The International Centre for Criminal Law Reform and Criminal Justice Policy

RESPONDING TO VICTIMS OF IDENTITY CRIME:

A MANUAL FOR LAW ENFORCEMENT AGENTS, PROSECUTORS AND POLICY-MAKERS

MARCH 2011

This project was made possible by the funding and support received from Public Safety Canada, the Law Foundation of British Columbia, the United Nations Office on Drugs and Crime, and the International Centre for Criminal Law Reform and Criminal Justice Policy. The views and opinions expressed herein are those of the author and do not represent any overarching official policy or opinion on the part of either the International Centre or the Canadian government.

March 2011

INTERNATIONAL CENTRE FOR CRIMINAL LAW REFORM
AND CRIMINAL JUSTICE POLICY
LE CENTRE INTERNATIONAL POUR LA RÉFORME DU DROIT CRIMINEL
ET LA POLITIQUE EN MATIÈRE DE JUSTICE PÉNALE

1822 East Mall, Vancouver, B.C. / C.-B., V6T 1Z1 Canada
Tel/Tél: + 1 (604) 822-9875 Fax/Téléc: + 1 (604) 822-9317
Email/Courriel: icclr@law.ubc.ca www.icclr.law.ubc.ca

The International Centre for Criminal Law Reform and Criminal Justice Policy

RESPONDING TO VICTIMS OF IDENTITY CRIME:

A MANUAL FOR LAW ENFORCEMENT AGENTS, PROSECUTORS AND POLICY-MAKERS

Philippa Lawson

MARCH 2011

Responding to Victims of Identity Crime: A Manual for Law Enforcement Agents, Prosecutors and Policy-Makers

ISBN: 978-0-9868799-0-6

The International Centre for Criminal Law Reform and
Criminal Justice Policy (ICCLR) /
Le Centre international pour la réforme du droit criminel
et la politique en matière de justice pénale (CIRDC)

1822 East Mall, Vancouver, B.C. / C.-B.
V6T 1Z1 CANADA
Tel / Tél: + 1 (604)-822-9875 Fax / Téléc: + 1 (604)-822-9317
Email / Courriel: icclr@law.ubc.ca www.icclr.law.ubc.ca

Printed and bound in Vancouver, British Columbia, Canada

ACKNOWLEDGMENTS

The International Centre for Criminal Law Reform and Criminal Justice Policy ("ICCLR") would like to thank all of the individuals and institutions who contributed their time and expertise so generously to the production of: Responding to Victims of Identity Crime: Manual For Law Enforcement, Prosecutors and Policymakers.

In particular thanks are due to Ms. Philippa Lawson, Barrister and Solicitor, the primary author of this publication, for her laudable efforts and expertise in crafting this Manual. The project was supported by Eileen Skinnider, Director of Human Rights and Research, and Yuli Yang, Project Coordinator. A special word of thanks is extended to Annemieke Holthuis, Counsel, Criminal Law Policy Section, Justice Canada, for her support throughout the project.

ICCLR is especially grateful to the following members of the Advisory Committee for their guidance and advice:

Jennifer Chan	Policy Analyst, Serious and Organized Crime Division, Public Safety Canada
Corrina Clement	Senior Policy Analyst, Policy Centre for Victim Issues, Justice Canada
William J. Crate	Director, Security, Canadian Bankers Association
Robert Daly	Manager, Serious and Organized Crime Division, Public Safety Canada
Jonas Dow	Crown Counsel, Ministry of Attorney General of British Columbia
Joshua Hawkes Q.C.	Director, Policy Unit, Appeals & Prosecution Policy Branch, Ministry of Justice and Attorney General of Alberta
Janet Henchey	General Counsel, International Assistance Group, Justice Canada
Annemieke Holthuis	Counsel, Criminal Law Policy Section, Justice Canada
Joanne Klineberg	Counsel, Criminal Law Policy Section, Justice Canada
Kathleen Macdonald	Executive Director, ICCLR
Kathy MacDonald	Constable, Cyber Awareness Co-ordinator, Crime Prevention Unit, Calgary Police Service
Kevin McQuiggin	Inspector, Forensic Services Section, Vancouver Police Department
Brian Montague	Detective, Vancouver Police Department
Paul Proulx	Staff Sergeant, Canadian Anti-Fraud Centre, Royal Canadian Mounted Police
Christopher D. Ram	Counsel, Criminal Law Policy Section, Justice Canada
Kevin Scott	President, Canadian Identity Theft Support Centre

