account closure. A phishing typically spams a large number of users with an email message. The email is designed to deceive or scare the user into following a hyperlink embedded in the email to a website controlled by the phisher. The hook is a website that mimics the appearance of a legitimate institution, designed to convince the user of its legitimacy. Victims are tricked into entering passwords or account information to avoid disruption or cancellation of their service. Finally, the catch is when the phisher makes use of the collected information for some harmful purpose such as fraud or identity theft (Smyth & Carleton, 2011).

Online Auction Fraud:

In an online auction, sellers can hide their identities, which provides sellers a significant opportunity to cheat buyers. Online auction fraud, which occurs both during

and after auctions, can involve any one or more of the following scenarios: misrepresentation of items, illegitimate bidding to preserve a low price, intentional fake bidding by the seller to drive the price up, adding hidden charges to an item, non-delivery of items, offering black market goods, and fraudulent online credit card transactions (Smyth & Carleton, 2011). In particular, the fraudulent online credit card transactions can lead to identity theft and other methods of fraud.

Phony Website Fraud:

The process of buying goods and services directly online, without a bid, is also subject to fraud. Criminals create fraudulent websites, designed to look legitimate to trick consumers into entering their credit card data or other personal information (Smyth & Carleton, 2011). The personal information gathered by the perpetrator can then be used for other criminal activities such as identity theft and fraud

Online Dating Fraud:

In this type of scenario, the scammer posts an attractive photo on an online dating site and sends out messages to other members on the site expressing interest. The next step is to engage in a one-on-one conversation with the potential victim, usually through email or instant message. The offender creates a personal relationship in order to ask for cash, merchandise, or other favors. The scammer only continues to lure the victim until credit card information, bank account details, or actual money can be extracted from the target (Smyth & Carleton, 2011). When a personal relationship is established, the scammer can collect as much personal information from the victim as possible to commit other crimes such as identity theft and fraud.

Credit Card Fraud:

Credit card fraud is the most common incident of identity-related fraud (Berg, 2009). Online shoppers are frequently willing to trade-off their privacy concerns in return for benefits such as convenience. Credit card fraud occurs when goods and services are obtained using active credit cards that have been obtained through illicit means. The offender can either use the victim's identity in order to apply for and obtain new credit cards or can fraudulently use an existing card belonging to the victim. Obtaining

counterfeit cards created from stolen information can do this or the credit cards can also be cloned using illicit card readers during an otherwise legitimate transaction (Smyth & Carleton, 2011).

Insider Fraud:

Insider fraud takes place when internal employees use the Internet to anonymously gain access to data that is not related to their jobs and misuse it for personal gain. Rogue insiders can also gain electronic access to the records of customers and other employees and use those records to fraudulent ends. These malicious acts are commonly perpetrated by current employees and contractors, as well as disgruntled former employees who have been dismissed, laid off, or who have resigned (Smyth & Carleton, 2011). The use of this stolen data can be used to commit other cyber crimes such as identity theft and fraud.

Social Media Fraud:

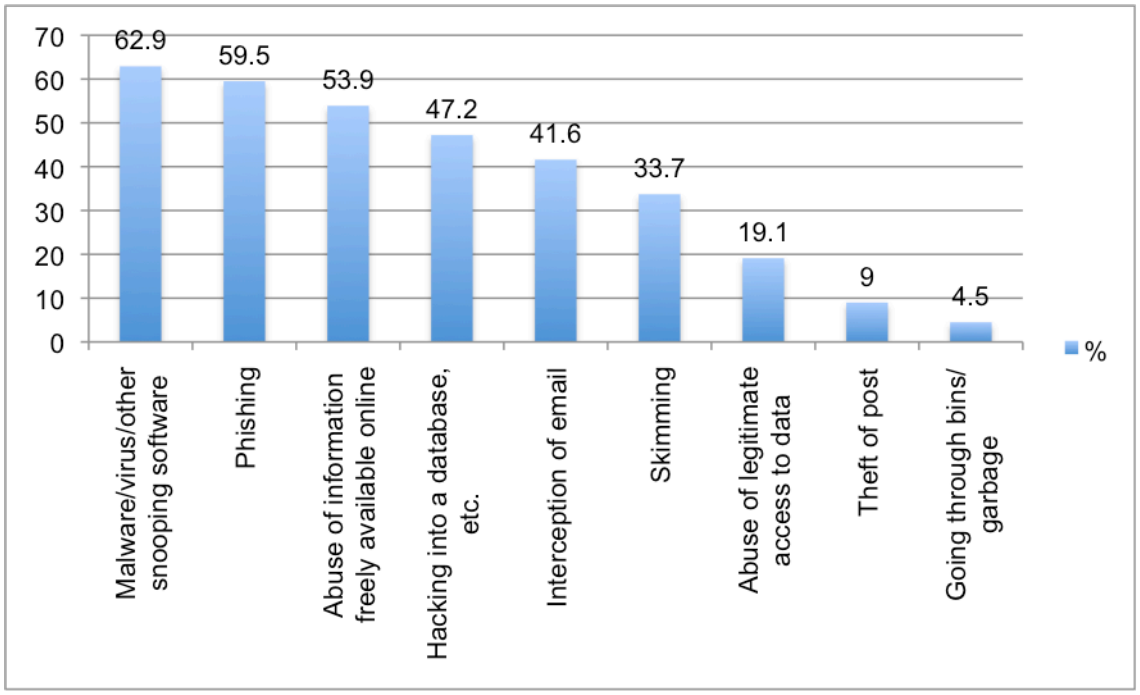
Social media sites generate revenue with targeted advertising, based on personal information. As such, they encourage registered users to provide as much information as possible. With limited government oversight, industry standards, or incentives to educate users on security, privacy, and identity protection, users are exposed to identity theft and fraud (Lewis, n.d.). With the increased global use of social media, there are more opportunities than ever before to steal identities or perpetrate fraud online. For example, a simple status update on Twitter, Facebook, and many other social media websites, can be used to benefit criminals in regards to identity theft and fraud. When it comes to stalking or stealing an identity, use of photo- and video-sharing sites like Flickr and YouTube provide deeper insights into you, your family and friends, your house, favorite hobbies and interests (Lewis, n.d.). These social networking sites have the greatest potential for abuse because they ask for sensitive information that can be used against you in a variety of malicious ways. The following profile elements can be used to steal or misappropriate your identity (Lewis, n.d.):

- Full name (particularly your middle name)
- Date of birth (often required)
- Home town

- Relationship status
- School locations and graduation dates
- Pet names (used as answers to security questions for online banking)
- Other affiliations, interests, and hobbies

The following figure provides an indication of trends with the most common methods of obtaining information for identity theft purposes; malware/virus/other snooping software being the most common and offline methods, like dumpster diving, being the least common.

Figure 2-2. Trends in Relation to the Methods Used by Offenders to Obtain Information for Identity Theft Purposes



Source: European Commission, 2012

2.5. Establishing the Characteristics of Cyber Fraud Offenders, Investigation, and Networks

Some of the essential features identified by researchers as to why cyber fraud is committed include the following (Smyth & Carleton, 2011):

- A perceived opportunity, such as the absence or bypassing of controls that enable fraud to be identified or prevented;
- An offender with a motivation to steal assets, whether through the existence of a financial crisis, the presence of debts, or living beyond one's means;
- A rationalization for acting illegally, such as the belief that the victim can bear the loss, or that the stolen funds will be repaid; and
- The absence of capable guardians, such as through inefficient business security practices, the absence of an effective regulatory framework, or a lack of effective fraud prevention resources and tactics.

A number of other recent trends have increased the number and frequency of cyber fraud incidents (Deloitte, 2010):

- An underground economy has evolved around stealing, packaging, and reselling information;
- Individuals and organizations are increasingly dependent upon computer-based technologies for the storage and processing of information and communications;
- Online banking, investing, retail and trade, as well as widespread intellectual property distribution, have created new opportunities for fraud and theft; and
- Economic hardships resulting from the 2008-2010 global financial recession created new opportunities to exploit peoples' fears and economic vulnerabilities.

Cyber fraud tends to be classified as a white-collar crime, but various studies have contextualized previous research on identity theft and highlighted the complexities in labeling the crime as white-collar (Copes & Vieraitis, 2009). Studies have shown that identity thieves are a diverse group. The majority of them were between the ages of 25 and 44 years, have at least some college, and were employed in a wide range of legitimate occupations (Copes & Vieraitis, 2009). Most criminologists support the basic assumption that white-collar crime must occur in the context of a legitimate occupation, but cyber fraud can be classified as either white-collar crime or property crime (Copes & Vieraitis, 2009). For example, according to various findings, identity thieves include property offenders (i.e. those who acquire information from other street offenders or from employees of certain businesses) and white-collar offenders (i.e. employees who acquire information from their place of work). Cyber fraud and, more specifically, identity theft should not simply be classified as white-collar crime because research shows that people commit this crime from a wide range of classes and backgrounds. It is best

categorized as an economic crime committed by a wide range of people from diverse backgrounds through a variety of legitimate and illegitimate occupations (Copes & Vieraitis, 2009). One of the major limitations to cyber fraud research is the lack of reporting to authorities. Therefore, the current research available is not conclusive and the demographic composition of cyber fraud criminals is difficult to determine, other than the fact that it tends to be an economically motivated crime. Even when some information is available, there is no indication of the basic socio-demographic characteristics of offenders. As such, research in the area of offenders is critically in need of development, but this can only be done thoroughly once mechanisms are in place to increase the reporting statistics to authorities (Wagner, 2007).

Newman and McNally developed an offender typology for these types of crimes in light of the fact that the defining trait of identity thieves is that they are "opportunists" (Newman & McNally, 2005):

1. Low-frequency offenders
    a. "Crisis Responders" appear to engage in criminality in response to some type of perceived crisis. "Perceived" being the operative word, offenders in this group might range from the parent who opens a utility account in their child's name because they have ruined their own credit or the criminal who needs to "lose" his real identity because a warrant is out for his arrest.
    b. "Opportunity Takers" respond to the desire to take advantage of some specific criminal opportunity. This group might include the cashier who notices that a customer has left their credit card and later uses it to make an unauthorized purchase, or the ordinary person who finds a wallet on the street.

2. High-frequency offenders
    a. "Opportunity Seekers" may not only search for opportunities to commit crime, they may create a situation amenable to committing a specific type of offense. This group would include the dumpster divers, scanners and your garden-variety thieves.
    b. "Stereotypical Criminals" are the highest-frequency offenders, with a mixed bag of criminal conduct, and their personal histories often include difficult childhoods, substance abuse, and other problems. Obviously, this category of offenders may span all types of identity theft, but is particularly relevant for organized crime activities and perhaps the drug-identity theft connection mentioned above.

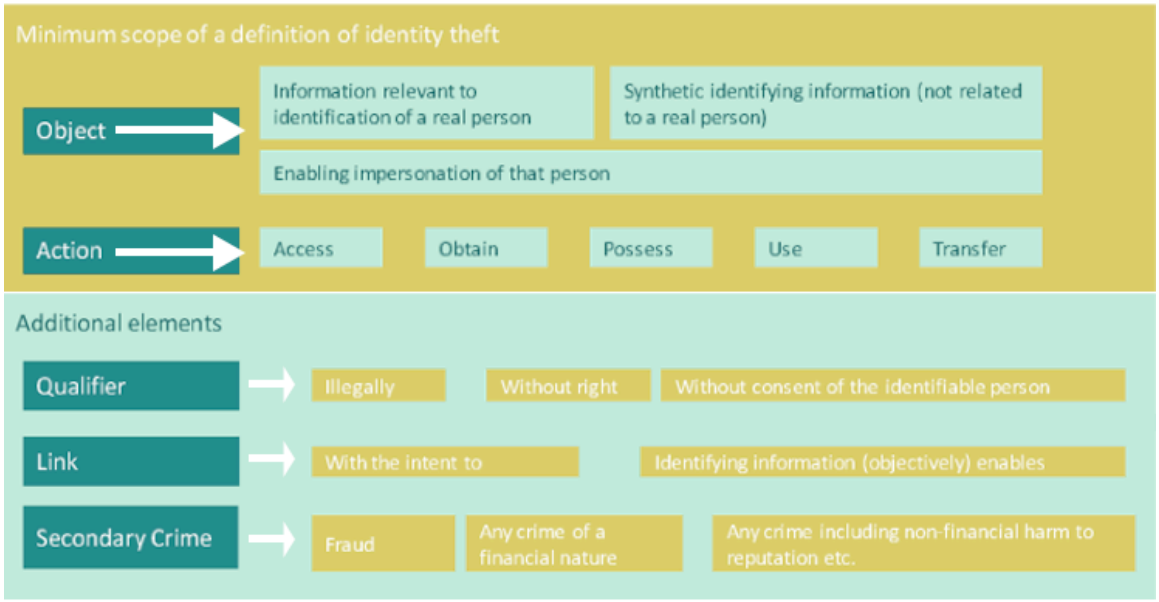
2.6. Identity Theft and Fraud (Definitions)

Identity theft is often described as the "quintessential crime of the information age", with impacts that are financially devastating and personally traumatic. One of the main issues with this crime is the lack of clarity in definition. In many nations there is neither a common terminology used to describe the phenomenon of identity theft (i.e. "identity theft", "identity fraud", and "identity-related crime") nor a common legal definition of it (European Commission, 2012). One author has described the 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." (Lombardi & Rosie, 2006)*

The list of definitions in Appendix A illustrates this point. Although they share many similar features, none of the definitions are identical in scope (CIPPIC, 2007). Another major concern with not having a commonly accepted definition of identity theft is the lack of consistency with the identification of primary and/or secondary victims within the definition itself. Some definitions focus solely on primary victims; whereas others go further to incorporate secondary victims. Without a clear definition, it is difficult for nations to propose and incorporate detailed legislation for this crime. However, notwithstanding the absence of a common definition, identity theft generally involves a number of key elements, as outlined in the following figure (European Commission, 2012):

Figure 2-3. Key Elements in Defining Identity Theft for the Purpose of a Legal Provision



Source: European Commission, 2012

To elaborate on the above diagram, the objective of identity theft, at the most basic level, involves the use of personal information in a pernicious and illegitimate manner for dishonest objectives. Immediately, therefore, consideration has to be given both to the type of information involved and the use to which it is put by the wrongdoer (European Commission, 2012). The object of the crime is therefore information relevant to identification of a real person or synthetic identifying information (not related to a real person), enabling impersonation of that person. The actions of the crime involve accessing, obtaining, possessing, using, and/or transferring identity information illegally, without right, and without consent of the identifiable person. This identifying information enables the criminal (who has the intent) to commit fraud, any crime of a financial nature, and/or any crime including non-financial harm to reputation, and so forth. For clarity, simplicity, consistency, and for the purposes of this research, the RCMP definitions (below) of identity theft and fraud will be used.

Identity theft refers to the preparatory stage of acquiring and collecting someone else's personal information for criminal purposes (RCMP, 2013).

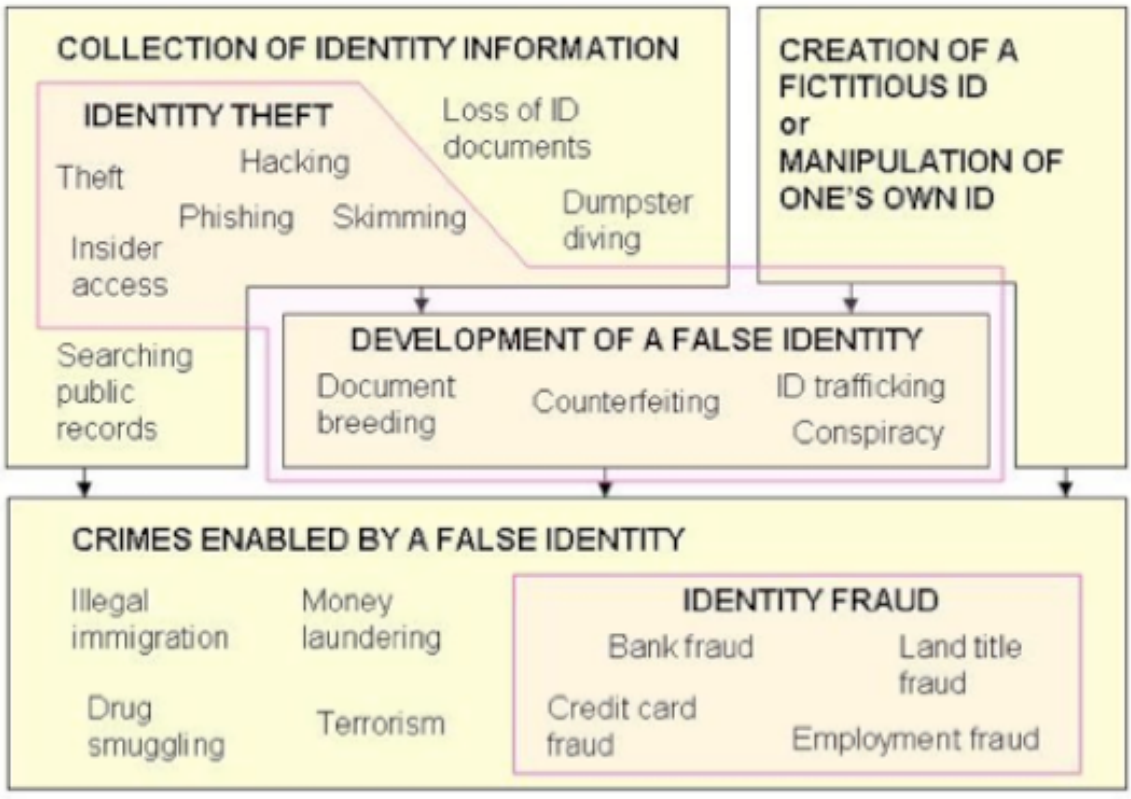
Identity fraud is the actual deceptive use of the identity information of another person (living or dead) in connection with various frauds (RCMP, 2013).

2.7. Identity Theft and Fraud (Evolution and Significance)

In some respects, identity theft is not a new phenomenon. For hundreds of years, people have claimed to be someone they are not for financial gain; to avoid responsibility for a misdeed, to gain social status, or to gain an employment position (CIPPIC, 2007). Document fraud, check swindling, and forgery have been techniques of choice for criminals for years, and are still a large part of current identity theft. Today, however, these crimes have become more complex, often involving many individuals, sophisticated techniques and technology, and inter-jurisdictional activity (CIPPIC, 2007). The Internet is a truly global medium, especially in the realm of electronic commerce. Thus, the Internet has been the source of many new legal and social issues facing the global community. The availability of personal data on the Internet, due considerably to the rapid increase in commercial activity on the medium, has caused an increase in cases of identity theft (Davis, 2003). Identity theft has been 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 (CIPPIC, 2007). A hallmark of identity theft is repeat victimization: the thief will usually engage in a series of fraudulent uses.

Sproule and Archer show the transition from the collection of personal information and the development of false identities to the use of false identities to commit fraud. They have proposed a useful definitional model of identity theft below (Sproule and Archer, 2006).

Figure 2-4. Definitional Model of Identity Theft



Source: Sproule & Archer, 2006

Identity theft is highly significant because a person's identity is unique and highly personal and to have one's identity information misappropriated by another is a privacy violation of the highest order. As it may be some time before a victim realizes what has happened, the financial costs of identity theft may be significant, creating very heavy emotional costs. 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 (CIPPIC, 2007). However, the effects of identity theft may go far beyond financial loss. Victims of traditional theft can usually replace most of their possessions, but a victim of identity theft may suffer a loss of reputation and standing in their community, as well as damage to their credit rating (CIPPIC, 2007). It may take considerable time and expense to resolve the resulting problems. There are even situations where, long after the event, victims may find themselves denied credit, or even arrested for crimes committed by the identity thief.

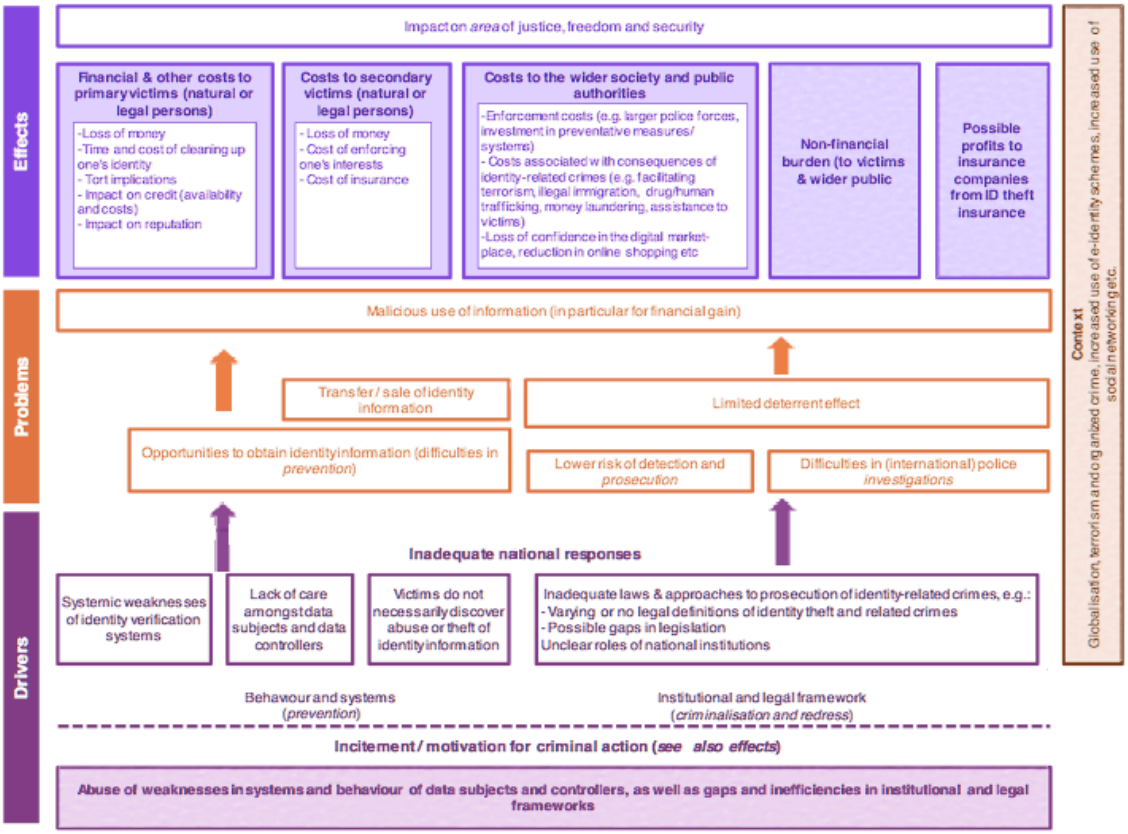
Law enforcement agencies have noted that identity theft is also a concern for this reason: it is often used as a means of furthering or facilitating other forms of fraud, organized crime, and terrorism (CIPPIC, 2007). Especially troubling is the now established link between identity theft and national security. Identity theft is often committed to facilitate crimes such as credit card fraud, document fraud, or employment fraud, which in turn can affect not only the nation's economy but also its security. Consequently, in securing the nation and its economic health, policymakers are tasked with reducing identity theft and its impact (Finklea, 2012). Governments in Canada, the United States, and 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, identity theft continues to challenge the best efforts of governments, law enforcement, the corporate sector, and individual citizens (CIPPIC, 2007).

Identity theft is a large problem globally and continues to grow exponentially, aided by the Internet, other advancements in technology, and the fact that so few individuals are ever charged and convicted of identity theft. It has become the perfect non-violent yet highly lucrative crime (BC FIPA, 2005). In 2012, there were a reported 17 thousand Canadian identity fraud victims and a total reported dollar loss of approximately $16 million (CAFC, 2012). Between 1998 and 2003, identity theft reports in Canada soared 500 per cent, according to Vanessa Giuliani, a fraud specialist with the credit information and reporting agency, Equifax Canada Inc. In Canada, Equifax and TransUnion, the two largest credit bureaus, receive approximately 1400 to 1800 complaints of identity theft per month (CIPPIC, 2007). However, the numbers are probably understated, as many cases go unreported. Given the nature of this crime, the potential exists that a number of victims may never know that they have been victimized. The issue of discovering and identifying the crime also affects known estimates of identity theft, reporting behaviours, and data collection efforts, since the crime may have been perpetrated more than six months prior to being discovered. Discovery may also be related to a number of additional variables such as the method of theft, the total losses associated with the theft, and particular victim socio-demographic characteristics (Newman & McNally, 2005). Nevertheless, even when the misuse is uncovered, the best available estimate suggests that 38% of victims do not report the crime to anyone

(Newman & McNally, 2005). Those who do report may not have their complaint recorded in official statistics, particularly if they report to the police, since police resources are being utilized and prioritized elsewhere. Businesses may elect not to report fraud to police because the incident is too minor. They may also be concerned about the ability to recover losses successfully through legal channels and that the time and resources needed to report an incident to the authorities and to assist in its prosecution will not justify the potential return on this investment (Smyth & Carleton, 2011).

The following chart (European Commission, 2012) sets out the identity theft problem tree, which outlines the identifying problems, drivers, and effects for individuals, businesses, and public authorities, while taking into consideration the effects on primary and secondary victims of identity theft.

Figure 2-5. Identity Theft Problem Tree



Source: European Commission, 2012

The above problem tree was developed by the European Commission and is an excellent framework to help address the issues here in Canada. The problem tree is based on a "matrix" of drivers, where incitement/motivation for criminal action and inadequate national responses lead into the identification of problems and effects. The incitement/motivation of criminals is closely linked to the effects, in terms of economic gain for the perpetrators and/or causing other types of harm to the victim, for example. Furthermore, research reveals that there is a low risk of detection, which is an additional incentive for criminals (European Commission, 2012). Inadequate national responses can further be divided into inadequate prevention measures and inadequate criminalization and redress measures. Inadequacies in criminalization and redress measures complicates law enforcement, leads to difficulties in international police cooperation, and to a lower risk of detection of identity-related crimes (European Commission, 2012). With regards to the effects of identity theft, there are financial and other costs to primary victims (natural or legal persons), costs to secondary victims (natural or legal persons), costs to the wider society and public authorities, and non-financial burdens to victims and the wider public. There are also potential profits to insurance companies from identity theft insurance.

Identity information is used for a variety of crimes. A non-exhaustive list is as follows (European Commission, 2012):

- Transferring/selling identity information for use for or funding of other criminal activities (i.e. organized crime, terrorism);
- Various frauds (financial fraud, money laundering, social services fraud, etc.);
- Human trafficking, smuggling of people, illegal migration;
- Stalking, bullying/harassment/damage reputation;
- Funding of and use for the purpose of other types of criminal activities (i.e. drugs trafficking, terrorism, organized crime)

While it is clear from the research carried out that identity theft is frequently associated with financial fraud, identity theft is also often related to money laundering as it is commonly used in the process of converting "dirty" money into "clean" money. There is also a distinction to be made between fraud affecting the private sector and fraud vis-à-vis the public sector, like social services fraud. This is especially common in the healthcare sector and various studies have been done specifically on medical identity

theft. Social benefit fraud relates to the unjustified claim for social benefits with the purpose of gaining an illegitimate financial benefit from public institutions or authorities. Social benefit fraud is conducted by using falsified identification or supporting documents to unlawfully apply for social benefits (Rand Europe, 2011). With the increasing importance of communication channels and social media (especially social networks) on the Internet, there is a growing prevalence of cyber bullying since perpetrators tend to hide behind false identities and profiles to carry out such attacks. There is also a clear link between the transfer/selling of identity information and organized crime, and in many instances, terrorism. Ideologically/politically motivated groups commit identity theft in order to raise funds and launder money to commit other crimes, as is the case for many terrorist cells, like Al Quaeda. The 2010 Report on Organized Crime of Canadian authorities states that:

> *"Organized crime groups are known to produce, supply, or use false identities. The increased availability and ease of access to personal information and business records online makes it easier for criminals to steal information and use it fraudulently. Organized crime uses three main methods: modification of some aspect of their own identity; creation of a wholly fictitious identity; or theft of someone else's identity, either living or dead. These false identities assist organized criminals to avoid detection by law enforcement, particularly when travelling and to protect their assets from confiscation. Individuals also use false identification to carry out or enable criminal activity where evidence of an identity is a key requirement, such as fraud, financial crimes, or people smuggling. Other forms of misrepresentation may also be used, such as false information on a company or vehicle identity, consignments, business accounts, and transactions" (CSIS, 2010).*

It is clear that identity theft and related crime are a multilevel and multistate phenomenon. The below table illustrates the frequency of use of identity-related information for the purpose of various types of crime. Financial fraud tends to be the most popular form of criminal activity with the use of false identity-related information.

Table 2-1. Frequency of Use of Identity-related Information for the Purpose of Various Types of Crime

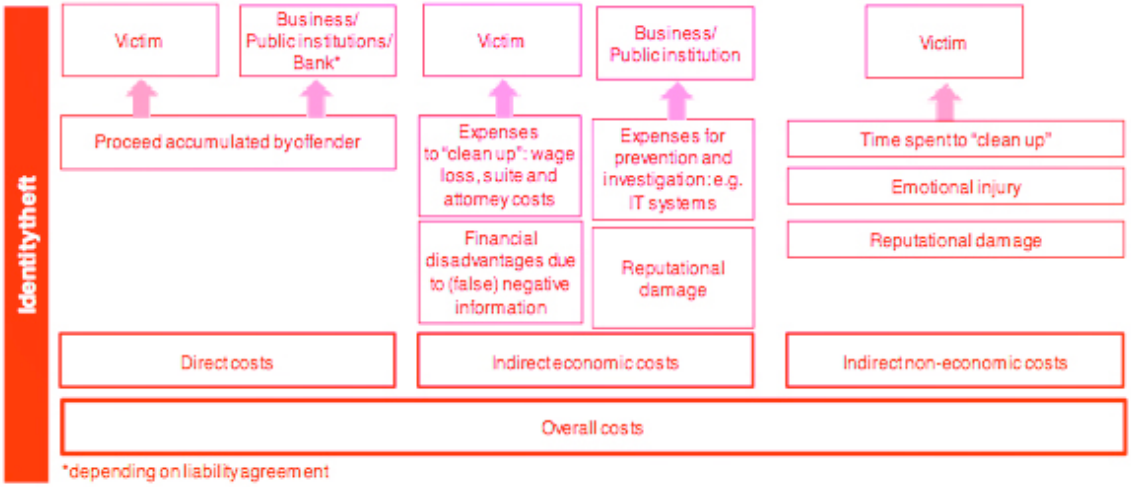
Options	Rarely		Very Little		Not Very Often		Sometimes		Quite Often		Very Often		Don't Know		Total	
	#	%	#	%	#	%	#	%	#	%	#	%	#	%	#	%
Transferring (selling) identity information	0	0.0	3	3.4	7	7.9	21	23.6	10	11.2	23	25.8	25	28.1	89	100
Human trafficking	4	4.5	7	7.9	11	12.4	9	10.1	6	6.7	8	9.0	44	49.4	89	100
Money laundering	3	3.4	5	5.6	5	5.6	16	18.0	15	16.9	19	21.3	26	29.2	89	100
Financial fraud	1	1.1	2	2.2	2	2.2	10	11.2	10	11.2	42	47.2	22	24.7	89	100

Source: European Commission, 2012

2.8. Identity Theft and Fraud (Costs)

Estimating the costs of identity theft is a much more difficult task than estimating its extent. There is an abundance of costs associated with identity theft, which include financial costs to businesses, the criminal justice system, and individuals, non-financial personal costs, and societal costs. The following figure provides a typology of costs for victims resulting from identity theft.

Figure 2-6. Typology of Costs



Source: Deloitte, 2012

In the diagram above, overall costs consist of direct costs, indirect economic costs, and indirect non-economic costs to both the primary and secondary victims. In terms of financial costs to businesses, the collective losses occasioned by credit card fraud, insurance fraud, and health care fraud are in the hundreds of billions of dollars per year (Newman & McNally, 2005). When business systems are infiltrated to steal identities, there are costs to recover these losses, costs for investigative procedures, costs to cover resources necessary to implement or maintain the new system, and soft costs that can be expected to upgrade the system in later years (Newman & McNally, 2005). In terms of direct losses, credit card companies take the biggest hit when the crime of identity theft is committed. In general, financial institutions indemnify for identity theft losses or other associated costs. Many consider such losses as a cost of doing business, and have found it easier to write off the loss rather than to investigate or prosecute such cases (Newman & McNally, 2005). The Canadian Bankers Association reported that in 2012, credit card fraud totalled approximately $440 million (CBA, 2013). They also reported that total debit card counterfeit costs totalled $38 thousand in 2012 (CBA, 2013). Figures derived from Equifax's fraud solution database for the financial sector reveal that there was more than $650 million in fraud incidents attempted across Canada in 2011 (Equifax, 2012). The greatest dollar value of attempted fraud activity was within mortgage applications, at over $400 million (Equifax, 2012). Other significant findings reported by Equifax included:

- Approximately $1.7 million attempted fraud activity was detected daily
- Fraud incidents for Loan Applications amounted to $160 million, Deposit Account and Credit Card applications, totalled $48 million and $17 million, respectively
- Credit card application fraud incidents accounted for more than 40 percent of the total number of incidents attempted, but less than 3 percent of the estimated total dollar value
- Mortgage application fraud incidents accounted for 13 percent of the total number of fraud incidents, equating to two-thirds of the total estimated dollar value
- The highest relative fraud detection rates were in the months of April and May, while the lowest were in November and December

Financial costs to the criminal justice system consist of investigation costs, federal prosecution costs, and corrections costs. Even though businesses bear the financial burden, some costs are borne by individuals directly. There are plenty of out-of-pocket expenses that victims of identity theft incur, for example, legal fees (Newman & McNally, 2005). Individuals suffer various types of additional costs as a result of their victimization, which can include the time and effort required to resolve various problems created by the theft, the emotional impact or feeling of violation that often results, and the frustration of being harassed by debt collectors or dealing with various agencies in trying to resolve problems (Newman & McNally, 2005). There are also the opportunity costs: for example, a victim's inability to obtain a job, purchase a car, or qualify for various types of loans. National security risks and threats, public safety risks and threats, burdens created by the presence of illegal immigrants, higher premiums or other costs passed on by companies to consumers, and overall decreased confidence in the promised benefits of the information age are all common societal costs incurred when identity theft takes place (Newman & McNally, 2005).

The types of effects arising from identity theft and the extent to which primary and secondary victims are affected is summarized in the table below:

Table 2-2. Types of Effects on Victims

Effects	Primary Victim	Secondary Victim
Loss of money	X	X
Time and cost of cleaning up one's identity	X	
Tort implications	X	
Impact on credit (availability and costs)	X	
Impact on reputation	X	
Costs of enforcing one's interests		X
Cost of insurance		X
Psychological and social distress	X	X

Source: European Commission, 2012

2.9. Identity Theft and Fraud (Challenges for Investigation)

There are eleven main challenges to the investigation of identity theft crimes (CIPPIC, 2007).

1. According to Canadian law enforcement agencies, the greatest challenge to enforcing identity theft laws is identifying the suspect, and identifying when, where, and how the victim's identity was compromised.
2. There is a lack of physical proximity, as there may be a large geographical separation between the victim and the identity thief.
3. The typical identity theft crime involves at least three parties: the thief, the victim(s) and the defrauded institution(s). In some situations, one or more of these three parties may be located in different jurisdictions. In such a scenario, law enforcement agencies must deal with multiple jurisdictions, which may have completely different laws or legal systems.
4. According to police, criminals are increasingly using the Internet to engage in various elements of their crimes and to hide from law enforcement agencies. As new technologies emerge, more and more challenges present themselves when investigating identity theft crimes.
5. Information breeding and related crimes also pose challenges. A single piece of personal information may be used to create forgeries or to obtain additional pieces of information. Identity theft can complicate the investigations of other crimes as well.
6. It is very difficult to determine the actual number of identity thefts because many victims and organizations fail to report the theft and

fraud. This poses many challenges for law enforcement agencies and researchers in the field.

7. Financial institutions often only become more cooperative when they suffer a major loss due to the theft.
8. There are limits on sharing information for investigatory purposes. The Canadian Association of Chiefs of Police has called for greater access to federal and provincial government databanks for the purpose of validating identification documents. Privacy laws however place limits on the sharing of information among agencies in order to protect Canadians from the abuse of their personally identifiable information.
9. There is currently a lack of resources to investigate identity theft. Law enforcement agencies may find it difficult not only to obtain needed resources but also to quantify in monetary and staffing terms the resources devoted to identity crimes.
10. Police need special training in order to be able to investigate identity theft crimes effectively. The exploitation of technology through phishing and the use of malware are expected to increase over time. Currently, there is a lack of training in this field.
11. Law enforcement agencies point to perceived deficiencies in the Canadian Criminal Code as a key challenge in prosecuting identity theft crimes.

Most law enforcement officers feel new policies would help deter identity theft opportunities. Officers made several recommendations, ranging from new laws and department policies to tighter security and cooperation from private financial institutions (The Police Chief, 2005). Often one incident of fraud may require multiple paths of investigation to be followed, which can lead to duplication of procedures and wasted time, effort, and expense (Smith, 2008). Individuals or organizations may choose to go to the police, private lawyers to claim compensation, relevant corporations such as banks or insurance companies to seek redress, dedicated consumer complaint-handling bodies such as healthcare complaints commissioners, professional regulatory boards, or ombudsmen, associations, and regulatory bodies such as those for lawyers or accountants (Smith, 2008). Knowing which avenue to pursue, and which procedures to follow pose difficult and complicated choices for everyone. Without having one major regulatory body overseeing these types of complaints, and without coordination in handling these issues, many unnecessary problems will continually occur.

2.10. Identity Theft and Fraud (Canadian Legislation)

The table below indicates which countries have specific criminal legislation dedicated to identity theft or have relevant provisions in other criminal law (Robinson, Graux, Parrilli, Klautzer & Valeri, 2011).

Table 2-3. Country Comparisons

Country	Specific ID Theft Law	Relevant Provisions in Criminal Law	Case Law?	Specific Dedicated Reporting Point?	Public Awareness Campaign
Canada	Yes	Yes	No	No	No
United States	Yes	Yes	Yes	Yes	Yes

Source: Robinson et al., 2011

The value added of this table shows the differences between Canada and the United States in terms of mechanisms in place to combat identity theft. For example, the United States covers all categories, whereas Canada does not have case law, a specific dedicated reporting point for victims, or public awareness campaigns – all of which would help prevent and reduce identity theft.