Peter Stabler	Crown Counsel, Ministry of Attorney General of British Columbia
Robin Tremblay	Counsel, Policy Centre for Victim Issues, Justice Canada
Sylvie Tremblay	Sergeant , National Identity Fraud Coordinator, Commercial Crime Branch, Royal Canadian Mounted Police
Louis Zuniga	National Crime Prevention and Youth Services, Royal Canadian Mounted Police

ICCLR appreciates the expert advice and contributions received from the United Nations Core Group of Experts on Identity-related Crime including: Demostenes Chryssikos, Luca Castellani, Jeppe Holt Jensen, Eugenio Curia, Christopher Ram, Edwin Delwel, Jan Vancoillie, Jonathan Rusch , Patrick Cain, Fons Knopjes, Anko Blokzijl, Marcos Salt, Gilberto Martins de Almeida, Baosheng Zhang, Marco Gercke, and Michael Murungi.

Finally, ICCLR would like to thank Public Safety Canada, the Law Foundation of British Columbia and the United Nations Office on Drugs and Crime for providing us with the support and funding to undertake this initiative.

Please note that the analysis and recommendations in this Manual do not necessarily reflect the views of any of the aforementioned individuals or organizations.

THE INTERNATIONAL CENTRE FOR CRIMINAL LAW REFORM AND CRIMINAL JUSTICE POLICY AND ITS RELATED WORK IN ECONOMIC FRAUD AND IDENTITY RELATED CRIME

The International Centre for Criminal Law Reform and Criminal Justice Policy ("ICCLR" or the "Centre") is an independent, international institute based in Vancouver, Canada. Founded in 1991, ICCLR is a joint initiative of the Government of Canada, University of British Columbia, Simon Fraser University, the International Society for the Reform of Criminal Law, and the Province of British Columbia. It is officially affiliated with the United Nations ("UN") pursuant to a formal agreement in 1995 between the Government of Canada and the UN. Through its activities, the Centre contributes to the priorities of Canada and the United Nations in the field of criminal law and criminal justice.

The mandate of the Centre is to promote the rule of law, democracy, human rights, and good governance in criminal law and the administration of criminal justice, domestically, regionally and globally. The Centre's programmes assist with the current Canadian priorities including efforts to combat transnational organized crime and corruption; to ensure safe and secure communities for Canadians; to emphasize the rights of victims; to actively promote protection of children, women and vulnerable populations; to enhance effective and fair justice systems; and to promote international cooperation in the fight against serious crimes. The underlying premise of ICCLR's efforts is that a fair, responsible, ethical and efficient criminal justice system forms the foundation for economic development, social progression and human security.

The Centre's programmes and projects specifically related to or addressing Economic Fraud and Identity Related Crime include:

- A paper on **Identity-Related Crime Victim Issues** that focused on the range and typology of identity-related crime victims; relevant legal rights; and an inventory of best practices for victim remediation. The paper was presented to the United Nations Office on Drugs and Crime Core Group of Experts on Identity Related Crime, circulated as a Conference Room Paper at the UN Crime Commission meeting in April 2009, and is available on the ICCLR website.

- An ancillary meeting on **Prevention of Economic Fraud and Identity-related Crime** in 2009 at the 18th Session of the UN Commission on Crime Prevention and Criminal Justice. The meeting was organized to support the Canadian draft resolution: International Cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime (E/CN.15/2009/L2).

- A symposium, **National and International Perspectives on Identity Theft and Fraud,** on June 20, 2008, in Vancouver, Canada. The Symposium was designed to support the discussions and awareness raising efforts of the then recently introduced Government of Canada Bill C-27 to amend the Criminal Code to address identity theft and fraud, as well as the ongoing work of experts based on UN Economic and Social Council Resolution 2004/26 of 21 July 2004.

EXECUTIVE SUMMARY

Identity crime is a serious crime with potentially devastating effects on individual victims. With recent amendments to the Canadian Criminal Code creating new offences for identity theft and identity fraud, it is incumbent on law enforcement to take reports of such crime and to investigate them thoroughly. It is also incumbent on law enforcement to assist victims by providing appropriate advice and referrals.