Canada has specific identity theft law and relevant provisions in criminal law, but does not have case law related to identity theft, a centralized reporting point for victims, or a public awareness campaign. The United States law covers all these aspects.

Table 2.4 below indicates the maximum and minimum criminal sanctions available from criminal law provisions in Canada and the United States (Robinson et al., 2011).

Table 2-4. Maximum and Minimum Available Criminal Sanctions

Country	Maximum Criminal Sanction	Minimum Criminal Sanction
Canada	Up to 14 years (Section 380(1) of the Criminal Code)	Up to 6 months (Section 342.01 of the Criminal Code)
United States	Life imprisonment (Title 18 Section 1030 US Criminal Code)	Up to 1 year (Section 2701-2711 US Criminal Code)

Source: Robinson et al., 2011

In Canada, the maximum sentence is up to 14 years in prison and the minimum sentence is up to 6 months in prison. In the United States, the maximum sentence is life imprisonment and the minimum sentence is up to 1 year in prison.

Table 2.5 below illustrates in further detail the existence of reporting mechanisms, whether they are online or offline, and whether they cover identity theft specifically or all forms of crime. The table also illustrates whether there is a feedback mechanism for keeping the victim or individual who made the report appraised of the progress of the case (Robinson et al., 2011)

Table 2-5. Reporting Mechanisms

Country	Dedicated Off/Online Portal?	ID Theft	All Crime	Feedback
Canada	None	n/a	n/a	n/a
United States	Online	Yes	Yes	No

Source: Robinson et al., 2011

Canada currently has no existing reporting mechanisms, whereas the United States has online reporting mechanisms for identity theft specifically, and all other crimes. However, the U.S. does not have feedback mechanisms for victims in place.

There are a variety of types of legislative instruments that may be developed, enacted, or used to address identity theft and fraud. These include (Robinson et al., 2011):

- Identity theft legislation (such as in Canada, France, or the United States) that specifically criminalizes varying types of misuse
- Legislation with regard to the protection of personal data (including regulations that govern the circumstances under which personal data can be collected and for which it might be processed, and security breach notification laws)
- Legislation and regulations relating to identity documents and numbers (such as national identity cards or social security numbers) that governs the existence, use and forgery of specific identity tokens or credentials
- General penal provisions with respect to fraud, forgery and usurpation of titles (providing these provisions are phrased sufficiently broadly they may be useful and appropriate for sanctioning even high-tech instances of identity theft), which may have been amended as a result of international harmonization

initiatives in the field of high-tech crime (i.e. the Council of Europe Convention on Cybercrime)

- Regulations specific to a particular sector (i.e. aimed at fighting organized crime or terrorism). Generally such legislation provides an indication of the success of the track record of operational efforts to address this problem
- Non-criminal regulations (administrative infractions, civil suits and torts, which may result in non-criminal fines and/or the awarding of damages to victims) might be available and should be taken into account

In Canada, authority to enact legislation is divided between the Parliament of Canada and the provincial legislatures, as set out in the Constitution. The federal government's sphere of authority includes unemployment insurance, banks, and criminal and privacy matters. The provincial sphere includes consumer reporting agencies, consumer protection, collection agencies, highway and transportation, personal health, vital statistics and privacy (CIPPIC, 2007). Direct responses to the problem of identity theft fall under a number of Federal Departments (Industry Canada, n.d.):

- The Department of Justice for specifying new offenses;
- The Office of Consumer Affairs for Federal/Provincial/Territorial responses and educating consumers on how to avoid becoming a victim;
- The Department of Public Safety to issue advisory alerts, address organized crime aspects, and address national security aspects of identity theft.

In May 2007, the Federal Privacy Commissioner called on the Canadian government to take immediate action to stem identity fraud. On the 31st of March 2009 the Act to amend the Criminal Code (identity theft and related misconduct), Bill S-4, was introduced in the Senate (Tunstall, 2009). The Act came into force on the 8th of January 2010, and, with a few additional offences, covers the same provisions proposed in 2007 by Bill C27, and has amended the Criminal Code to cover identity-related crimes (Robinson et al., 2011). More specifically, this bill covers certain activities not previously covered by other provisions of the Criminal Code, such preparatory activities. As the legislation is only recently enacted in 2010, it is too early to predict how it will impact identity theft and related crime.

Section 403 of the Criminal Code has provisions relating to Fraud, Forgery, and Cybercrime, which federally regulates privacy and data security, alongside the Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA). In

addition, several privacy laws are also implemented at the provincial level, for example Ontario's Freedom of Information and Protection of Privacy Act. The Personal Information Protection and Electronic Documents Act (PIPEDA) is relevant to identity theft because it addresses the security of personal information. Unfortunately, the principles are drafted in very broad terms and the statute lacks both strong enforcement powers and penalties for noncompliance (CIPPIC, 2007). A major limitation to PIPEDA is that it does not include a requirement that individuals whose personal information might be at risk be notified in the event of a security breach (Office of the Privacy Commissioner of Canada, 2013).

In terms of reporting mechanisms in Canada, there is no one-stop-shop mechanism in place. There are several points of information, and a range of different entities operates these websites and hotlines, which include Canadian law enforcement agencies, ministries, other governmental entities, and non-profit organizations. An example would be the Canadian Anti Fraud Center. However, none of these hotlines/websites seem to coordinate the efforts of law enforcement, rather they provide guidance on the steps to be taken after having become a victim, and raise awareness by providing information material to the public (Robinson et al., 2011). Given that there is no one-stop-shop mechanism in place, victims still have to report to the local law enforcement office and contact several administrative agencies in order to remedy the identity theft.

Chapter 3. Methodology

This research is cyber fraud regulations. This research aids the process of formulating and implementing new or updated policies and legislation to address the escalating global issue of cyber fraud, and more specifically, identity theft. The background describes current gaps in policy in Canada.

3.1. Qualitative Document Content Analysis

Cyber fraud and identity theft is an expanding phenomenon and research in this area is growing throughout the world. This method includes the analysis of the most important policy and academic documents at the national and local levels. Statistics Canada and The Canadian Anti-Fraud Centre are the two central fraud data repositories from which most of the statistical evidence was gathered and analyzed in order to formulate policy options for Canada. The Canadian Internet Policy and Public Interest Clinic has conducted a vast amount of research in this area and their working papers in this area will be consulted and applied in order to further develop this research.

Canadian and U.S. cyber fraud legislation is reviewed and analyzed to determine similarities and areas of improvement. Legislation is an important aspect of this research because it is a vital tool to combat cyber fraud and identity theft. Analyzing legislation identifies the current legal framework for battling this issue and identifies gaps within Canadian legislation and policies. It is necessary for legislation to evolve as technology advances and creates more avenues to commit cyber fraud.

3.2. Secondary Research

Cyber fraud has become a primary concern for individuals, businesses, governments, and law enforcement agencies globally. It is a relatively new phenomenon and is continually evolving as technology advances. There is little need for primary research in this field since there is plentiful secondary research available. There are a number of research organizations focusing solely on cyber crime and a variety of surveys have been administered relating to identity theft that is incorporated into my analysis. Three main studies are analyzed in my research. The first study is an impact assessment on a proposal for a new legal framework on identity theft, conducted by the European Commission. The second and third studies are directed towards businesses and how cyber fraud impacts everyday operations.

3.3. Method to Develop Jurisdictional Review

To identify best practices for addressing the policy problem, I compare Canadian legislation to United States legislation. To avoid selection bias, I chose to compare Canada to the United States because they both have very similar cyber security strategies in place and are members of various international organizations dealing with cyber crime. To conduct this jurisdictional review I used governmental websites, including the Department of Justice (Canada), Department of National Defence (Canada), Office of the Privacy Commissioner of Canada (Canada), Federal Trade Commission (United States), and State of California's Penal and Civil Code (United States).

3.4. Methodological Challenges and Limitations

Certain methodological challenges and limitations were present while conducting research for this capstone. The first difficulty was determining which pieces of legislation to analyze, since cyber fraud does not yet have its own section within the Canadian legal framework. There is a range of legislation and policies dealing directly and indirectly with cyber fraud, and since there have been problems defining cyber fraud and identity theft,

some of the current legislation is vague and indirectly refers to this specific crime, making it difficult to locate in the Canadian legal framework.

Cyber fraud is a relatively new phenomenon and therefore there are limitations to the available research. One of the major issues is the lack of reporting to law enforcement agencies by individuals and organizations for a variety of reasons. If cyber fraud is not reported, it makes it very difficult to obtain accurate statistics. Researching the underlying reasons for the causes of cyber fraud and conducting victim and criminal profiling poses various challenges when there is a lack of reporting to authorities. Since reporting issues have been identified, various sensitivity analyses can be done to offset certain biases. There are also other concerns related to the logistics of data collection for organizations hit by cyber fraud and the lack of communication between data sources based in a competitive business environment. If companies start collecting the data, it would provide better insight into cyber fraud. There are also economic motivations behind industries not reporting cyber fraud. For example, organizations that do not suffer directly may not find it necessary to report the crime to authorities.

Chapter 4. Analysis

4.1. Consumers/Individuals

A survey of Canadian consumers was conducted in 2008 by the McMaster eBusiness Research Centre (MeRC) on behalf of the Ontario Research Network on Electronic Commerce (ORNEC). The survey was designed to determine the nature and extent of identity theft and fraud in Canada. It also examines the concerns of Canadian consumers and their behavior related to the prevention and detection of identity theft and fraud. According to the results of the survey, 6.5% of Canadian adults, or almost 1.7 million people, were the victim of some kind of identity fraud in 2008. These victims spent over 20 million hours and more than $150 million to resolve problems associated with these frauds (Sproule & Archer, 2008). The results of this particular survey showed that 57% of the victims did not know how their personal information was accessed, but when they did know, the identity fraud was most often associated with a business transaction conducted either in person or online (Sproule & Archer, 2008). According to the literature, very few people tend to report identity theft and fraud to the authorities. In Sproule and Archer's study, only 13% of identity theft victims reported the crime to police, 6% to credit reporting agencies, and 0.5% to the now named Canadian Anti-Fraud Centre. There are two issues here – the lack of reporting by victims and the lack of clarity of who to report the crime to.

This particular survey and the literature also indicated that Canadian consumers' level of concern about identity fraud is higher than it was a year ago, and the level of concern increases with age (Sproule & Archer, 2008). Sproule and Archer's study highlighted the following:

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

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

- Canadian consumers take the following measures to keep their personal information from prying eyes or unauthorized access:
  - 92% never or rarely give information over the phone to people claiming to do surveys or offer promotional goods or services
  - 88% make sure that no one is watching, all of the time or most of the time, when using an ABM or debit card machine
  - 35% have reduced or stopped giving their credit card to waiters or gas station attendants
- Safe online practices are also important to protect personal information, and Canadian consumers report the following practices:
  - 75% use hard-to-break passwords all of the time or most of the time
  - 59% use different passwords for different applications all of the time or most of the time
  - While consumers change their important passwords at least every 2-5 years, 30% report that they never change these passwords
- Frequent and careful monitoring of accounts is the best way to detect and minimize the effects of identity fraud. Most check their online bank accounts regularly, however:
  - 49% had never requested a copy of their credit report
  - 77% had never checked land registry records

The Generation Y Online Security Survey of April 2010 from the United States emphasizes that young adults often engage in risky online behaviour, which often puts them in the crosshairs of identity thieves. The survey indicated that young adults are not always as careful as they should be when posting and accessing information online and most admitted to using the same password for all of their online accounts (European Commission, 2012). According to this particular survey and the literature, convenience

trumps safety. Fifty-five percent of those surveyed indicated they never check their credit report, 35% do not always check bank records after making online purchases, and 31% admit they do not always take steps to verify a website is legitimate before submitting credit card information (European Commission, 2012). More public awareness needs to be brought to the attention of consumers, and government and businesses need to take charge in this front.

There are (at least) two main policy issues associated with identity theft with respect to consumers. First, who will bear the financial costs when an identity thief steals goods? Will it be the person whose identity is stolen, the merchant targeted by the thief, or a financial intermediary? A number of parties can take steps to reduce the prevalence of identity theft. Consumers can take additional care to make sure that their credit cards are not stolen or that they keep their information private. They can also monitor their accounts more closely to detect unauthorized charges more quickly (Anderson, Durbin, & Salinger, 2008). Of course, the steps each party will take to prevent identity theft depend on what liability that party faces if theft occurs. Generally, Canadian and United States law prevents consumers from being held responsible for more than $50 in fraudulent charges. However, most credit card issuers go beyond these protections and promise consumers zero liability for fraud, since fraud protection has become an important selling point both for the card associations and card issuers. For debit cards and for credit card billing errors, consumers face a version of negligence standard, where they generally have no liability for charges as long as they report the fraud within a specified time period (Anderson, Durbin, & Salinger, 2008). In effect, the liability rule provides an incentive for consumers to monitor accounts regularly, which is an important preventative mechanism for fraud. Ultimately, everyone needs to do their part in preventing identity theft and fraud, but consumers should not and do not bear most of the financial costs. Business and Government have to lead the identity theft battle, not consumers. Business practices cause many identity theft opportunities and may impede consumer recovery. Opportunities for identity theft often result from the implementation of technology to improve profitability. Businesses that handle sensitive personal information may not implement procedures required to protect this data.

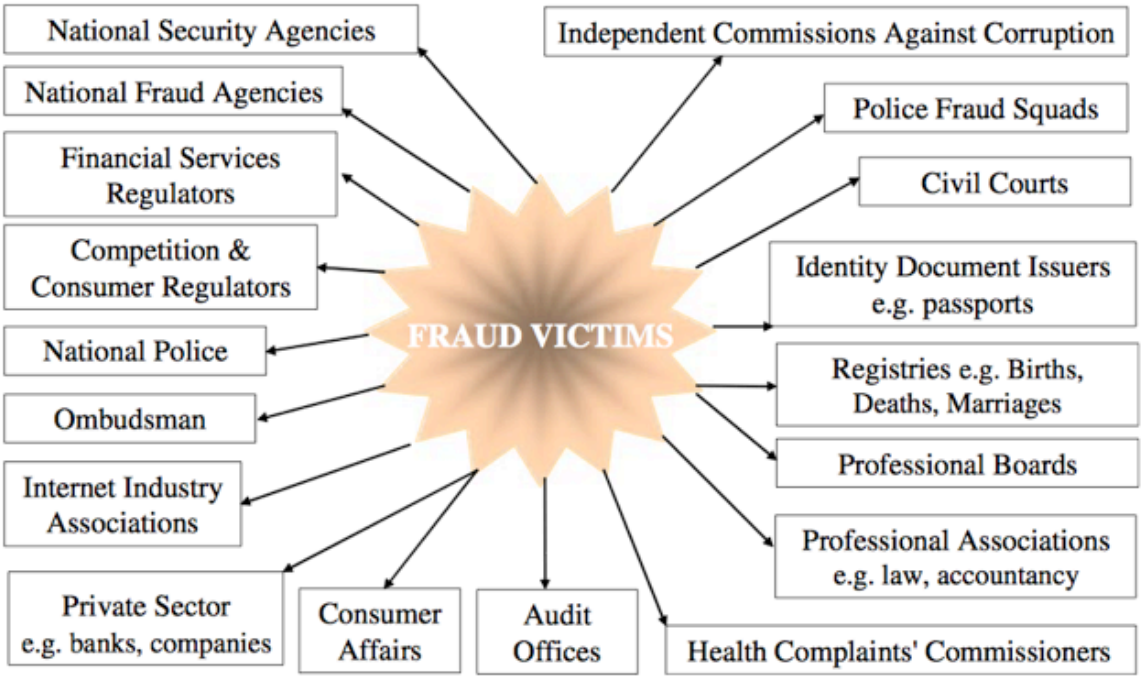
Second, what rights should consumers have to challenge or limit access to information about their identity and credit history? In Canada, if you have been a victim of identity theft or fraud, you are asked to contact the fraud departments of both credit bureaus (Equifax Canada Inc. and TransUnion Canada) and request a fraud alert be placed on your file. You should ask each agency to send you a copy of your credit report. You can also request a security freeze, preventing credit issuers from obtaining access to your credit files without your permission. This prevents thieves from opening up new credit cards. Credit freeze laws seek to increase consumers' ability to control their own risk of identity theft. Consumers bear some of the cost when thieves open up fraudulent accounts, and creditors and credit reporting agencies may not take this cost into account when using a consumer's credit report. Credit freeze laws give consumers the option of insisting on extra precautions, which may be burdensome for the consumer but can ensure that any potential consumer harm from issuing credit reports is taken into account (Anderson, Durbin, & Salinger, 2008). In terms of credit freeze laws (Canadian Consumer Initiative, 2008):

- Consumers should have a free credit freeze facility
- The consumer should be permitted to lift credit freezes with a special code for certain creditors either permanently or for a period of time
- Consumers should be notified of attempts to access credit reports or credit scores after a credit freeze has been issued
- Consumers should have a right to a credit report clean up where entries relating to fraudulently obtained credit are removed

As indicated in Sproule & Archer's 2008 study, identity theft and fraud is massively underreported. Fraud is not a national police priority, so even when reports are taken, little is done with them. Many victims therefore don't report at all, so the official crime statistics display just the tip of the iceberg, and developing a strategic law enforcement response is impossible because the information to target investigations does not exist. There are various strategies that could be developed to encourage greater reporting of identity theft and fraud and a nationally coordinated response would assist those who make the official reports, and enable information to be gathered which may assist in the development of improved fraud prevention strategies and interventions. If individual nations can develop a nationally coordinated response to fraud, then international sharing of information would also be facilitated (Smith, 2008).

When fraud victimization occurs, there are many avenues of response that may be followed – some obligatory under official policies and laws, and others depending on the scale and circumstances of the offense. However, fraud is not often reported officially and repeat-victimization tends to occur. Individuals or organizations may choose to go to the police, private lawyers to claim compensation, relevant corporations such as banks or insurance companies to seek redress, dedicated consumer complaint-handling bodies such as health care complaints commissioners, professional regulatory boards, or ombudsmen, associations and regulatory bodies such as those for lawyers or accountants, internet industry associations, or public sector organizations such as audit offices (Smith, 2008). Many of these are shown diagrammatically below.