This Manual is designed to support and strengthen the understanding of Canadian law enforcement officers, investigators, prosecutors and policy-makers about victims of identity related crime, so as to better assist victims of these types of crimes and ultimately to reduce the incidence and impact of such crimes. Improving law enforcement response to victims not only serves to help victims recover their reputations and prevent further damage, but it also contributes to the identification and prosecution of identity criminals.

The manual includes six modules and several printable appendices for use by police officers and investigators in their daily operations. It is designed to be useful both as a quick reference tool in specific cases and as a more detailed source of information for professional training purposes.

Module 1 sets out the background, scope and purpose of the Manual, and explains terminology used.

Module 2 provides more detailed background about identity crime in general, its extent and impact in Canada, and relevant legislation in Canada and internationally.

Module 3 focuses on the needs of identity crime victims, and is designed to enhance law enforcement understanding of the impact of this crime on its victims (individual and institutional).

Module 4 explains the role of law enforcement in responding to identity crime victims, and sets out the form and content of an effective response. It includes advice for police officers, investigators and prosecutors in dealing with individual victims of identity crime.

Module 5 focuses on corporate and government victims, providing advice on how to respond to them.

Module 6 addresses the need for coordination among law enforcement and other government agencies, as well as with the private sector, in order to respond effectively to victims, especially in cases involving more than one jurisdiction.

Module 7 is distinct from the rest of the Manual. It provides guidance to policy-makers on best practices for protection of identity crime victims through legislation and policy. In particular, it provides a review of identity crime victim rights and remedies in Canada,

noting best practices and gaps in comparison with laws and initiatives in the U.S. It shows that victims of identity crime in Canada lack many rights and remedies that victims of identity crime in the U.S. now have.

Finally, the Manual includes several Appendices, most of which are short, printable checklists, forms or guides designed for use by police or by victims themselves. Police may consider providing copies of the victim self-help guides and forms to victims.

Although designed for use by law enforcement agencies, prosecutors and policy-makers, the Manual will also serve as a useful resource for private sector entities that deal with victims of identity-related crime, as well as for victims and victim advocates.

The information in this Manual is current as of March 2011. It is hoped that future versions will be published with updated information as needed.

TABLE OF CONTENTS

Module 1: Introduction 1

1.1 Background 1
1.2 Purpose of Manual 1
1.3 Terminology 2
1.4 Future Versions of the Manual 2

Module 2: Identity-Related Crime: Definition, Scope and Legal Context 3

2.1 Definition and Scope 3
2.2 Identity Criminals and their Techniques 5
2.3 Extent and Overall Impact of Identity Crime in Canada 7
2.4 Criminal Code Offences 8
2.5 Other Relevant Domestic Laws 10
2.6 International Context of Identity Crime 12
2.7 International Law Relevant to Identity Crime 13

Module 3: Identifying and Understanding Victims of Identity Crime 15

3.1 Range and Types of Identity Crime Victims 15
3.2 The Importance of Identifying and Reporting Identity Crime 15
3.3 Impact of Identity Crime on Individual Victims 16
3.4 Understanding individual victims of Identity Crime 18
3.5 Understanding Corporate and Government Victims 19

Module 4: Responding to Individual Victims of Identity Crime 21

4.1 Role of Local Law Enforcement 21
4.2 Communicating with the Victim 22
4.3 What Victims Need from Law Enforcement 23
(1) The Police Report 23
(2) Advice 24
(3) An Understanding of What Happens Next in the Criminal Investigation 25
(4) Impersonation Alert on Criminal Database File 26
4.4 Information to Include in the Police Report 26
4.5 Working with Individual Victims in the Investigation of Identity Crime 28
4.6 Working with Individual Victims in the Prosecution of Identity Crime 28

Module 5: Responding to Institutional Victims of Identity Crime 31

5.1 Fraudulent use of Corporate or Government Trademark 31
5.2 Theft of Personal Information from Corporate/Government Holdings 32
5.3 Working with Institutional Victims in the Investigation and Prosecution of Identity Crime 32

Module 6: Coordinating Victim Response with Other Agencies 35

6.1 Roles, Responsibilities and Best Practices in Identity Crime Victim Remediation 35
6.2 Coordinating with Other Government/Law Enforcement Agencies to Assist Victims 38
6.3 Coordinating with the Private Sector to Assist Victims 41
6.4 Dealing with Inter-jurisdictional Challenges in Victim Assistance 42

Module 7: Identity Crime Victim Rights and Remedies 45

7.1 Legal Rights and Remedies for Identity Crime Victims in Canada 45
7.2 Legal Gaps in the Canadian Approach to Victims of Identity Crime 48
7.3 Policy Gaps in the Canadian Approach to Victims of Identity Crime 52

Appendices 55

A. Guide for Police Officers Receiving Identity Crime Complaints 57
B. Information to Include in the Police Report 59
C. Identity Crime Victim Statement/Affidavit form 61
D. Identity Crime Victim Self-Help Guide – detailed version 69
DD. Identity Crime Victim Self-Help Guide – summary version 73
E. Identity Crime Victim Action Log 75
F. Identity Crime Prevention Tips – detailed version 77
FF. Identity Crime Prevention Tips – summary version 81
G. Resources for Identity Crime Victim in Canada 83
H. Resources for Identity Crime Victims in the USA 85
I. Legal Rights and Remedies for ID crime victims in Canada (Table) 87
J. References 99

Module 1: Introduction: Purpose of Manual

1.1 Background

Identity crime is one of the fastest growing and most serious economic crimes in North America., continuing to top the list of complaints to the Consumer Sentinel Network.[1] Federal and provincial governments, privacy commissioners, affected private sector organizations, consumer groups and others are attempting to address the problem through public education, policy initiatives and law reform, but Canadians continue to be victimized, often seriously. Although identity crime presents special challenges, law enforcement agencies have an ethical and professional obligation to assist identity crime victims and bring criminals to justice.

Victims of crimes involving their identity information often don't know where to turn for help. They are frequently frustrated by the lack of response from law enforcement agencies, especially when they don't know how, where, or by whom their information was stolen and used. All they may know is that their savings have evaporated, that creditors are demanding payment for loans they never took, or that they are being accused of crimes they never committed.

Law enforcement agencies do not have the capacity to investigate every reported identity crime, but they can help every victim by recording all complaints of identity crime, directing victims to tools and resources for restoring their reputations, and providing victims with copies of the incident report that they can use in their remediation efforts.

Supporting and assisting victims not only helps to mitigate the effects of the crime, it also facilitates police investigations, can uncover important new evidence, and helps to prevent ongoing victimization, a common feature of identity-related crime.

This manual is designed to assist law enforcement agencies and prosecutors deal effectively with victims of identity-related crime, not only to help victims recover their reputations and prevent further damage, but also to improve state efforts to identify and prosecute identity criminals. It also includes a review of identity crime victim rights and remedies in Canada, noting best practices and gaps in comparison with laws and initiatives in the U.S.A.

1.2 Purpose of Manual

This manual has two primary purposes:
(a) to help law enforcement agencies and prosecutors respond effectively to victims of identity crime (Modules 2-6), and
(b) to provide guidance to policy-makers on best practices for protection of identity crime victims through legislation and policy (Module 7, in particular).

[1] Federal Trade Commission, Consumer Sentinel Network Data Book, February 2010.

Although designed for use by law enforcement agencies, prosecutors and policy-makers, the manual will also serve as a useful resource for private sector entities that deal with victims of identity-related crime. Several Appendices are designed for victims themselves (i.e., information and forms that police can provide to victims); these are obviously useful to individual victims.

NOTE: This is not a manual on how to investigate and prosecute identity crime, although it includes information helpful in that regard.

1.3 Terminology

As discussed in Module 2.1, the term "identity crime" refers to a wide range of criminal activity including the fraudulent use of another person's identity information as well as the theft, creation, replication, manipulation, possession, or sale of identity information for the purpose of committing fraud or other crimes. Any number of these discrete crimes can be involved in a given incident.

The terms "identity theft" and "identity fraud", although frequently used to refer to this broad category of criminal activity, are defined more narrowly in the *Criminal Code*: *identity theft* refers to the collection, possession and trafficking in identity information; *identity fraud* refers to the fraudulent use of such information.

The term "identity-related crime" is commonly used at the international level to encompass all crimes involving the creation, theft, manipulation, misuse, and sharing of identity information as well as related offences such as trafficking in instruments of forgery. We use the shorter term "identity crime" in this Manual to refer to the range of identity-related offences in Canada.