Figure 4-1. Current Avenues of Complaint for Fraud Victims



Source: Smith, 2008

Knowing which avenue to pursue, and which procedures to follow pose difficult and complicated choices for everyone. Often a single case of identity theft may result in information being posted at federal, provincial, and municipal law enforcement agencies, credit reporting agencies, credit issuers, financial institutions, telecommunications companies, and regulatory agencies. This, in turn, leads to the inefficient 'stove-piping'

of relevant data and intelligence. Additionally, in many cases, agencies do not or cannot share information with other agencies, making it difficult to determine whether an identity theft complaint is related to a single incident or a series of incidents (Smith, 2008). To combat these problems, it would be beneficial to have a standardized electronic identity theft police report form and establish a central identity theft/fraud reporting agency. The United Kingdom has done this with the establishment of a so-called 'Identity Fraud Tsar', which coordinates the efforts of government, police, and the private sector in dealing with identity fraud (Smith, 2008). Canada has made progress in this front with the creation of the Canadian Anti-Fraud Centre (CAFC). The CAFC is the central agency in Canada that collects information and criminal intelligence on all forms of mass marketing fraud, including advance fee fraud letters (e.g. West African fraud letters), Internet fraud, identity theft complaints and others. The CAFC does not conduct investigations but provides valuable assistance to law enforcement agencies all over the world by identifying connections among seemingly unrelated cases (RCMP, 2012). Prior to the establishment of the CAFC, PhoneBusters and Reporting Economic Crime Online (RECOL) were the two national initiatives that aimed to combat fraudulent activities in Canada. PhoneBusters was a national anti-fraud call centre jointly operated by the Ontario Provincial Police and the RCMP and RECOL was a web-based crime-reporting system that allows Canadians to make complaints regarding suspected identity theft, fraudulent letter or telemarketing scams, and other white- collar crimes. The merging of RECOL and PhoneBusters formed the basis for the creation of the Canadian Anti-Fraud Centre (Public Safety Canada, 2006). That being said, more public awareness and emphasis needs to be placed on the CAFC being the central reporting agency in order for it to truly serve as that purpose. For example, the RCMP's website lists various reporting avenues consumers can take, rather than placing more emphasis on the CAFC being the main avenue for simplicity and consistency purposes. If a consumer chooses to report only to the police and credit card companies, and not report to the CAFC, then there may be a statistical loss of data if the police and credit card companies don't share the intelligence they received with the CAFC. This results in inaccurate identity theft/fraud statistics for further research purposes. Also, the multiple avenues of reporting listed on the RCMP's website might deter the consumer from reporting anything at all because of not knowing where to begin or feeling overwhelmed. Increasing the level of reporting of fraud would help to ensure that similar patterns of

offending by the same or other offenders are uncovered by police and that appropriate fraud prevention strategies may be identified and implemented. If the true nature of fraud remains undisclosed and uninvestigated, then it is difficult to devise appropriate measures to guard against it. The community may also suffer where crime has not been dealt with as incidents will not find their way into official crime statistics and the educative and deterrent effects of publicity in preventing crime will be avoided. Effective reporting may, instead, enhance the feeling in the community that fraud is, in fact, unlawful and likely to result in prosecution where it is detected (Smith, 2008).

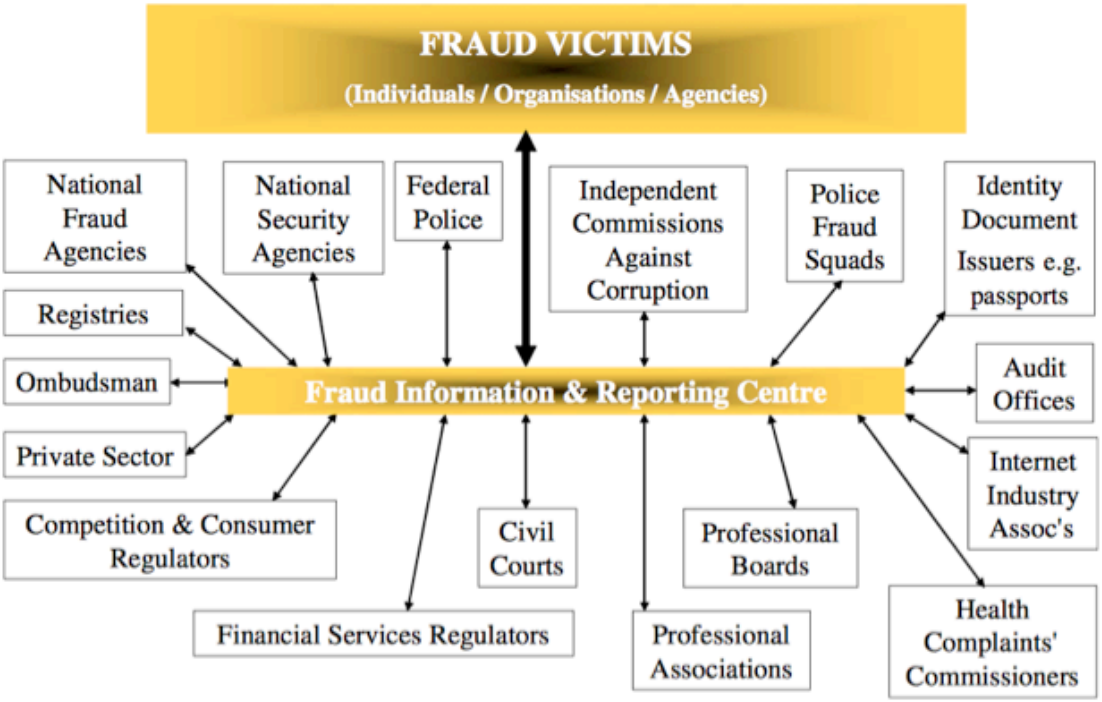
The main barriers to effective reporting, as identified in the literature, is as follows (Smith, 2008):

- Some victims may simply never realize they have been victimized
- In the case of online fraud, difficulties may arise in locating the offender who may be resident overseas or who may have used an anonymous re-mailing system in carrying out the fraud
- Often victims of economic crime may be unwilling to incur further time and expense in pursuing legal remedies
- Some businesses who have been victimized focus all their attention on re-instating systems quickly so as to prevent loss of business
- Some police departments are not yet identity theft victim friendly and simply do not have the resources to take action
- Lack of evidence
- Believe there is an immaterial amount involved
- Concern about costs and resources required to prepare complaint
- Concern about adverse publicity
- Believe that no progress will be made if reported
- Concern about the effectiveness of the criminal justice process in deterring the further incidence of fraud within the organization or within the community generally
- The experiences of fraud victims may also lead them to believe that it is impossible to recover losses through legal avenues

Other mechanisms to encourage reporting can include improving the use of whistleblower protection legislation and policies to protect individuals who report suspected fraud, creating and improving electronic systems to make reporting simple

and efficient, providing regular feedback to complainants about what is being done with their cases, enacting legislation to make it obligatory to report fraud in certain cases, and establishing and maintaining a central agency which would receive reports from all sources and which would coordinate investigatory action by sending reports to appropriate agencies (Smith, 2008). A diagram of a coordinated approach to fraud reporting is presented below to contrast Figure 4.1.

Figure 4-2. A Coordinated Approach to Fraud Reporting



Source: Smith, 2008

It is important to note that the adoption of a coordinated approach to reporting fraud, such as the establishment of a central reporting agency, would result in instances of fraud being reported more often. This has two implications. First, there may be a belief that the problem of fraud is increasing exponentially due to normally unreported crimes now being reported. Second, there may be an expectation that all the matters, which have been reported, will be investigated and will result in prosecution and punishment. The current systems in place for responding to fraud are still somewhat disparate and uncoordinated across the public and private sectors in Canada. When fraud has been reported, information needs to be kept in such a way that it can be used for risk

management and trend analysis purposes, and this should be done by the CAFC and coordinated with Statistics Canada. Hopefully, if fraud reporting were to increase, the actual incidence of fraud may be reduced once it becomes apparent that these crimes result in official action being taken.

4.2. Businesses/Organizations

Some experts in this research area believe that business and government, not consumers, must lead the battle on identity theft. Business practices cause many identity theft opportunities and may impede consumer recovery. Opportunities for identity theft often result from the implementation of technology to improve the corporate bottom line, and businesses that handle sensitive personal information may not be implementing procedures required to protect this data (Canadian Consumer Initiative, 2008). Businesses must limit collection of personal data to the minimum necessary for the purpose of the transaction. Expansive collection for potential secondary marketing purposes simply risks over-collection and subsequent data loss or risk abuse. Use of sensitive personal identifiers such as Social Insurance Numbers (SIN) and drivers license numbers (DLN) exacerbates this problem and provides identity thieves with greater opportunities to access victim's personal finances (Canadian Consumer Initiative, 2008). Business and government must realize that they hold personal information in trust for consumers. Identity theft due to their information holdings and handling practices is a real possibility and business and government must take steps to manage the risk. Simple changes to business models must be made immediately. Some examples include:

- Truncating credit card number receipts should be demanded by business of credit card debit card terminal suppliers
- Secure destruction of personal information holdings after appropriate hold periods
- Business should carefully check ID, should not give out account details to third parties, and should be extremely careful in extending credit
- Phasing out of reliance on SINs and DLNs is essential by businesses who unnecessarily obtain this information during business operations

- Consumers should be immediately notified when personal information leaks occur

Fraudulent acts against businesses in Canada can result in substantial losses to those directly affected by the crime, but these crimes also have an impact on all Canadians who rely on the products and services the businesses provide. In the past, official statistics on business fraud in Canada have been limited in that they only reflect incidents of fraud that come to the attention of police (Statistics Canada, 2006). The European Commission's 2012 study found that Canadian GDP costs of identity theft in 2011 totaled approximately 3 billion dollars or 0.14% of total 2011 GDP. Table 4.1 below displays these results in comparison to the United Kingdom, France, Australia, and the United States.

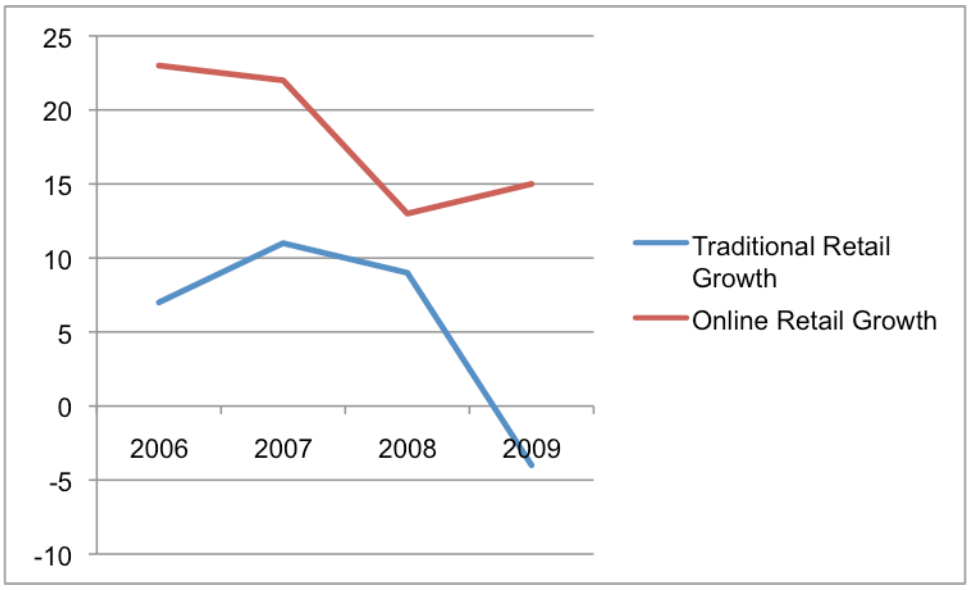
Table 4-1. GDP Costs of Identity Theft (2011)

Country	Costs (billion per year)	% of GDP (2011)
UK	3.132	0.11%
FR	0.722	0.02%
AUS (min)	1.219	0.07%
AUS (max)	5.487	0.31%
CAN	2.931	0.14%
US (max)	103.157	0.57%

Source: European Commission, 2012

Various studies have shown that identity theft is twice as likely to occur in English-speaking countries, given that English is the global language of business (Gorman, 2008). This would explain why France incurs less identity theft related costs compared to that of Canada and the United States. Identity theft is also strongly correlated to the number of users online. The United States ranks second worldwide in terms of Internet users, which would help explain why their identity theft related costs are twice as much compared to Canada (Internet World Stats, 2012). In addition to the economic and social impacts already identified earlier, identity theft has potentially serious implications for the digital market. The growing importance of e-commerce for the retail service sector in particular in recent years is illustrated in the following figure. The digital economy is growing, and as technology advances, so does the opportunities for cyber fraud and identity theft.

Figure 4-3. Traditional Retail Growth vs. e-Commerce Growth (Global)



Source: European Commission, 2012

Businesses are affected both as primary and secondary victims. A study done by the International Cyber Security Protection Alliance Ltd. in 2012 showed that cyber crime attacks conducted within that year resulted in total financial losses of approximately $5.3 million or $14.8 thousand per affected organization, on average, in Canada. Of this sum, financial fraud accounts for the largest portion (36%, $1.9 million, or $6.4 thousand per attack). The table below outlines these results in greater detail.

Table 4-2. Costs Incurred by Businesses Due to Cyber Crime Attacks

	Sum			Total Cost/Loss (A+B+C)	Average Cost Per Attack
	Financial Loss (A)	Cost of Recovery (B)	Loss of Business (C)		
Financial fraud	$1,162,553	$155,030	$575,100	$1,892,683	$6,438
Theft of devices containing company information	$215,700	$361,800	$271,999	$849,499	$4,007
Malware, such as Trojans, Worms, and Virus attacks	$283,475	$456,259	$32,203	$771,937	$454
Sabotage of data or networks	$347,499	$104,300	$131,499	$583,298	$5,952

	Sum			Total Cost/Loss (A+B+C)	Average Cost Per Attack
	Financial Loss (A)	Cost of Recovery (B)	Loss of Business (C)		
Telecommunications fraud	$178,200	$169,300	$153,000	$500,500	$1,209
Denial of Service	$50,000	$172,050	$11,700	$233,750	$1,067
Phishing, Spear Phishing, and Social Engineering	$123,135	$11,455	$17,445	$152,035	$103
Unauthorized access or misuse of website	$40,510	$50,599	$28,599	$119,708	$161
Advanced Persistent Threats (APTs)	$0	$100,300	$0	$100,300	$1,454
Misuse of social networks by employees	$39,299	$9,999	$16,098	$65,396	$113
Theft of other hardware	$42,300	$17,510	$0	$59,810	$1,031
Total Cost/Loss	$2,482,671	$1,608,602	$1,237,643	**$5,328,916**	

Source: ICSPA, 2012

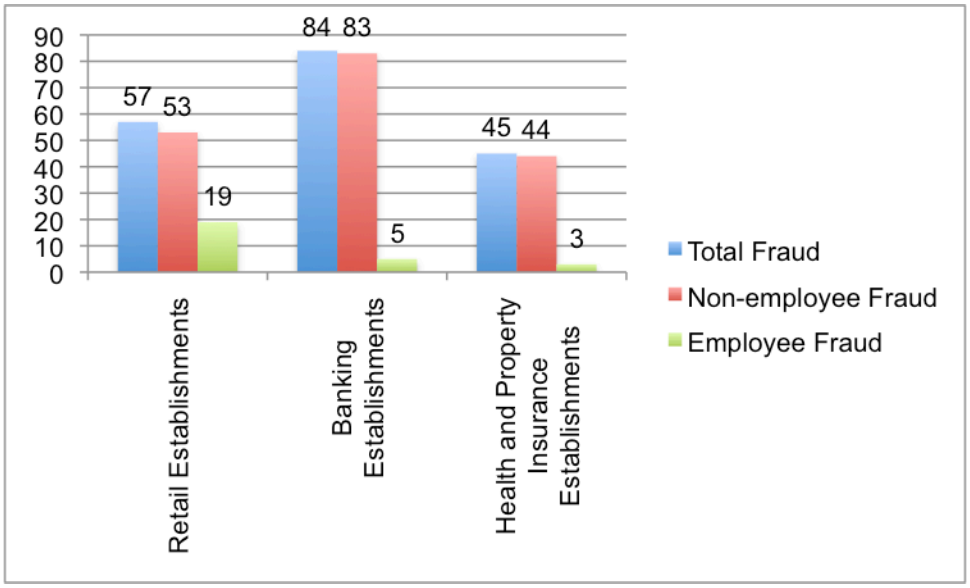
The ICSPA study also indicated that although a majority of respondents (64%) say that senior management takes cyber crime threats seriously, there are considerable gaps in Canadian businesses' preparedness against cyber crime. Large businesses are somewhat better prepared than medium and small ones, but still much remains to be done to prevent and deal with such attacks. The study presented the following facts (ICSPA, 2012):

- A majority (64%) employs just one or two ways to raise awareness of cyber crime in organizations, mostly through emails (59%) and corporate guidelines/ manuals (54%). Nearly one-in-five (19%) organizations do nothing to raise awareness of cyber crime, and this is more frequent among small organizations than medium and large ones
- Risk assessment processes are not common among surveyed businesses; only 22% employ them, and 77% do not. This behaviour holds across industries. The likelihood of employing such processes increases with revenues
- Few organizations (6%) report accreditation of IT security standards, and this percentage is equally low across industries and revenue levels
- Of those without accreditation, just over half (56%) say they carry out regular security audits. Regular audits also increase with revenues

- Most organizations (69%) do not have formal procedures in place to follow in the event of a cyber crime; only 28% do. Again, such procedures are more common in large businesses than in medium or small ones
- Similarly, only about a third (28%) has a trained crisis management team, and it is somewhat higher only among organizations with the largest revenues ($100 million or more), at 41%. Typically, senior management and senior/key IT security personnel (e.g., head of IT, CIO, IT director) would deal with any type of cyber crime incident. The same individuals would most likely make a decision to involve external agencies in the case of cyber crime attacks
- Canadian businesses have minimal awareness of the 2010 Cyber crime security strategy (7%)

A study done by Statistics Canada in 2008 showed that approximately half of retail and insurance business establishments surveyed, and approximately 84% of banking establishments, experienced some type of fraud in 2007. These results are displayed graphically below.

Figure 4-4. Percent of Business Establishments with Fraud



Source: Taylor-Butts & Perreault, 2008

Similar to the literature on consumers, businesses also have confusion as to which external agencies they would contact in the event of cyber crime attacks. Lastly, according to the ICSPA study, Public Safety Canada and the RCMP's roles in raising awareness of cyber crime is relatively low at only 12%. Businesses feel that the media (TV, news, newspapers, internet) should be the key element in the awareness building

strategy. Public Safety Canada and the RCMP are the appropriate organizations to serve as the main source of awareness, knowledge, and support in building awareness of cyber crime. They should also bring awareness to the Canadian Anti-Fraud Centre being the central reporting agency for these types of crimes. Businesses expect these two organizations to be more visible in fulfilling these roles. Mainstream media appears to be an effective choice for initial awareness building; however communication and outreach to businesses should go beyond mass media, reaching them with more targeted publications and messages. Statistics Canada's 2008 study also supports these claims since nearly half of retailers and insurance establishments never or rarely contact police when fraud is detected (Taylor-Butts & Perreault, 2008). Most often than not, fraud losses are considered too minor to warrant contacting police. There are multiple gaps in cyber crime preparedness among Canadian businesses, from a lack of trained personnel to a lack of strategies and procedures that could mitigate such attacks. Two factors could be responsible for this situation (ICSPA, 2012):

- The damage (financial or reputational) caused by cyber attacks have not been significant to merit shifts in attitudes and behaviour
- Organizations do not have enough awareness and knowledge of what strategies they should be implementing to minimize their vulnerability against such attacks

The Statistics Canada study identified the following suggested initiatives for the further prevention of fraud in businesses (Taylor-Butts & Perreault, 2008):

- Retail industry
  - Better employee and client training and awareness (60%)
  - Cooperation and exchange of information among businesses in the same industry (e.g. through networks, associations, conferences, etc.) (48%)
  - Partnerships between the police and businesses (44%)
  - A national fraud reporting centre that all victims could report to and that could be a source for businesses and the public to obtain information on fraud scams, prevention, etc. (36%)
- Banking industry
  - Cooperation and exchange of information among businesses in the same industry (e.g. through networks, associations, conferences, etc. (92%)
  - Better employee and client training and awareness (91%)

- Better public awareness and public information campaigns (76%)
- Investment in better detection and security technology (73%)
- Partnerships between the police and businesses (73%)

- Insurance industry
  - Cooperation and exchange of information among businesses in the same industry (e.g. through networks, associations, conferences, etc.) (74%)
  - Better public awareness and public information campaigns (61%)
  - Cooperation and exchange of information between all types of businesses (e.g. through networks, associations, conferences, etc.) (57%)
  - Better employee and client training and awareness (56%)
  - Partnerships between the police and businesses (56%)

The Canadian government, law enforcement agencies, and private sector organizations in Canada are making significant efforts in providing preventative information related to cyber crime to the public. Industry Canada and the Office of Consumer Affairs, Public Safety and Emergency Preparedness Canada, and the Royal Canadian Mounted Police all have websites and publications available to the public to educate them on cyber crime. These education campaigns need to continue and find new and creative ways to reach the public.

4.3. Law Enforcement Challenges

In Canada, the RCMP is responsible for the investigation of all computer crime offences within its jurisdiction, as well as those in which the Government of Canada is victimized, regardless of the source of the offender, as well as offences involving organized crime affecting the interests of Canada. Commercial crime sections of the RCMP operate in every major city throughout Canada and include at least one investigator trained in the investigation of computer crime (Smyth & Carleton, 2011). The RCMP High-Tech Crime Forensics Unit in Ottawa further supports these initiatives. However, as noted earlier, the anonymous nature of the Internet presents a significant problem for both law enforcement officials and victims because as many as half of victims do not know how their personal information was obtained (Smyth & Carleton, 2011). Offenders often mask their identities and are able to ‘loop’ or ‘weave’ their attacks

through servers located in multiple jurisdictions. Electronic impersonation, otherwise known as 'spoofing', can also help to obscure the attacker's identity, as do anonymous remailers, and the encryption of digital information. Therefore, official crime statistics about online fraud display just the tip of the iceberg, so developing a comprehensive and proactive law enforcement response is extremely difficult. Since the prerequisite to beginning any investigation is identifying the suspect, this is one of the greatest challenges with regards to solving this type of crime. A secondary challenge is the difficulty in identifying when, where, and how the victim's identity was compromised. An investigation needs to narrow down the possible circumstances that allowed the victim's identity to be compromised (CIPPIC, 2007).

According to police, criminals are increasingly using the Internet to engage in various elements of their crimes and to hide from law enforcement agencies. The Internet affords identity thieves a great deal of anonymity, especially for the more technologically inclined thieves who use botnets (i.e. software robots) to hide their tracks. When identity thieves use new technologies, it is difficult for law enforcement agencies to discern a pattern of activity by an individual or group of individuals engaged in large-scale identity theft. Many identity theft cases will therefore go un-investigated because the chances of catching identity thieves on the Internet are minimal in an unregulated borderless cyber space (CIPPIC, 2007). Cyber crimes evolve and advance as technology evolves and advances. Criminals will always find new ways to use the Internet to commit crimes, and so law enforcement needs to always remain one step ahead. For example, collecting evidence is another problem associated with online identity theft. The evidence will generally consist of IP addresses used in certain time frames, server logs and emails. Simply understanding the evidence requires a certain amount of technological knowledge. More on-going training and resources need to be provided to law enforcement agencies so they can be better equipped to tackle cyber crimes.

In addition, the lack of coordination in handling complaints, even between agencies within the same jurisdiction, poses significant problems because individual incidents can be relevant to a wide range of agencies and may result in information being recorded at federal, state/provincial, and local law enforcement agencies, as well

as credit reporting agencies, financial institutions, and regulatory agencies (Smyth & Carleton, 2011). This results in an inefficient backlog of relevant data and, given that many agencies do not coordinate and share intelligence, it is hard to tell if a complaint is linked to a single incident or to a series of incidents. In a recent internal audit of the RCMP's technological crime program, it was found that there existed a backlog that poses a serious risk to its work. The audit report identified that program managers are concerned that the number of requests for assistance and devices being analyzed by the program have been increasing each year (Bronskill, 2013). The report says the audit was undertaken in recognition of an increase in criminal activity involving computers and other electronic devices and cited a need to establish and implement clear strategic direction for the program. A senior RCMP officer commented that the technological crime program finds itself in a period of unprecedented global technological change during an era of austerity, effectively creating an extremely challenging operating environment (Bronskill, 2013). While the federal Cyber Security Strategy of 2010 provided money for administrative help, there was none for front-line investigators to address gaps in service delivery. These law enforcement programs need federal funding from Canada's Cyber Security Strategy of 2010 and a clear strategic direction implemented so proper resources and training can be utilized. There is no doubt that law enforcement budgets are shrinking, and given these budget reductions, cyber crime has fallen to be a lower priority for police, with most efforts directed at violent crimes such as robbery, murder, and sexual assault. Policing cybercrime is expensive and requires personnel whose training is constantly updated and newer equipment to examine the thousands of new gadgets released by manufacturers. There is simply no way the police can handle cyber crime by themselves. New and innovative models of public-private partnerships will be required if we are to have any hope of making an impact on newly emerging forms of technology crime.

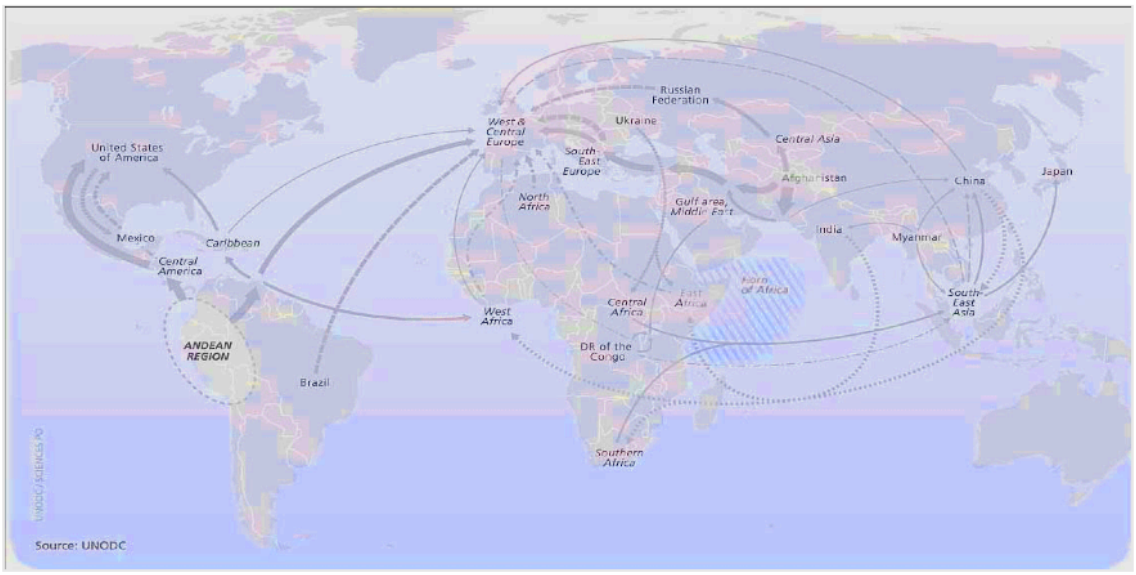
Another major challenge faced by law enforcement agencies is a lack of physical proximity. Unlike most physical crimes, there may be a large geographical separation between the victim and the identity thief. In an ordinary theft case, police can isolate the neighborhood and go door to door to talk to witnesses. In an identity theft case, traditional methodology no longer applies (CIPPIC, 2007). Identity theft does not respect local, provincial, regional or international borders and therefore locating and prosecuting

perpetrators becomes a very difficult task. The cross-border dimension of identity theft involves the following types of cases (European Commission, 2012):

- Situations where the perpetrator is based in one country and the victim in another
- A criminal acquires information and then transfers/sells it to a second criminal. (One or both of these criminals may be based in a different country than the victim)
- A criminal acquires information in one country and uses it in a second country

These are of course only examples and the cross-border dimension can take on many other forms. The typical identity theft crime involves at least three parties: the thief, the victim(s) and the defrauded institution(s). A credit card may be stolen in one city and then used in another city or, as is more often the case, online. Fraudulently purchased items may then be shipped to an address in yet another city. The thief is usually in a different jurisdiction than the victim, especially when personal information belonging to the victim was acquired via the Internet. The defrauded institution, such as a bank, might be headquartered in yet another jurisdiction (CIPPIC, 2007). In such a scenario, law enforcement agencies must deal with multiple jurisdictions, which may have completely different laws or legal systems. Some businesses might refuse to provide information to law enforcement agencies from other jurisdictions unless they are served with search warrants or similar judicial instruments (CIPPIC, 2007). The United Nations Office on Drugs and Crime (UNODC) carried out a threat assessment of transnational organized crime in 2010, which also included identity theft. The diagram is presented below and shows the flows of crimes related to identity theft and involving organized crime.

Figure 4-5. UNODC Threat Assessment of Identity Theft



Route

Vector:	Internet
Location of perpetrators:	Both developing and developed countries

Dimensions

Annual market volume:	About 1.5 million victims globally
Annual value:	About US$1 billion globally

Offenders

Groups involved:	Data acquisition is primarily an individual activity; "cashing out" may involve organized groups

Source: UNODC, 2010

As is shown in the figure, flows from developing and emerging countries (South America, Africa, and South-East Asia) primarily target Western countries (USA, Canada, and Europe). It is not clear from the source whether the flows refer to the acquisition of identity data and/or the secondary crime (European Commission, 2012). Thus, the international community has begun to realize the need for international cooperation on this issue. Uniformity in civil and criminal laws regarding identity theft is needed in order for the international community to function effectively within the Internet medium, especially since no entity currently controls the information that passes over the Internet. One important goal of international cooperation is uniformity. Uniformity is especially important in dealing with the Internet because international borders are practically invisible in this medium and it helps bring identity thieves to justice. Uniformity also aids

consumers and e-commerce participants by allowing for a degree of predictability in the kinds of laws and enforcement mechanisms available when an identity theft occurs over the Internet (Davis, 2003). However, international cooperation in combating identity theft is difficult because each nation or group of nations have different ideas about how to combat the issue, a different view of how much privacy invasion is allowed under a crime-fighting or civil litigation plan, and a different system for regulating and granting jurisdiction (Davis, 2003). For example, Europeans consider personal privacy to have the utmost importance, and commercial concerns are addressed as secondary to this primary issue. In the United States, however, the government has taken a more "hands-off" approach because of deeply ingrained laissez-faire economic attitudes. International cooperation faces the complicated task of balancing the competing needs of protecting consumers and encouraging e-commerce growth.

The Council of Europe Convention on Cybercrime is an example of international cooperation for fighting cyber crime and identity theft. In addition to criminalizing certain types of activities, the convention attempts to foster cooperation between countries in prosecuting such crimes. This convention aims to define computer crimes to promote uniform national legislation, common criminal procedures, and resources for cooperation on an international level (Davis, 2003). Four ways to foster international cooperation on identity theft have been identified:

1. Global treaty
2. Formal body to coordinate enforcement
3. Formal body to try crimes
4. Cooperation and compromise

One major step toward uniformity and prevention of identity theft over the Internet is the creation of a truly global treaty on the subject. The Council of Europe Convention on Cybercrime is an important step in this direction. It is a workable agreement, assuming that it actually will be expanded to include other parts of the world as well as crime specific laws and civil remedies dealing with data protection and identity theft. Secondly, the participating nations must make a formal coordinated effort to resolve the enforcement and jurisdictional issues involved in identity theft over the Internet. Thirdly, another step that an international coordinated effort may need to explore is the creation

of a formal body to try major identity theft crimes on an international level. An existing tribunal to try such issues could be expanded or a new tribunal to handle such cases could be created. Either way, this will cost the international community a great deal of time and money. One possible solution is that those countries that agree to use the new or updated tribunal as the forum for international identity theft disputes could bear the burden of funding such a venture. Lastly, in dealing with the privacy issue, both sides will have to compromise before uniformity is possible. Nations must also re-examine the concept of sovereignty before full international cooperation over Internet issues is possible. Realistically, the feasibility of this happening is very minimal. Trust is an essential element of this redefined sovereignty and nations must earn the trust of others and learn to trust the judgments of others for international cooperation to truly become a reality. Unfortunately this is easier said than done in a post-9/11 world.

The fact is that there is only limited cooperation across national borders in matters of policing. While this certainly happens in some areas, such as narcotics trafficking, money laundering and the trade in child sexual abuse images, in many other areas, such as standard financial fraud and cyber crime, cooperation is far from robust. Criminals can take advantage of the lack of cooperation with significant transnational institutions capable of dealing with cyber crime in real time. The request of a police agency in one country to obtain evidence in another requires complex legal instruments for cooperation, such as the Mutual Legal Assistance Treaties (MLAT). Using an MLAT, it can often take up to two years to get evidence in a case from another nation. Clearly a two-year time frame is unworkable when IP logs and criminal evidence disappears in days, if not hours (Goodman, 2013).

4.4. Legislation

In contrast to Canada, many U.S. jurisdictions have passed legislation specifically aimed at preventing identity theft, assisting its victims, improving prosecution and conviction rates, and otherwise addressing its consequences. Both federal and state identity theft statutes exist and most were passed in recent years. With many bills awaiting approval, additional U.S. legislation in this area can be expected (CIPPIC, 2007). In addition to specific identity theft legislation, the United States has federal

statutes dealing with false identification, data protection, and credit, as well as other general statutes applicable to identity theft. Arizona was the first state to pass legislation recognizing identity theft as an independent crime (Newman and McNally, 2005). All 50 states have now enacted legislation making identity theft a misdemeanour or a felony offence. Anecdotal evidence suggests that state laws have been effective in increasing awareness of identity theft if not deterring the crime (Newman and McNally, 2005). Most identity theft prosecutions take place at the state level because federal prosecutors will generally not take a case that involves small amounts of money (Newman and McNally, 2005).

The federal Identity Theft and Assumption Deterrence Act of 1998 is a landmark in the evolution of United States identity theft legislation. It was the first statute to define identity theft and portray it as a violation of federal law (CIPPIC, 2007). This particular statute makes it easier to prosecute identity thieves because the definition is so broad (Federal Trade Commission, 2003). The statute defines personal information broadly, to include government-issued identifiers, such as Social Security and passport numbers, biometric information, and telecommunication and electronic identifiers (CIPPIC, 2007).

Along with federal legislators, state legislators have passed specific laws explicitly criminalizing identity theft (Robinson, Graux, Parrilli, Klautzer, & Valeri, 2011). California is a leader state in developing an innovative legal framework to combat this crime, and is often used as a framework for other states (CIPPIC, 2007). The California Penal Code contains an identity theft-specific provision. This provision also covers corporate identity theft, which defines a “person” as “a natural person, firm, association, organization, partnership, business trust, company, corporation, limited liability company, or public entity” (California Penal Code). The California Penal Code gives identity theft victims the right to obtain information about any account opened in their name by an identity thief, upon presentation of a police report. The California Civil Code contains provisions requiring public agencies and businesses to notify California residents of any unauthorized access to their computerized personal information held by the agency or business. Californians also have the right to place a security freeze on their credit file, and have the right to obtain a copy of the police report on their identity theft case (California Civil Code).

The identity theft problem has created a host of new issues for the international law community because it can be perpetrated easily over the Internet (Davis, 2003). Uniformity in civil and criminal laws regarding identity theft is needed in order for the international community to function effectively within the Internet medium. No entity currently controls the information that passes over the Internet (Crane, 2001). International cooperation faces the complicated task of balancing the competing needs of protecting consumers and encouraging e-commerce growth (Davis, 2003). More importantly, differences in regulatory and jurisdictional concepts present another major obstacle to creating international cooperation on identity theft issues.

Identity theft is one of the fastest growing crimes in North America and legislation simply cannot keep up with the evolution of technology. Improvements have been made in Canada; identity theft specific laws have started being put in place within the Criminal Code. One major concern today is data breach laws, since only Ontario's Personal Health Information Protection Act unequivocally requires organizations to notify members of the public if their personal information has been compromised (Edwards, n.d.). Most consumers who have been victims of identity theft crime have no idea how it happened. Some do not learn that their personal information has been misused for a considerable time, and usually only find out when they are notified by law enforcement or by a private sector agency. Consequently, dissemination of information about identity crime to Canadians is a critical element of prevention (RCMP, 2013). Just recently, Target stores in the United States were hit by a data security breach affecting forty million debit and credit card accounts and the personal information of seventy million customers (The Canadian Press, 2014). The breach occurred over the holiday season so Canadians may also have been impacted if shopping south of the border during that time. Data thefts at Target and luxury retailer Neiman Marcus Group LLC have rekindled enthusiasm in policy makers in Canada and the United States for a single federal law on how customers should be notified about such breaches. Prompt notification to consumers in these cases can help them mitigate the damage caused by identity theft.

There are two major rationales for these laws. First, notification can transform private information about firm practices into publicly known information as well as change practices within the firm (Romanosky, Telang & Acquisti, n.d.). Hence, by

highlighting an organization's poor security measures, legislators hope to create an incentive for all organizations (even those that have not been breached) to improve the protection of their data. This, in turn, is expected to reduce the probability of breaches and resulting harm, including identity theft. Second, consumers have a right to know when their personal information has been compromised at the hands of business operations. Having been notified of a breach of their personal information, consumers will make informed decisions and take appropriate actions to prevent or mitigate the impact of identity theft. Notifications can also enable law enforcement, researchers, and policy makers to better understand which firms and business sectors are better (or worse) at protecting consumer and employee data (Romanosky, Telang & Acquisti, n.d.). Therefore, we can expect two effects from these laws: increasing consumer precautions, and increasing organizational precautions to avoid breaches. To be clear, data breach disclosure laws are meant to influence safety and protection measures by both organizations and potential victims of identity theft, rather than criminal behavior. Arguments presented against using these mandatory security-breach laws include the following (Romanosky, Telang & Acquisti, n.d.):

- If the probability of suffering identity theft following a data breach is very low, then costs incurred as a result of the laws would be unwarranted (Firms would be forced to notify consumers without benefit, and consumers would be needlessly freezing and "thawing" their credit reports)
- Consumers may become desensitized if they receive too many notices
- These laws might impede e-commerce and stifle technological development by discouraging firms to innovate using consumers' personal information (or stop collecting it altogether)
- Negative influences on business and stock prices for the organization after disclosure of a breach

Nonetheless, a study conducted by Romanosky, Telang, and Acquisti showed that the adoption of these disclosure laws reduce identity thefts, on average, by 6.1 percent. As information security and privacy concerns rise, we will increasingly see legislation used as a tool for consumer protection, generating policy debates and significant lobbying. Clearly, it appears that the effectiveness of data breach disclosure laws relies on actions taken by both firms and consumers. Firms can improve their controls; however, once notified, consumers themselves are expected to take

responsibility to reduce their own risk of identity theft (Romanosky, Telang & Acquisti, n.d.).