1.4 Future Versions of the Manual

This is version 1.0 of the Manual. Many services, policies and practices relevant to victims of identity crime in Canada are currently in a state of development. It is expected that there will be future revised versions of the Manual so as to reflect significant developments such as the establishment of a Canadian identity crime victim support centre, expected by 2012. Please send suggestions for revisions to icclr@law.ubc.ca.

Module 2: Identity Crime: Definition, Scope and Legal Context

2.1 Definition and Scope

Identity crime involves the unauthorized gathering, trading or use of another person's personal information (e.g., credit card numbers, social insurance numbers, drivers licence numbers) to gain something of value or to facilitate other criminal activity. Typically involving financial fraud, it can devastate the victim's credit rating, ruin their reputation in the community and cause emotional trauma akin to that suffered by victims of violent crime. Identity crime is often part of a larger criminal enterprise, making it particularly serious from a law enforcement perspective. It is also often conducted trans-provincially and trans-nationally, creating extra challenges for investigation, prosecution and victim assistance.

Identity crime offences can be divided into three categories: identity theft, identity fraud, and other related crimes.

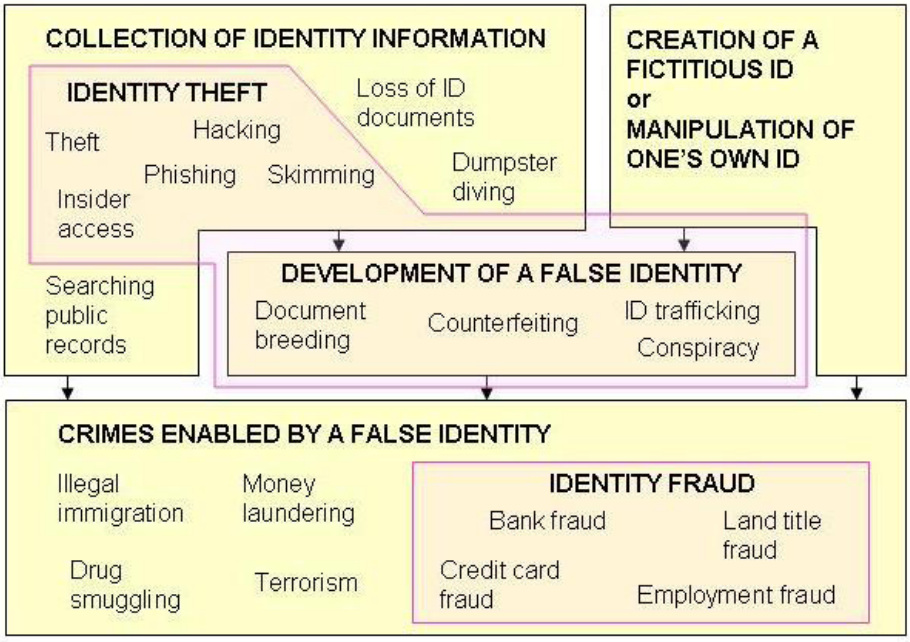
> *Identity theft* encompasses various activities involving the collection, possession and trading of another person's identity information for illegal use. See s.402.2 of the *Criminal Code*.
>
> *Identity fraud* refers to the fraudulent use of that information. See s.403 of the *Criminal Code*.
>
> *Other identity-related crimes* include various intermediate crimes involving the collection, use or trading of identity information for criminal purposes or of tools for manufacturing identity documents. Examples of such offences include redirection of mail, specific credit card offences and creating, possessing or dealing in forgery instruments.

"Identity information" is defined in s.402.1 of the *Criminal Code* as "any information — including biological or physiological information — of a type that is commonly used alone or in combination with other information to identify or purport to identify an individual, including a fingerprint, voice print, retina image, iris image, DNA profile, name, address, date of birth, written signature, electronic signature, digital signature, user name, credit card number, debit card number, financial institution account number, passport number, Social Insurance Number, health insurance number, driver's license number or password."

NOTE: Identity crimes may involve the personal information of live or deceased individuals. They may also involve synthesized identities using information from more than one victim, or combining fictional data with a real person's information. The above definition arguably includes such cases since even fictional information "purports to identify an individual".

See Module 2.3 for a list of key relevant *Criminal Code* offences.