Identity theft has attracted the attention of several of Canada's privacy commissioners. The Ontario's Information and Privacy Commissioner recently published a white paper calling for embedding privacy rules in online identification systems in order to minimize breaches. The "7 Laws of Identity" identified in this paper are as follows (Edwards, n.d.):

1. ID systems should not collect, use, or disclose ID without a user's consent
2. ID systems should minimize the amount of personal identification collected
3. ID systems should share personal information only as necessary and as little as possible
4. Universal online ID systems should support a range of identifiers with varying degrees of observability and privacy appropriate to the intended use and relationship
5. Universal online ID systems should be technologically neutral and not require a particular vendor's proprietary technology
6. Online ID systems should be easy for users to understand
7. Universal online ID systems should have a simple, consistent user interface

To add to these "7 Laws of Identity", security research suggests that for a positive identification, elements from preferably two, or even better, all three, factors of authentication should be verified. These factors of authentication include the following (European Commission, 2012):

- **Ownership factor**: Something the user has (i.e. a wrist band, ID card, security or software token, or a telephone)
- **Knowledge factor**: Something the user knows (i.e. a password or a pass phrase, a PIN number, a "challenge response" whereby the user must answer a question, etc.)
- **Inherence factor**: Something the user is or does (i.e. unique identifiers such as fingerprint, retinal DNA sequence, pattern, face, voice, signature, or other biometric identifiers)

The rationale for adopting specific legislation for identity theft was to, on the one hand, to provide support to victims and, on the other hand, act as a deterrent against this type of crime by making it a criminal offense. Prior to criminal legislation, citizens had the possibility to sue the offender(s) in civil court in order to obtain restoration of damage. This option is still very much open to victims of identity theft. However, identity theft is a criminal offence and therefore, criminal sanctions are necessary for a just society to operate. The European Commission's study on identity theft provided a brief comparison between the advantages and disadvantages of criminal and civil recourse, which is identified in the table below.

Table 4-3. Advantages and Disadvantages of Civil and Criminal Recourse

Type of Recourse	Advantages	Disadvantages
Criminal Recourse	• Penalties available (fines/imprisonment) may be a more effective deterrent • Demonstrates that the conduct is sanctionable in wider social terms as distinct from being a mere personal wrong • More possibilities may exist for cross-border cooperation between police and judicial authorities	• Always an element of discretion in whether a prosecution is undertaken by the police or public prosecutors • Higher standards of legal proof may make successful conviction more difficult • It may be more difficult to compensate the primary victim
Civil Recourse	• Initiative to take action remains with the person affected • Pecuniary compensation may result from successful judgment • Interim measures may be more easily available (i.e. injunctions)	• The risk of legal costs to the victim • The likelihood the proceedings will be more time-consuming and burdensome to the victim • Difficulty in proving degree of loss/damage in some cases

Source: European Commission, 2012

4.5. Analysis Summary

Table 4-4. Summary of Analysis Findings

Consumers/Individuals	• Two main policy issues: 1) Who bears the costs when an identity thief steals goods – primary victim, secondary victim, or financial intermediary? 2) What rights should consumers have to challenge or limit access to information about their identity and credit history? • Consumers are expected to take reasonable precautions to prevent identity theft and the steps each party takes to prevent identity theft directly correlates to liability • Ultimately everyone needs to do their part in preventing identity theft and fraud, but consumers should not and do not bear most of the financial costs • Businesses and government have to lead the identity theft battle, not consumers • Credit freeze laws seek to increase consumers' ability to control their own risk of identity theft • Consumers should have a credit freeze facility • The consumer should be permitted to lift credit freezes with a special code for certain creditors either permanently or for a period of time • Consumers should be notified of attempts to access credit reports or credit scores after a credit freeze has been issued • Consumers should have a right to a credit report clean up where entries relating to fraudulently obtained credit are removed • Identity theft is massively underreported because consumers do not have a central reporting agency to report identity theft and related crimes • Consumers feel the reporting mechanisms currently in place to report identity theft and related crimes are too tedious, time consuming, and confusing
Businesses/Organizations	• Business and government, not consumers, must lead the battle on identity theft • Business practices cause many identity theft opportunities and may impede consumer recovery • Businesses are affected both as primary and

	secondary victims • Truncating credit card number receipts should be demanded by business of credit card debit card terminal suppliers • Secure destruction of personal information holdings after appropriate hold periods • Business should carefully check ID, should not give out account details to third parties, and should be extremely careful in extending credit • Phasing out of reliance on SINs and DLNs is essential • Consumers should be immediately notified when personal information leaks occur because of business operations
Law Enforcement Challenges	• Anonymity of criminals • Lack of coordination in handling complaints • Lack of physical proximity • Lack of uniformity in civil and criminal laws within the international community
Legislation	• Need for credit freeze laws • Need for security breach disclosure laws

Chapter 5. Policy Objectives and Options

5.1. Policy Objectives

Table 5-1. Policy Objectives

General Objectives	Specific Objectives
• To combat identity theft, identity fraud, and identity related crime • More generally, to promote security, combat crime, and protect victim's rights	• To reduce identity theft and related crime • To improve the capacity to prevent and tackle identity theft and related crime both in public and private sectors, including in relation to cross-border aspects of the problem • To ensure that primary and secondary victims of identity-related crime obtain support and redress • To protect business, in particular SMEs, which tend to be more vulnerable to identity theft and its consequences than larger organizations • To improve the knowledge base regarding identity theft, fraud, and related crime • To ensure legislation evolves as technology evolves • To utilize non-legislative intervention to combat identity theft, fraud, and related crime

Table 5-2. Overview of Policy Options

Policy Option	Sub-Options
1. Status Quo	• Further research • No legislative or non-legislative intervention required at this time
2. Non-legislative Intervention	• 2.1: Increase resources dedicated to combat cyber fraud in law enforcement agencies and businesses (including on-going education and training programs) • 2.2: Establish a central reporting/statistical agency for identity theft and fraud • 2.3: Improve/establish more sophisticated information sharing networks
3. Legislative Intervention	• 3.1: Update credit freeze and security breach disclosure laws • 3.2: Establish a national/international common standard definition of identity theft • 3.3: Establish international cooperation and partnerships
4. Combined Intervention	• Combination of non-legislative and legislative intervention without the international dimensions (2.1, 2.2, 2.3, 3.1, and 3.2)

Below is a more detailed qualitative description of each of the policy options. More specifically, for each of the options described above, the following aspects are considered: the rationale for considering the policy option; content and scope; and timeframe for implementation.

Policy Option 1 – Status Quo

Rationale:

- The status quo policy option should always be considered, since the other options are compared against the baseline
- Before legislative and non-legislative intervention can take place, more research, surveys, and studies should be undertaken given that identity theft is difficult to prevent, detect, and prosecute since technology is the medium used to commit the crime

Content and Scope:

- Existing and planned initiatives, research, and studies at the national and international level in the field of identity theft, identity management systems, cybercrime, and cyberspace governance
- Focus is placed on intelligence gathering in the field of identity theft, identity management systems, cybercrime, and cyberspace governance before any action is taken to prevent and reduce identity theft

Timeframe:

- Ongoing

Policy Option 2 – Non-legislative Intervention

Rationale:

- The lack of resources assigned to combat identity theft and fraud is hindering investigations and creating major backlogs in enforcement agencies
- There is a lack of official reporting of identity theft and fraud from victims due to confusion of where to report the crime and which avenues are best suited for victims to take for efficiency and effectiveness
- The lack of information flow between enforcement agencies, businesses, and/or consumers is hindering investigations and is costing excess time and money

Content and Scope:

- More money from Canada's 2010 Cyber Security Strategy needs to be allocated to federal, provincial, and local law enforcement agencies to properly combat identity theft and fraud at the federal, provincial, and local levels
- More resources (personnel, equipment, technology, etc.) needs to be available to law enforcement agencies and businesses to properly combat identity theft and fraud
- Education and training programs need to be implemented in law enforcement agencies and in businesses to educate and train personnel on these types of crimes and on various preventative measures
- These education and training programs should be ongoing and should evolve just as technology advances and evolves
- The Canadian Anti-Fraud Centre (CAFC) is an excellent starting point for establishing a central reporting/statistical agency for identity theft and fraud
- The CAFC should be broadened to have the three-fold role of providing support to victims (serve as "one stop shops"), collect information concerning the problem of identity theft and partner with Statistics Canada for

maintaining official statistics and records, and drive awareness campaigns to educate the public on identity theft and ways to prevent oneself from being a victim of the crime

- This central reporting agency (CAFC) will be the main point of contact for all victims of identity theft and fraud and will be the only place victims need to go to report the crime
- The CAFC will help coordinate and assist police investigations
- The establishment of more sophisticated domestic and global information sharing networks will provide the requisite information for accurate validation, verification, and authentication
- Data sharing policies and standards should be established, along with accessible databases for law enforcement

Timeframe:

- 1-2 years for the establishment of a central reporting agency (expanding CAFC's role)
- 6-8 months for the development of solid education and training programs for personnel
- Education and training programs will be ongoing in law enforcement agencies and in businesses
- 3-5 years for establishing partnerships, policies, standards, and accessible databases for information sharing purposes

Policy Option 3 – Legislative Intervention

Rationale:

- The lack of coverage of primary and secondary victims in national legislation
- Limited awareness of the extent of identity theft and fraud
- Too much ambiguity and inconsistency in the definitions of identity theft and fraud domestically and globally
- Identity theft and fraud are cross-border crimes and therefore international cooperation is essential for effective and efficient criminal investigations

Content and Scope:

- Credit freeze and data security breach disclosure laws are the specific legislation in question that need to be established/modified

- Credit freeze laws are working successfully in the United States of America in the various states that have implemented this legislation
- Studies have been done on security breach disclosure laws and demonstrate that this type of legislation has been proved to reduce identity theft and fraud
- Credit freeze legislation:
    - Consumers should have a free credit freeze facility
    - The consumer should be permitted to lift credit freezes with a special code for certain creditors either permanently or for a period of time
    - Consumers should be notified of attempts to access credit reports or credit scores after a credit freeze has been issued
    - Consumers should have a right to a credit report clean up where entries relating to fraudulently obtained credit are removed
    - Businesses and credit bureaus should educate consumers on the central role of the credit bureaus in detecting and preventing loss through identity theft
- Data breach security legislation:
    - Law requires "an agency, or a person, or business that conducts business in Canada, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of Canada whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." In addition the law would permit delayed notification "if a law enforcement agency determines that it would impede a criminal investigation." The law would also require any entity that licenses such information to notify the owner or licensee of the information of any breach in the security of the data
- There should always be an ongoing review of Canadian cyber fraud legislation since technology is always advancing and evolving

Timeframe:

- The timeframe that a bill becomes a law varies in Canada, and depends on whether or not there is a majority or minority government and depends on the piece of legislation itself
- It is also hard to determine when a common standard definition will be decided upon at a national and international level (this could take years)

Chapter 6. Criteria and Measures

This section provides an assessment of impact of the various policy options based upon various criteria and measures. The expected impacts have been rated in relation to the status quo. At the end of this section, the ratings of the policy options are compared. The framework for assessing the impacts is structured around the following criteria:

- *Effectiveness* – the degree to which the policy options are capable of achieving the policy objectives
- *Efficiency* – the input or effort required to achieve a given output, where the latter is determined by the policy objectives
- *Stakeholder Impact* – who is potentially affected by the policy options (i.e. consumers, businesses, government, law enforcement agencies, etc.)
- *Economic and Financial Impacts* – the extent to which different policy options are likely to reduce the negative economic/financial effects of identity theft/fraud
- *Feasibility* – the feasibility of the policy options includes considerations of the practical feasibility in implementing the policy option, including the likely support from stakeholders as well as enforcement considerations

The impacts of the policy options have been scored on a scale from -3 to +3 in terms of the expected changes compared to the status quo. To reflect this, Policy Option 1 – Status Quo has been scored with 0, since the other policy options are compared against the status quo situation. A rating of 0 implies that the other options would not result in any major change compared to the status quo. A negative rating implies that the option presented is expected to worsen in relation to the status quo. A positive rating implies that the option presented is expected to improve in relation to the status quo. The scale is measured as follows:

- -3: Large negative impact
- -2: Medium negative impact
- -1: Small negative impact

- 0: Neutral
- +1: Small positive impact
- +2: Medium positive impact
- +3: Large positive impact

*Policy Option 4 scores were weighted more heavily and multiplied by 3 since Policy Options 2 and 3 had three score-able categories each. The criteria and measures summary is presented in the table below.

Table 6-1. Criteria and Measures Summary

Criteria	Status Quo	Non-legislative Intervention			Legislative Intervention			Combined Intervention
	PO1	PO 2.1	PO2.2	PO2.3	PO3.1	PO3.2	PO3.3	PO4*
Effectiveness	0	+3	+2	+3	+2	+1	+3	+3 (x3)
Efficiency	0	+3	+3	+3	+2	+2	+3	+3 (x3)
Stakeholder Impact	0	+3	+3	+3	+1	+3	+3	+3 (x3)
Economic & Financial Impacts	0	+2	+1	+1	+3	+1	+3	+3 (x3)
Feasibility	0	+1	+2	+1	+1	+1	+1	+1 (x3)
Total Score	**0**	**12**	**11**	**11**	**9**	**7**	**13**	
Total Policy Score	**0**	**34**			**30**			**39**

Chapter 7. Impact Assessment of Policy Options

Based on the above summary, Policy Option 4 (combined non-legislative and legislative intervention – removing the international dimensions) is expected to have the most positive impacts in terms of reducing and tackling the problem. Below is an assessment of each of the policy options.

7.1. Policy Option 1 – Status Quo (Total Score: 0)

Before legislative and non-legislative intervention can take place, more research, surveys, and studies should be undertaken since identity theft is a relatively ambiguous phenomenon in contrast to other major crimes. In order for this option to be truly effective and efficient, more resources would need to be assigned by the federal government to properly research and study this crime. It would also be difficult to gather accurate statistical intelligence when there is a lack of reporting by victims. A central reporting agency would help reduce this problem. In other words, in order for further research to be beneficial, Policy Option 2 (non-legislative intervention) would need to be implemented. Therefore, Policy Option 1 (Status Quo) does not achieve any of the policy objectives outlined in Table 5.1, except perhaps “to improve the knowledge base regarding identity theft, fraud, and related crime”, but not even to its full potential. Maintaining the status quo is not perceived as an appropriate option. Identity theft and fraud are expected to grow and evolve due to all of the available data online and increased sophistication of criminal schemes. Therefore, the assessment suggests that some form of intervention may be needed to help prevent and tackle identity theft and related crime. Since this option is the status quo, it is scored as neutral, or having neither a positive or negative impact.

7.2. Policy Option 2 – Non-legislative Intervention (Total Score: 34)

7.2.1. Policy Option 2.1 – Increase resources dedicated to combat cyber fraud in law enforcement agencies and businesses (including on-going education and training programs) (Score: 12)

There exists an inefficient backlog of identity theft cases in many law enforcement agencies. There is recognition of an increase in criminal activity involving computers and other electronic devices and these law enforcement agencies cite a need to establish and implement clear strategic direction for cyber crime programs. Some of these technological crime programs find themselves in a period of unprecedented global technological change during an era of austerity, effectively creating an extremely challenging operating environment. While the federal Cyber Security Strategy of 2010 provided money for administrative help, none was allocated for front-line investigators to address gaps in service delivery. These law enforcement programs need federal funding and a clear strategic direction implemented so proper resources and training can be provided and utilized.

(i) Effectiveness (Score: +3)

Increased resources dedicated to combat cyber fraud in law enforcement agencies and businesses would be highly effective to achieve all of the objectives outlined in Table 5.1. More resources would eliminate the major backlog that is currently accruing in law enforcement agencies and would assist the prosecution of more criminals in a timely manner. Law enforcement personnel would be better trained in this area of crime, which would result in more effective investigations. The capacity and capabilities of our agencies, particularly law enforcement agencies, needs to keep pace with evolving technologies if police are to perform their duties in the digital environment. At the most basic level, all police officers need to know how to gather and analyze digital evidence, leaving specialist units to focus on more complex cybercrimes. Specialist units within law enforcement agencies must have the training and capabilities to detect and investigate the more complex and sophisticated use of technology in criminal activities. Enforcing businesses to have specific mandatory preventative mechanisms and

resources in place would also effectively reduce identity theft and related crime. This policy sub-option is scored as having a large positive impact for effectiveness.

(ii) Efficiency (Score: +3)

Increased resources dedicated to combat cyber fraud in law enforcement agencies and businesses would be highly efficient to achieve all objectives outlined in Table 5.1. With more resources assigned to law enforcement agencies, investigations can be much more efficient in achieving quicker results. With more resources allocated to businesses, these measures can be highly efficient in preventing major security breaches, therefore resulting in reduced identity theft cases. This policy sub-option is scored as having a large positive impact for efficiency.

(iii) Stakeholder Impact (Score: +3)

Increased resources dedicated to combat cyber fraud in law enforcement agencies and businesses will have a direct impact on all major stakeholders of identity theft: consumers, businesses, law enforcement agencies, and government. More resources for law enforcement and government agencies will allow personnel to do a more thorough job of tackling this type of crime, which then impacts consumers. Consumers will be able to report their crime in a timely manner with full confidence that something will be done about it. Businesses are also directly impacted with increased resources and can effectively and efficiently help reduce and eliminate data breaches. With more resources, consumers are also better informed of this type of crime and better informed of ways they can prevent themselves from becoming victims or the steps to take in situations if they do become a victim of identity theft or fraud. With regards to stakeholder impact, this policy sub-option is scored as having a large positive impact.

(iv) Economic and Financial Impacts (Score: +2)

Increased resources dedicated to combat cyber fraud in law enforcement agencies and businesses have a moderately positive impact with reducing the costs of identity theft for victims. More resources will allow law enforcement officials to investigate crimes more effectively and efficiently, which will limit the financial and social costs on victims due to a quicker turnaround. More resources also mean better

preventative mechanisms in place within businesses, which will eliminate the negative financial costs of the crime altogether if it does not take place. Therefore, this policy sub-option is scored as having a medium positive impact in terms of the economic and financial impacts of identity theft.

(v) Feasibility (Score: +1)

Increased resources dedicated to combat cyber fraud in law enforcement agencies and businesses have low feasibility, given that resources are quite costly and law enforcement budgets are shrinking. Cyber crimes are not the only type of crimes, and therefore, priority needs to be given to crimes with the greatest impact on society. Due to the lack of research and knowledge of cyber crime, identity theft and related crimes are unfortunately put on the backburner at times and are not a national police priority. This policy sub-option is scored as having a small positive impact in terms of feasibility.

7.2.2. Policy Option 2.2 – Establish a central reporting/statistical agency for identity theft and fraud) (Score: 11)

As indicated in Sproule & Archer's 2008 study, identity theft and fraud is massively underreported. A nationally coordinated response would assist those who make the official reports, and enable information to be gathered which may assist in the development of improved fraud prevention strategies and interventions. If individual nations can develop a nationally coordinated response to fraud, then international sharing of information would also be facilitated. When fraud victimization occurs, there are many avenues of response that may be followed – some obligatory under official policies and laws, and others depending on the scale and circumstances of the offence. However, fraud is not often reported officially and repeat-victimization tends to occur. There are too many reporting avenues to take, therefore the establishment of a central reporting agency has been suggested to take the lead on identity theft and related crime. The CAFC has been recommended to take on this role. The goal of the adoption of a coordinated approach to reporting fraud, such as the establishment of a central reporting agency, would hopefully result in instances of fraud being reported more often. However, this has two implications. First, there may be a belief that the problem of fraud is

increasing exponentially due to normally unreported crimes now being reported. Second, there may be an expectation that all the matters, which have been reported, will be investigated and will result in prosecution and punishment. The current systems in place for responding to fraud are still somewhat disparate and uncoordinated across the public and private sectors in Canada. When fraud has been reported, information needs to be kept in such a way that it can be used for risk management and trend analysis purposes, and this should be done by the CAFC and coordinated with Statistics Canada. Hopefully, if fraud reporting were to increase, the actual incidence of fraud may be reduced once it becomes apparent that these crimes result in official action being taken.

(i) Effectiveness (Score: +2)

The effectiveness of a central reporting agency has a positive-medium impact on the objectives outlines in Table 5.1. A major barrier to determining the extent of the identity fraud threat is the absence of a centralized information collection and sharing mechanism for incidents of identity theft and fraud. The CAFC would prove to be an effective model for the development of this nationally centralized agency since it has already been established and is already proving to be effective. Its role would simply need to be expanded and more centralized. A central reporting agency may be effective in improving the number of complaints received or coordinating law enforcement efforts, but it might not be directly effective in reducing the amount of identity theft and related crime. It would be more of an administrative/coordinative mechanism and will lead to more effective investigations of criminal offences relating to identity theft. Therefore, since it only achieves most but not all objectives outlined in Table 5.1, this policy sub-option has been scored as having a medium positive impact on effectiveness.

(ii) Efficiency (Score: +3)

The establishment of a central reporting agency for identity theft and related crime is highly efficient given that it would be an administrative/coordination mechanism. Victim reporting would become more efficient in one centralized place, coordination of police investigations would become more efficient given that all the needed intelligence is in one central location, and public awareness campaigns would be more efficient being driven out of a central one-stop shop. This policy sub-option has been scored as having a large positive impact on efficiency.

(iii) Stakeholder Impact (Score: 3)

The establishment of a central reporting agency for identity theft and related crime directly impacts all stakeholders. It would be a central reporting agency for victims to report crimes, and is a central intelligence database for law enforcement agencies and government. All stakeholders of this crime would benefit from having this established. Therefore, stakeholder impact is scored as having a large positive impact.

(iv) Economic and Financial Impacts (Score: +1)

The establishment of a central reporting agency is meant to streamline the reporting and intelligence gathering process of the crime of identity theft and related crime. It does not, however, have much direct impacts in reducing the negative economic and financial costs of the crime. Therefore, this policy sub-option has been scored as having a small positive impact with regards to the economic and financial impacts of identity theft.

(v) Feasibility (Score: +2)

Given that the CAFC has already been established, feasibility of expanding its role and purpose will not be too difficult. It will still take plenty of time, resources, and funding to complete this daunting task. It will take time before all stakeholders are familiar with the new system and will take time until the new system is operating effectively and efficiently. Therefore, this policy sub-option is scored as having a medium positive impact in terms of feasibility.

7.2.3. Policy Option 2.3 – Improve/establish more sophisticated information sharing networks (Score: 11)

The establishment of sophisticated domestic and global information sharing networks will provide the requisite information for accurate validation, verification, and authentication. Comprehensive policies and regulations must be developed to define how personal information and records can be shared, who can have access to them, and under what circumstances they can be shared. Specialized domestic and global commercial, private, and government databases must be made available or created. The

CAFC would be a good place to start, considering it has been recommended that it be the central reporting agency for identity theft and related crime. These databases must provide personal identifier records that can be accessed by concerned entities, without jeopardizing privacy or the security of the data, and at the same time reducing liability and providing indemnification. This will require numerous agreements among governments, governments and the private sector, and private sector organizations. Global data collection and information sharing is a more challenging task relative to national data collection and information sharing. Public-private partnerships should be formed to help acquire or gain access to global data, especially data from the riskiest parts of the world, to help protect borders and promote commerce. Trusted information sharing systems need to be developed that will effectively and efficiently authenticate identity, while maintaining the privacy and security of personal identifier information. There must be an oversight committee to monitor the use of such a system to ensure accountability.

(i) Effectiveness (Score: +3)

Identity theft is a cross-border crime, and therefore information flow is essential. The establishment of sophisticated domestic and global information sharing networks will prove to be highly effective at preventing identity theft, reducing identity theft, and prosecuting identity theft criminals (European Commission, 2012). Information sharing also leads to effective criminal investigations. This policy sub-option will be highly effective at achieving the policy objectives outlined in Table 5.1 (European Commission, 2012), and is therefore scored as having a large positive impact.

(ii) Efficiency (Score: +3)

The establishment of sophisticated domestic and global information sharing networks will prove to be highly efficient at preventing identity theft, reducing identity theft, and prosecuting identity theft criminals (European Commission, 2012). To efficiently prevent and reduce identity theft, while simultaneously providing support to victims, information sharing is an essential part of criminal investigations and the collection of intelligence. Therefore, this policy sub-option is scored as having a large positive impact with regards to efficiency.

(iii) Stakeholder Impact (Score: +3)

The establishment of sophisticated domestic and global information sharing networks impacts all major stakeholders of identity theft and related crime. Information needs to be constantly flowing between all involved parties, and therefore establishing these sophisticated systems and networks will help facilitate this. More specifically, a website or electronic platform could be established and divided into three main parts:

- Part 1 – for individuals/businesses, where contact details for reporting mechanisms (i.e. the CAFC) are provided in an easily understandable format. This part of the website would be open to all.
- Part 2 – for experts/law enforcement agencies, where legislation would be provided with a more technical focus, as well as information on relevant actors working in the field. A closed community for sharing information real time and good practices would be established. Information could also be shared on risks. This section of the website could be based on registration.
- Part 3 – would serve as an electronic library with public reports containing statistics etc. It would be possible to upload reports and thereby create an online knowledge centre.

The CAFC would be a perfect choice for this platform. This policy sub-option is scored as having a large positive impact on stakeholders.

(iv) Economic and Financial Impacts (Score: +1)

The establishment of sophisticated domestic and global information sharing networks wouldn't directly result in negating the costs of identity theft. It rather serves the purpose of creating a knowledge and intelligence-sharing platform. Indirectly, it would help reduce identity theft and related crime, therefore reducing these economic and financial impacts down the line. This is why this criterion was scored as having a small positive impact.

(v) Feasibility (Score: +1)

The sub-option of establishing sophisticated domestic and global information sharing networks has relatively low feasibility, but is not impossible given the right mechanisms. Specifically with respect to global information sharing, feasibility is more complicated given the difficulty of establishing international relations and trust. Even domestically, many organizations have issues sharing intelligence and with plenty

of hurdles to jump through. This sub-option would take time and a lot of patience and trust in order to work effectively and efficiently, and is scored as having a small positive impact.

7.3. Policy Option 3 – Legislative Intervention (Total Score: 30)

7.3.1. Policy Option 3.1 – Update credit freeze and security breach disclosure laws (Score: 9)

Credit freeze laws seek to increase consumers' ability to control their own risk of identity theft. Consumers bear some of the cost when thieves open up fraudulent accounts, and creditors and credit reporting agencies may not take this cost into account when using a consumer's credit report. Credit freeze laws give consumers the option of insisting on extra precautions, which may be burdensome for the consumer but can ensure that any potential consumer harm from issuing credit reports is taken into account. In terms of credit freeze laws in Canada:

- Consumers should have a free credit freeze facility
- The consumer should be permitted to lift credit freezes with a special code for certain creditors either permanently or for a period of time
- Consumers should be notified of attempts to access credit reports or credit scores after a credit freeze has been issued
- Consumers should have a right to a credit report clean up where entries relating to fraudulently obtained credit are removed

Another major concern with legislation relating to identity theft is data breach laws, since only Ontario's Personal Health Information Protection Act unequivocally requires organizations to notify members of the public if their personal information has been compromised. Most consumers who have been victims of identity theft crime have no idea how it happened. Some do not learn that their personal information has been misused for a considerable time, and usually only find out when they are notified by law enforcement or by a private sector agency. Consequently, dissemination of information about identity crime to Canadians is a critical element of prevention. Therefore, we can expect two effects from these laws: increasing consumer precautions, and increasing

business precaution in avoiding breaches. To be clear, data breach disclosure laws are meant to influence safety and protection measures by both organizations and potential victims of identity theft, rather than criminal behaviour.

Arguments presented against using these mandatory security-breach laws include the following:

- If the probability of suffering identity theft following a data breach is very low, then costs incurred as a result of the laws will be unwarranted
- Firms will be forced to notify consumers without benefit, and consumers would be needlessly freezing and "thawing" their credit reports
- Consumers may become desensitized if they receive too many notices
- These laws might impede e-commerce and stifle technological development by discouraging firms to innovate using consumers' personal information (or stop collecting it altogether)
- Negative influences on business and stock prices for the organization after disclosure of a breach

(i) Effectiveness (Score: +2)

Studies have been undertaken and the results show that these mandatory security-breach laws and credit freeze laws are quite effective in reducing identity theft. These laws have proven successful and effective in the United States. It should be noted that these pieces of legislation focus solely on post-criminal activity and do not necessarily prevent identity theft completely (especially when criminals feel they will not get caught). Therefore, this criterion was scored as having a medium positive impact, given that it achieves most, but not all, objectives outlined in Table 5.1.

(ii) Efficiency (Score: +2)

Similar to the effectiveness criterion, studies have been undertaken and the results show that these pieces of legislation are efficient methods of minimizing the financial and social costs of identity theft. The goal of any piece of legislation is to deter criminals from committing the offence. It does not efficiently prevent identity theft as it primarily focuses on post-crime measures, and is therefore scored as having a medium positive impact.

(iii) Stakeholder Impact (Score: +1)

This policy sub-option positively impacts victims, but has the potential to negatively impact businesses (i.e. stock prices, market influence, etc.), and has no direct relevance to the other stakeholders. In time, if proven successful, these pieces of legislation will eventually impact all stakeholders if it achieves all policy objectives. Therefore stakeholder impact is scored as having a small positive impact.

(iv) Economic and Financial Impacts (Score: +3)

Credit freeze and data security breach laws allow victims to act immediately and mitigate the financial risks of identity theft and fraud. The longer it takes for victims to take action, the greater the financial burden. These pieces of legislation directly impact the economic and financial costs of the crime, and therefore score as having a high positive impact.

(v) Feasibility (Score: +1)

There is uncertainty in the passage of any piece of legislation in Canada; enacting a law depends on whether or not there is a majority or minority government and depends on the piece of legislation itself. Therefore, this policy sub-option is scored as having a small positive impact in terms of feasibility.

7.3.2. Policy Option 3.2 – Establish a national/international common standard definition of identity theft (Score: 7)

One of the main issues with identity theft is the lack of clarity with its definition. In many nations there is neither a common terminology used to describe the phenomenon of identity theft (i.e. “identity theft”, “identity fraud”, and “identity-related crime”) nor a common legal definition of it. Another major concern with not having a commonly accepted definition of identity theft is the lack of consistency with the identification of primary and/or secondary victims within the definition itself. Some definitions focus solely on primary victims; whereas others go further to incorporate secondary victims. Without a clear definition, it is difficult for nations to propose and incorporate detailed legislation for this crime.

(i) Effectiveness (Score: +1)

Establishing a national/international common standard definition of identity theft will be effective for producing thorough and accurate legislation to combat the crime itself and all related sub-crimes. However, this is a small piece of the puzzle and it does not achieve all of the objectives outlined in Table 5.1. Also, agreeing on a common definition at the national level is difficult enough, at the international level even more so. Therefore, this criterion has been scored as having a small positive impact.

(ii) Efficiency (Score: +2)

Research shows that establishing a national/international common standard definition of identity theft would be an efficient way to establish thorough and detailed legislation that will deter and prosecute criminals of identity theft and related crime. It is an efficient way to ensure both primary and secondary victims of identity theft and fraud are incorporated and supported. This common definition would also help key players from an international standpoint given that there is a common framework established. Given that this policy sub-option achieves most, but not all policy objectives, this criterion is scored as having a medium positive impact.

(iii) Stakeholder Impact (Score: +3)

A national/international common standard definition of identity theft would directly impact all major and minor stakeholders of identity theft. The common standard definition would assist government and policy makers in identifying legislative gaps, and would ensure both primary and secondary victims are identified and supported. The common standard definition would also assist law enforcement agencies prosecute more easily, effectively, and efficiently. Therefore, this criterion is scored as having a large positive impact.

(iv) Economic and Financial Impacts (Score: +1)

A national/international common standard definition of identity theft would not have much direct impact on negating the economic and financial impacts of identity theft. In would, however, make a difference in the long run. A clearer standard definition of the crime would improve prosecution and victim support measures, which would hopefully

reduce the amount of economic and financial impacts. Therefore, this criterion is scored as having a small positive impact.

(v) Feasibility (Score: +1)

Agreeing upon a national/international common standard definition of identity theft is not the easiest task. Many conferences and workshops would need to be organized and planned at the national level and at the international level. This type of activity could be added to the agenda of an OECD working party. Coming to a mutual agreement among all parties takes time and resources, and doesn't always happen (especially at the international level). Feasibility would be easier at the national level compared to the international level. Treaties (i.e. Council of Europe Convention on Cybercrime) would first need to be established with respect to identity theft before this standard definition could be agreed upon effectively and efficiently. Therefore, this criterion is scored as having a small positive impact.

7.3.3. Policy Option 3.3 – Establish international cooperation and partnerships (Score: 13)

Identity theft and fraud are cross-border crimes, thus, the international community has begun to realize the need for international cooperation on the issue. Uniformity in civil and criminal laws regarding identity theft is needed in order for the international community to function effectively within the Internet medium, especially since no entity currently controls the information that passes over the Internet. One important goal of international cooperation is uniformity. Uniformity is especially important in dealing with the Internet because international borders are practically invisible in this medium and it helps bring identity thieves to justice. However, international cooperation in combating identity theft is difficult because each nation or group of nations have different ideas about how to combat the issue, a different view of how much privacy invasion is allowed under a crime-fighting or civil litigation plan, and a different system for regulating and granting jurisdiction. International cooperation faces the complicated task of balancing the competing needs of protecting consumers and encouraging e-commerce growth.

The Council of Europe Convention on Cybercrime is an example of international cooperation for fighting cyber crime and identity theft. In addition to criminalizing certain types of activities, the convention attempts to foster cooperation between countries in prosecuting such crimes. This convention aims to define computer crimes to promote uniform national legislation, common criminal procedures, and resources for cooperation on an international level.

First, one major step toward uniformity and prevention of identity theft over the Internet is the creation of a truly global treaty on the subject (i.e. The Council of Europe Convention on Cybercrime). Second, the participating nations must make a formal coordinated effort to resolve the enforcement and jurisdictional issues involved in identity theft over the Internet. Third, another step that an international coordinated effort may need to explore is the creation of a formal body to try major identity theft crimes on an international level. Fourth, in dealing with the privacy issue, both sides will have to compromise before uniformity is possible. These established partnerships should be private-private, private-public, and public-public. There are only so many resources at the disposal of government and law enforcement agencies, so establishing private-public relationships at both national and international levels will help combat the crime of identity theft.

(i) Effectiveness (Score: +3)

Establishing international partnerships and cooperation is one of the most effective ways to combat identity theft and fraud since these crimes are committed at an international level through cyberspace. Uniformity at the international level has been proven to be highly effective in bringing criminals to justice. Therefore, this criterion has been scored as having a high positive impact, given that it achieves all policy objectives.

(ii) Efficiency (Score: +3)

Establishing international partnerships and cooperation is also one of the most efficient ways to combat identity theft and fraud. Having global treaties created, along with formal bodies to try major identity theft crimes, proves to be an efficient way to bring criminals to justice. Without international partnerships and cooperation, investigations

get stalled and take longer to complete which is not very efficient at all. Therefore, this criterion has been scored as having a high positive impact.

(iii) Stakeholder Impact (Score: +3)

Establishing international partnerships and cooperation directly impacts all stakeholders in the process of preventing identity theft, reducing identity theft, and prosecuting identity theft criminals. Therefore, this criterion is scored as having a high positive impact.

(iv) Economic and Financial Impacts (Score: +3)

Given that international partnerships and cooperation help streamline all aspects of the investigative process of identity theft and fraud, the economic and financial impacts are reduced tremendously. Minimal financial damage to victims is the result of more effective and efficient investigations. This policy sub-option is scored as having a large positive impact with respect to the economic and financial impacts of identity theft.

(v) Feasibility (Score: +1)

International cooperation faces the complicated task of balancing the competing needs of protecting consumers and encouraging e-commerce growth. More importantly, differences in regulatory and jurisdictional concepts present another major obstacle to creating international cooperation on identity theft issues. Therefore, international cooperation is not as feasible as the other policy options, and therefore this criterion is scored as having small positive impact.

7.4. Policy Option 4 – Combined Intervention (Total Score: 39)

This policy option ignores the international aspects of Policy Options 2 and 3, and contains the following elements:

- 2.1: Increase resources dedicated to combat cyber fraud in law enforcement agencies and businesses (including on-going education and training programs)

- 2.2: Establish a central reporting/statistical agency for identity theft and fraud
- 2.3: Improve/establish more sophisticated information sharing networks
- 3.1: Update credit freeze and security breach disclosure laws
- 3.2: Establish a national common standard definition of identity theft (international element removed)

Given that identity theft is given a low priority in most nations, it would be safe to assume that is also the case at an international level. This is slowly changing, however, as most nations and international organizations are becoming more aware of the drastic negative effects of identity theft and related crime, and the impact on the economy. Before Canada can join the battle on identity theft at the international level, it first needs to improve processes at home. Identity theft is very much an international crime, and international partnerships and cooperation are vital to successfully achieve all of the objectives outlined in Table 5.1, but to be effective and efficient, small steps need to be taken at a time. There are quite a few obstacles present when trying to achieve international cooperation, especially within police agencies. First, getting career professionals involved in defining a problem and proposing solutions is often hindered by agency politics. Second, obtaining political support in each participating country takes legal authority to operate and expenditure of money, personnel hours, and other agency resources. Obtaining political support means overcoming short or long-term rivalry between countries, convincing politicians that change from the status quo is needed, and convincing politicians and their constituencies that building an effective international police relationship is important enough, considering other claims on their time and their countries' resources, to merit their prompt attention. Lastly, another serious obstacle to attaining political support is the need to diplomatically work out fundamental differences in law enforcement style, which also takes time and resources. There are no one-size fits all approaches in international matters, and long-term commitment is needed to build cooperation. Therefore, it is recommended that Canada implement the domestic policy options before tackling the international aspects. Once the domestic options have been successfully implemented, coordination at the international level is strongly recommended.

All criminal matters need a combination of non-legislative and legislative intervention. Improving communication seems to be a recurring theme with respect to

identity theft and related crime, and both non-legislative and legislative intervention can be used to improve this area (i.e. credit freeze and data security breach disclosure laws, central reporting agency, improved information sharing networks, and increased resources). Therefore, this combination of non-legislative and legislative intervention seems to be the most effective and efficient way to combat identity theft and achieve the objectives outlined in Table 5.1. This is why this policy option has been scored as having a high positive impact for both these criteria. The combination of all national policy sub-options also directly impacts all stakeholders and greatly improves the chances of negating the economic and financial costs of identity theft and related crime. Therefore, both stakeholder and economic and financial impacts receive scores as having a high positive impact as well. Given that there are so many sub-options to implement, feasibility is scored as having a low positive impact due to time, money, and resource constraints that might not be readily available at this time.