A useful visual model of identity-related crime has been proposed by Sproule and Archer.[2]



It can be difficult to distinguish between ordinary fraud and identity fraud. In the case of identity fraud, the criminal possesses information relating to the identity of a person (e.g.: name, address, telephone number, date of birth, mother's maiden name, Social Insurance Number (SIN), driver's licence number, health card number, account number, password) and then masquerades as the victim, effectively taking over their identity.

In some cases, the criminal simply uses the victim's account information (e.g., credit card number) to make fraudulent transactions on that single account and the crime ends there. In other cases, the criminal uses the victim's personal information to open up bank, utility and cell phone accounts, secure new credit cards, apply for and obtain benefits, secure employment, commit crimes, evade authorities or begin a new life, often in another country. Criminals may also use the victim's email account to send threatening or defamatory messages. Such crimes can be devastating for the victim, affecting their credit and reputation for years.

There is little in the way of Canadian statistics breaking down identity fraud by type. A national survey conducted in 2006 and 2008 by the McMaster eBusiness Research Centre

[2] Susan Sproule and Norm Archer, *Defining and Measuring Identity Theft*, presentation to the second Ontario Research Network in Electronic Commerce (ORNEC) Identity Theft Workshop, (Ottawa, 13 October 2006).

indicates that credit card fraud is the most common form of identity fraud, followed by existing account fraud, and then new account fraud.[3]

Credit card fraud (17%) was the most common form of identity theft reported to the U.S.-based Consumer Sentinel Network in 2009, followed by government documents/ benefits fraud (16%), phone or utilities fraud (15%), and employment fraud (13%). Other significant categories of identity theft reported by victims in this database were bank fraud (10%) and loan fraud (4%).[4]

Identity crime is often part of a larger criminal enterprise: acts of terrorism, people smuggling, immigration scams and drug related crimes are often committed using stolen or fabricated identities.[5] Money-laundering schemes often involve identity crime, as criminals take over accounts of others and create new accounts in the victim's name, then use these accounts to transfer funds offshore or otherwise to obfuscate their activities.

2.2 Identity Criminals and their Techniques

Identity criminals range from otherwise law-abiding individuals who may have no prior criminal record to transnational professional criminal organizations whose income and activities are funded and facilitated by identity crime. Unless the victim has clear evidence pointing to a perpetrator, you don't know whether you are dealing with a local small time thief, a seasoned criminal, or a sophisticated international crime ring.

In addition to financial fraud, organized criminal groups use identity fraud to evade authorities and to travel across borders undetected. They also engage in the fabrication, buying and selling of identity information for financial gain, often exploiting weaknesses in identity document issuance. A significant proportion of transnational identity crime is associated with illegal migration and human trafficking.[6]

Identity criminals use a range of methods to gather personal information, including:

- stealing wallets; stealing mail; stealing unsecured information from homes
- sifting through trash and discarded computers
- gathering data from public sources and taking advantage of inadvertent exposure of personal data by corporations, government or other data-holders
- gathering data from social networking sites
- "pre-texting" (e.g., pretending to be someone else in order to obtain information about an individual's account from a service provider)
- bribing employees to hand over client/customer information
- computer hacking
- observing or recording people entering PINs and passwords
- "skimming" information from magnetic stripes on bank cards

---

[3] Susan Sproule and Norm Archer, *Measuring Identity Theft in Canada: 2008 Consumer Survey* – MeRC Working Paper #23 ["MeRC Working Paper #23"].

[4] Federal Trade Commission, *Consumer Sentinel Network Data Book*, February 2010, p.3.

[5] Criminal Intelligence Service Canada, *Report on Organized Crime 2010.*

[6] See for example U.S. Immigration and Customs Enforcement webpage on "Identity and Benefits Fraud" at http://www.ice.gov/identity-benefit-fraud

- using hidden computer programs (a.k.a. "spyware" or "malware") to gather personal data from people's computers
- fooling people into providing their personal information by posing as a trusted service provider by email ("phishing"), voice phishing ("vishing"), text messaging ("smishing"), fake websites, phone or otherwise
- purchasing stolen information from other criminals.

In many cases, the victim's identity information is obtained by the criminal through no carelessness or other fault of the individual victim. Sometimes, third parties are at fault for failing to secure their data holdings or allowing the information to be released without sufficient precautions. Individual victims may therefore be completely unaware that they have been victimized until the damage to their finances and reputation becomes evident.