Chapter 8. Recommendation and Conclusion

Overall, according to the assessment, Policy Option 4 is likely to have the largest impact on identity theft, as it would provide a comprehensive framework, addressing the current legislative gap with respect to reporting and communication mechanisms, and lack of knowledge, training, and available resources. The main disadvantage with Policy Option 4 is that it would take a considerable dedication of time and resources to implement. Funding will most likely come from Canada's Cyber Security Strategy, and re-distribution methods would need to be evaluated. Policy Option 4 contains the following combination:

- Policy Option 2 (Non-legislative intervention)
  - 2.1: Increase resources dedicated to combat cyber fraud in law enforcement agencies and businesses (including on-going education and training programs)
  - 2.2: Establish a central reporting/statistical agency for identity theft and fraud
  - 2.3: Improve/establish more sophisticated information sharing networks
- Policy Option 3 (Legislative Intervention)
  - 3.1: Update credit freeze and security breach disclosure laws
  - 3.2: Establish a national common standard definition of identity theft (international element removed)

In terms of rolling out the recommended policy option in the short, medium, and long term, I recommend the following:

Short term:

- Increase resources dedicated to combat cyber fraud in law enforcement agencies through re-allocation of the Cyber Security budget (including on-going education and training programs)
- Impose mandatory sanctions on businesses to ensure they have proper resources and mechanisms in place to prevent and combat cyber fraud (including on-going education and training programs)

These two sub-options would be more feasible to implement in the short term because lack of resources is one of the more prominent issues facing identity theft investigations, given the current backlog agencies are facing (RCMP, 2013). The seriousness of this crime has been portrayed throughout this study, so the goal would be to have the federal government allocate its current Cyber Security Strategy resources to this particular cybercrime. This would not be too difficult to accomplish since Cyber Security Strategy resources are already being allocated for cybercrime.

Since government and businesses should be leading the battle on identity theft (Canadian Consumer Initiative, 2008), government should be imposing mandatory sanctions on businesses as soon as possible since so much business is conducted online in cyberspace.

Medium term:

- Roll-out the establishment of the CAFC as being the central reporting/statistical agency for identity theft and fraud

This policy sub-option was recommended for the medium term because the CAFC has already been established as a reporting agency and is currently heading in this direction. The first step was combining both PhoneBusters and Reporting Economic Crime Online (RECOL) into one agency; the CAFC. Now focus can be placed on streamlining activities through this agency.

Long term:

- Continuously be improving and establishing more sophisticated information sharing networks

Improving and establishing more sophisticated information sharing networks for victims and law enforcement agencies will take a considerable amount of time to implement successfully since there are so many stakeholders involved. Comprehensive policies and regulations must be developed to define how personal information and records can be shared, who can have access to them, and under what circumstances they can be shared. This will require numerous agreements among governments, governments and the private sector, and private sector organizations (European Commission, 2012). An oversight committee would also need to be established to

ensure accountability. All these mechanisms require patience and trust to work effectively and efficiently.

Identity theft and related crime is a national crisis with global implications. Its pervasiveness must be recognized, especially as a facilitator of crimes that threaten national security, the economy, and personal privacy and security. Identity theft is highly significant because a person's identity is unique and highly personal and to have one's identity information misappropriated by another is a privacy violation of the highest order. As it may be some time before a victim realizes what has happened, the financial costs of identity theft may be severely significant, creating very heavy emotional costs. Using the misappropriated personal information of an individual, a criminal can make financial transactions as that person, emptying bank accounts, making purchases, and racking up debts. It may take considerable time and expense to resolve the resulting problems. There are even situations where, long after the event, victims may find themselves denied credit, or even arrested for crimes committed by the identity thief.

Identity theft and related crime impact individuals/consumers, businesses, hospitals, law enforcement agencies, and government at national and international levels. Combating identity theft is a very complex task, as it requires collaboration from all involved stakeholders, through efforts in education, technology development, security management, and law enforcement. No single entity can solve the problem. Technology is constantly advancing and evolving, and criminals will always find new and improved ways to commit crimes through the use of the Internet. Therefore non-legislative and legislative intervention mechanisms need to be constantly reviewed and be constantly evolving.

Without a national and global strategy, this crime will only continue to grow, as will the possibility of terrorist acts, financial crimes, drug trafficking, weapons smuggling, and human trafficking, all of which have an adverse impact on the global community and commerce. The recommendation offered here is an attempt to manage identity theft and fraud so that its growth will be contained and reduced. The goal is to get the issue identity theft and related crime higher on national and international political agendas,

since the repercussions are severe and detrimental to economic, social, and security stability.

References

Akkad, O.E. (2009, June 29). Identity Theft among Canada's fastest-growing crimes; In recent years, reports have soared 500 percent. *The Globe and Mail*.

Anandarajan, M., D'Ovidio, R. & Jenkins, A. (2013). Safeguarding Consumers Against Identity-related Fraud: Examining Data Breach Notification Legislation Through the Lens of Routine Activity Theory. *International Data Privacy Law*. 3(1), 51-60.

Anderson, K.B., Durbin, E. & Salinger, A. (2008). Identity Theft. *The Journal of Economic Perspectives*. 22(2), 171-192.

BC Freedom of Information and Provacy Association. (2005, April 30). *PIPEDA and Identity Theft: Solutions for Protecting Canadians*. Retrieved from http://fipa.bc.ca/library/Reports_and_Submissions/PIPEDA_and_Identity_Theft.pdf

Bronskill, J. (2013, January 29). Cybercrime Backlog Poses 'Significant Risk' to RCMP, Audit Warns. *The Canadian Press*.

Campbell, W. Identity Theft Canada: Stolen IDs Used To Obtain Real Passports, RCMP Report Says. (2012, September 9). *The Canadian Press.* Retrieved from http://www.huffingtonpost.ca/2012/09/09/identity-theft-canada_n_1868172.html

Canada Centre for Global Security Studies. (2011, November 24). *Ron Deibert Interviews Canada Centre Senior Fellow in Future Crime Marc Goodman*. Retrieved from http://munkschool.utoronto.ca/canadacentre/2011/11/24/citizen-lab-director-ron-deibert-interviewed-canada-centre-senior-fellow-in-future-crime-marc-goodman/

Canadian Anti-Fraud Centre. (2013). *Statistics*. Retrieved from http://www.antifraudcentre-centreantifraude.ca/english/statistics_statistics.html

Canadian Consumer Initiative. (2008, May). *Identity Theft Policy Position*. Retrieved from http://www.cci-icc.ca/CCI-pdf/CCI-BF-IDtheft-en.pdf

Canadian Internet Policy and Public Interest Clinic. (2007). *Identity Theft: Introduction and Background*. Retrieved from https://www.cippic.ca/sites/default/files/IDT_No.1-Introduction.pdf

Canadian Internet Policy and Public Interest Clinic. (2007). *Techniques of Identity Theft*. Retrieved from https://www.cippic.ca/sites/default/files/bulletins/Techniques.pdf

Canadian Internet Policy and Public Interest Clinic. (2007). *Legislative Approaches to Identity Theft*. Retrieved from https://www.cippic.ca/sites/default/files/bulletins/Legislation.pdf

Canadian Internet Policy and Public Interest Clinic. (2007). *Case Law on Identity Theft*. Retrieved from https://www.cippic.ca/sites/default/files/bulletins/CaseLaw_April_11,_2007.pdf

Canadian Internet Policy and Public Interest Clinic. (2007). *Enforcement of Identity Theft Laws*. Retrieved from https://www.cippic.ca/sites/default/files/LawEnforcement.pdf

Canadian Internet Policy and Public Interest Clinic. (2007). *Policy Approaches to Identity Theft*. Retrieved from https://www.cippic.ca/sites/default/files/bulletins/Policies.pdf

Clough, J. (2012). Principles of Cybercrime (1st ed.). *Cambridge: Cambridge University Press*. Retrieved from http://dx.doi.org.proxy.lib.sfu.ca/10.1017/CBO9780511845123

Cooney, P. (2014, February 24). Attorney General seeks national standard to protect against identity theft. *The Gazette*. Retreived from http://thegazette.com/2014/02/24/attorney-general-seeks-national-standard-to-protect-against-identity-theft/

Copes, H., & Vieraitis, L. (2007). U.S. Department of Justice. *Identity Theft: Assessing Offenders' Strategies and Perceptions of Risk*. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/grants/219122.pdf

Crane, W. (2001). DePaul University Journal of Art and Entertainment Law. *Legislative Updates: The World-Wide Jurisdiction: An Analysis of Over-Inclusive Internet Jurisdictional Law and an Attempt to Fix It*. Retrieved from https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&srctype=smi&srcid=3B15&doctype=cite&docid=11+DePaul-LCA+J.+Art+%26+Ent.+L.+267&key=2e2cd59a773d30945712a067c04e771c

Criminal Intelligence Service Canada. (2008). *Feature Focus: Identity Theft and Identity Fraud in Canada*. Retrieved from http://www.cisc.gc.ca/annual_reports/annual_report_2008/feature_focus_2008_e.html

Dadisho, E. (2013). The Police Chief. *Identity Theft and the Police Response: The Problem*. Retrieved from http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=493&issue_id=12005

Davis, E.S. (2003). A World Wide Problem on the World Wide Web: International Responses to Transnational Identity Theft via the Internet. *Journal of Law and Policy*. 201(12), 201-227.

Edwards, A. (2007). Identity Theft in Canadian Criminal and Regulatory Statutes. Retrieved from http://www.dww.com/dww/wp-content/uploads/2007/06/id_theft.pdf

Entrepreneurs Organization. (2013). *How Social Media Networks Facilitate Identity Theft and Fraud*. Retrieved from http://www.eonetwork.org/knowledgebase/specialfeatures/pages/social-media-networks-facilitate-identity-theft-fraud.aspx

Equifax. (2012, February 21). *Equifax Canada Reveals Attempted Fraud Incidents in the Financial Sector Amount to $650 Million in 2011*. Retrieved from http://www.consumer.equifax.ca/about_equifax/newsroom/en_ca?ncId=1187895492214

European Commission. (2012, December 11). *Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity Theft*. Retrieved from http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/final_report_identity_theft_11_december_2012_en.pdf

Finklea, K.M. (2014, January 16). Congressional Research Service. *Identity Theft: Trends and Issues*. Retrieved from http://www.fas.org/sgp/crs/misc/R40599.pdf

Federal Trade Commission. (2008, October 30). *Identity Theft and Assumption Deterrence Act*. Retrieved from http://www.ftc.gov/os/statutes/itada/itadact.htm

Federal Trade Commission. (2003). *Cybersecurity and Consumer Data: What's at Risk for the Consumer?*. Retrieved from http://www.ftc.gov/os/2003/11/031119swindletest.htm

Global Project on Cybercrime. (2011, October 14).*Cybercrime Startegies*. Retrieved from http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_cy_strats_rep_V20_14oct11.pdf

Gordon, G.R. & Willox, N.A. (2003, October). Identity Fraud: A Critical National and Global Threat. *LexisNexis*. Retrieved from http://veracity.lexis-nexis.com/presscenter/hottopics/ECIReportFINAL.pdf

Gorman, S. (2008, October 21). Identity Theft Twice as Likely in English-Speaking Countries. *Business Wire*. Retrieved from http://www.businesswire.com/portal/site/google/?ndmViewId=news_view&newsId=20081021005640&newsLang=en

Industry Canada. (2013). *Digital Policy Branch: Identity Theft*. Retrieved from http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/h_gv00171.html

International Cyber Security Protection Alliance. (2013). *Study of the Impact of Cyber Crime on Businesses in Canada*. Retrieved from https://www.icspa.org/fileadmin/user_upload/Downloads/ICSPA_Canada_Cyber_Crime_Study_May_2013.pdf

Internet World Stats. (2012). *Top 20 Countries with the Highest Number of Internet Users*. Retrieved from http://www.internetworldstats.com/top20.htm

Justice Laws Website. (2013). *Canada Post Corporation Act (R.S.C., 1985, c. C-10)*. Retrieved from http://www.laws.justice.gc.ca/eng/acts/C-10/

Justice Laws Website. (2013). *Criminal Code (R.S.C., 1985, c. C-46)*. Retrieved from http://laws-lois.justice.gc.ca/eng/acts/C-46/

Justice Laws Website. (2013). *Privacy Act (R.S.C., 1985, c. P-21)*. Retrieved from http://laws-lois.justice.gc.ca/eng/acts/p-21/

KPMG. (2011, July). Cyber Crime – A Growing Challenge for Governments. *Issues Monitor*.

Marquez, G.G. (2014, January 31). Lost in a Snap: How Should We React to Online Security Breaches? *LinkedIn*. Retrieved from https://www.linkedin.com/today/post/article/20140131175129-1523803-lost-in-a-snap-how-should-we-react-to-online-security-breaches?trk=eml-ced-b-art-Ch-2&ut=24o7m3MICVSS41&_mSplash=1

Newman, G.R., & McNally, M.M. (2005). U.S. Department of Justice. *Identity Theft Literature Review*. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf

Office of the Privacy Commissioner of Canada. (2013). *Identity Theft and Fraud*. Retrieved from http://www.priv.gc.ca/resource/topic-sujet/itf-vif/index_e.asp#research

Office of the Privacy Commissioner of Canada. (2013). *The Case for Reforming the Personal Information Protection and Electronic Documents Act*. Retrieved from http://www.priv.gc.ca/parl/2013/pipeda_r_201305_e.asp

Organization for Economic Co-operation and Development. (n.d.). *OECD Policy Guidance on Online Identity Theft*. Retrieved from http://www.oecd.org/sti/consumer/40879136.pdf

Parliament of Canada. (2009, October 22). *Chapter 28 – An Act to amend the Criminal Code (identity theft and related misconduct)*. Retrieved from http://www.parl.gc.ca/HousePublications/Publication.aspx?Doc=S-4_4&File=27&Language=E&Mode=1&Parl=40&Pub=Bill&Ses=2

Perrin, S. et al. (2006). BC Freedom of Information and Privacy Association. *PIPEDA and Identity Theft: Solutions for Protecting Canadians*. Retrieved from http://fipa.bc.ca/library/Reports_and_Submissions/PIPEDA_and_Identity_Theft.pdf

Peterson, L. (2009). Identity Theft: An Overview. *Canadian Points of View Reference Centre*.

Press, J. (2012, October 23). Canada falling behind on cyber-security despite spending almost $1B, Auditor-General says. *National Post*. Retrieved from http://news.nationalpost.com/2012/10/23/canada-falling-behind-on-cyber-security-despite-spending-more-than-1b-auditor-general-says/

Robinson, N., Graux, H., Parrilli, D.M., Klautzer, L., & Valeri, L. (2011). *Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime*. Retrieved from http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/rand_study_tr-982-ec_en.pdf

Romanosky, S. (2008). Heinz School of Public Policy and Management, Carnegie Mellon University. *Do Data Breach Disclosure Laws Reduce Identity Theft?*. Retrieved from http://www.consumerdatareporting.com/pdfs/carnegie%20mellon%20breaches%200508.pdf

Royal Canadian Mounted Police. (2013, January). *Economic Impact: National Identity Crime Strategy*. Retrieved from http://www.rcmp-grc.gc.ca/pubs/cc-dc/strat/ei-ie-eng.htm

Royal Canadian Mounted Police. (2013). *Identity Theft and Identity Fraud*. Retrieved from http://www.rcmp-grc.gc.ca/scams-fraudes/id-theft-vol-eng.htm

Smith, R.G. (2008, May 7). Coordinating Individual and Organizational Responses to Fraud. *Crime, Law, and Social Change*.

Smyth, S.M., & Carleton, R. (2011). Public Safety Canada. *Measuring the Extent of Cyber-Fraud: A Discussion Paper on Potential Methods and Data Sources*. Retrieved from http://publications.gc.ca/collections/collection_2011/sp-ps/PS14-4-2011-eng.pdf

Sproule, S. & Archer, N. (2008, July). Measuring Identity Theft in Canada: 2008 Consumer Survey. *McMaster eBusiness Research Centre*.

State of California Legislative Counsel. (1873). *California Civil Code*. Retrieved from http://www.leginfo.ca.gov/.html/civ_table_of_contents.html

State California Legislative Counsel. (1873). *California Penal Code*. Retrieved from http://www.leginfo.ca.gov/.html/pen_table_of_contents.html

Statistics Canada. (2012). *Breakdown of the Survey of Fraud Against Businesses Sample by Industry*. Retrieved from http://www.statcan.gc.ca/pub/85-571-x/2009001/t001-eng.htm

Taylor-Butts, A. & Perreault, S. (2009, December). Fraud Against Businesses in Canada: Results From a National Survey. *Statistics Canada*.

The Canadian Press. (2014, January 21). Target data breach may affect some Canadians. *CBC News*. Retrieved from http://www.cbc.ca/news/business/target-data-breach-may-affect-some-canadians-1.2504226

Time – Business & Money. (n.d.). *Here's How Your Identity Will Be Stolen: The Top 10 Scams*. Retrieved from http://business.time.com/2012/04/17/10-ways-youre-going-to-get-your-identity-stolen/slide/all/

Viellaris, R. (2013, September 21). Social media enables cyber criminals to build profiles for identity theft. *Couriermail.com.au*. Retrieved from http://www.couriermail.com.au/news/queensland/social-media-enables-cyber-criminals-to-build-profiles-for-identity-theft/story-fnihsrf2-1226723950119

Wang, W., Yuan, Y., & Archer, N. (2006). *A Contextual Framework for Combating Identity Theft*. Retrieved from http://ieeexplore.ieee.org.proxy.lib.sfu.ca/stamp/stamp.jsp?tp=&arnumber=1621057

Williams, L. (2007, February 15). *Feds flunk SIN system, says Auditor General. InterGovWorld.com*. Retrieved from http://www.intergovworld.com/article/c28603750a01040800109fbf60b90d67/pg0.htm

Willox, N.A. & Regan, T.M. (2002, March). Identity Fraud: Providing a Solution. *LexisNexis*. Retrieved from http://www.lexisnexis.com/about/whitepaper/identityfraud.pdf

Appendix A. Identity Theft 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 (CIPPIC, 2007).

"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 license 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 organization that published it (CIPPIC, 2007).

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)**
>
> "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 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)**
>
> "Identity theft is when someone uses your name and personal information to commit fraud or theft." **(Alberta Government)**

"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)**

"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 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)**

"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)**

"Personal identity theft is the unauthorized collection and fraudulent use of someone else's personal information." **(Alberta Motor Association)**

"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)**

"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 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 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)**

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 license 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." **(Allisona, S., Schuck, A & Lerschc, K., 2005)**

"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." **(Elbirt, A.J., 2005)**

"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." **(Wright, B., 2004)**

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 (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)**

"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 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)**

"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)**

"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**

“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)**

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)**

“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)**

“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)**

“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)**

“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)**

“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)**

United States

“Theft or misuse of personal or financial identifiers to gain value and/or facilitate criminal activity.” **(Federal Bureau of Investigation)**

Definitions from other organizations

“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 is the theft and fraudulent use of another person’s identity or personal information.” **(Fasken Martineau)**