The techniques of identity criminals are constantly evolving. While some use old-fashioned techniques like dumpster-diving and shoulder-surfing to gather personal information, others hack into computers or use new technologies in clever ways to steal identity information from unsuspecting victims. Many identity criminals are extremely computer-savvy and skilled at covering their tracks.

Identity criminals often use the identities of deceased persons to obtain official identity documents, to access government services or to evade authorities. In one scam discovered by Canadian police, detailed identity documentation for individuals who had died as children was being sold for use by foreign individuals of roughly the same age, who then were able to obtain Canadian passports and other official documentation using their own photographs together with the name, date and place of birth and other information about the victim. Using this documentation, they were able to access Canadian medical care.[7] The primary victim in this case was the Canadian citizen and taxpayer.

Identity criminals also create fictional identities by combining real and false information, or information from more than one victim. Synthetic identity fraud can be more difficult to detect than "true name" identity fraud, since records of the fraudulent activity do not immediately show up on victim credit reports or other records under the victim's name. In typical synthetic identity fraud now common in the US, the thief combines one victim's Social Security Number ("SSN") with another person's name and date of birth. Although the real SSN holder may not be affected by the subsequent frauds using her SSN, she may eventually be associated with them if creditors, debt collectors, tax authorities, law enforcement agencies or other authorities pursuing the fraud link the SSN back to her name.

Such cases can be particularly damaging and difficult for victims to resolve given the delay in detection and the often confusing combination of identity information.[8] But

[7] Joe Pendleton, Director of Special Investigations, Service Alberta, "The Growing Threat of Medical Identity theft in Canada", Presentation to the Electronic Health Privacy Conference, Ottawa, (Nov.3, 2008), http://www.ehip.ca; reported in Pauline Tam, "ID theft Scams Target Canada's Healthcare System", The Ottawa Citizen (Nov.3, 2008).

[8] Leslie McFadden, "Detecting Synthetic Identity Fraud", www.bankrate.com (May 16, 2007).

even if individuals whose identity information is used in synthetic identity fraud are not adversely affected by it, this form of identity fraud is extremely costly to businesses, consumers and the economy generally.

Identity criminals use the information they gather in many different ways, including:

- selling it to other criminals for use in identity-related crime
- accessing and using the victim's credit or debit card
- taking over the victim's bank account
- opening new financial accounts, loans or mortgages in the victim's name
- obtaining a mailbox in the victim's name to divert mail
- forging fake identity documents
- obtaining a passport or other identity document in someone else's name
- opening telephone or utility accounts in the victim's name
- obtaining government benefits in the victim's name
- obtaining employment, accommodation or other services using the victim's name
- concealing their identity while travelling illegally, smuggling drugs, engaging in money-laundering, terrorism or other crimes

2.3 Extent and Overall Impact of Identity Crime in Canada

Because most identity crime is not reported to law enforcement agencies,[9] and because statistics on identity crime are not yet being systematically gathered in Canada, we can only estimate the extent and overall impact of this crime by inference from those incidents that are reported, from surveys of a population sample, and from more extensive U.S. statistics.

Complaints-based data gathered by the Canadian Anti-Fraud Centre ("CAFC") suggests that identity crime is a significant and growing problem in Canada. The CAFC received calls from over 11,000 identity crime victims in each of 2008 and 2009, with total reported dollar losses growing from $9.6m. in 2008 to $10.9m. in 2009.[10] The CAFC estimates that the complaints it receives represent fewer than 5% of total fraud victims in Canada.[11]

A 2008 survey by the McMaster eBusiness Research Centre found that 6.5% of Canadians (nearly 1.7 million people) had been the victim of some kind of identity fraud in the preceding year.[12] Of these, approx. 1 million were victims of credit card fraud. Projecting survey results onto the Canadian population, annual losses due to identity fraud in Canada were estimated at $1.867b., total out of pocket costs incurred by victims were estimated at $155.7m., and total time spent by victims in remediation efforts was estimated to be 21.67m. hours. These figures do not include losses unknown to individual victims that are incurred by corporate and government victims of identity fraud.

---

[9] See –*MeRC Working Paper #23;* and United States Bureau of Justice Statistics, *Victims of Identity Crime, 2008*, National Crime Victimization Supplement (December 2010) ["US BJS 2008 survey"].

[10] CAFC Criminal Intelligence Analytical Unit, *Annual Statistical Report 2009: Mass Marketing Fraud and ID Theft Activities*.

[11] Monthly Summary Report, 2010.

[12] MeRC Working Paper #23.

Financial institutions maintain their own statistics on identity fraud involving their services. Reported losses in Canada due to payment card fraud alone were over $500 million in both 2008 and 2009, with debit card fraud losses rising by 36% over this period.[13] While the adoption of chip-and-PIN cards will reduce skimming and counterfeiting activity, payment card fraud is likely to continue as long as card-not-present transactions are permitted.

In the United States, a nationwide survey conducted by the Bureau of Justice Statistics in 2008 found that approx. 5% of persons over 16 years of age had been victimized by identity crime, at a total cost to the US economy of US$17.3b. over two years. Over half (53%) of these cases involved unauthorized misuse or attempted misuse of an existing credit card.[14] A privately conducted 2011 survey indicates that the rate of identity fraud may be falling, with 8.1m. people (3.5% of the U.S. population) falling victim to identity fraud in 2010, down from 11m. in 2009. However, the cost of resolving identity crime in the U.S. has grown, with victims having to spend much more time to clear their names in 2010 compared to previous years. This is apparently due to an increase in *new* account fraud which takes longer to detect and resolve than existing account fraud.[15]

2.4 Criminal Code Offences

The *Criminal Code* was amended in January 2010 to include new offences specifically targeting identity-related crime, most notably s.402.2 (identity theft) and s.56.1 (theft/fraud re: government-issued identity documents). At the same time, s.403 was renamed from "personation" to "identity fraud".

Sections 56.1, 402.2 and 403 are now the key provisions for identity crime in Canada. However, many other *Criminal Code* offences may be implicated in a given identity crime. Possible charges that should be considered by police officers in a given case of identity crime include the following:

Offence Name	Section	Description
Identity Theft*	402.2(1)	obtaining or possessing identity information with intent to use the information deceptively, dishonestly or fraudulently in the commission of a crime *NB: Convictions under this section entitle the victim to special restitution for expenses to re-establish their identity*

* Note: the definition of "identity information" in s.402.1 includes information "purporting to identify an individual", so this section can be used even where no real person has been victimized.

[13] Criminal Intelligence Service of Canada, *Report on Organized Crime 2010.*
[14] US BJS 2008 survey.
[15] Javelin Strategy and Research, 2011 Identity Fraud Survey Report, Consumer Version.

Procuring, possessing, or trafficking in government-issued identity documents	56.1	e.g., SIN card, driver's licence, health insurance card, birth certificate, death certificate, passport, immigration status document, citizenship certificate, Indian status certificate, employee ID card with photo and signature (see s.56.1(3))
Identity Fraud	403(1)	deceptive use of the identity information of another person, living or dead, in connection with offences involving fraud, deceit or falsehood *NB: Convictions under this section entitle the victim to special restitution for expenses to re-establish their identity*
Trafficking in identity information	402.2(2)	
Theft	322	
Theft from mail	356	
Possession of stolen property	354	
Credit card- related offences	342; 342.01	covers stealing, forging, possessing and using cards; possessing credit card data; card forgery instruments; NB: "credit card"includes debit card (see s.321)
Unauthorized use of computer	342.1, 342.2	Possession, use, trafficking of device to forge cards, etc.
Fraud	380	
Forgery	367	
Uttering or possessing forged document	368	
Possession of forgery instrument	368.1	
Forgery of passport	57	
Immigration fraud	58	fraudulent use of a certificate of citizenship
Executing a false document	374	
Forged trade-mark	407	
Passing off	408	
Uttering forged money	452(a)	
Counterfeiting	376	
Possession of counterfeit money instruments	458(d)	

False pretence or false statement	362	
Personating a police officer	130	
Perjury	131	
Obstructing justice	139(2)	
Organized crime	467.11ff	

2.5 Other Relevant Domestic Laws

Identity crimes may involve violations of other criminal and civil Canadian laws, including those listed below. In some cases, another investigative agency (e.g., Competition Bureau, Canadian Border Services Agency) may be involved under its legislation. In other cases, the victim may be able to pursue compensation under civil law rights of action (e.g., consumer protection and privacy legislation).

Federal legislation

Immigration Act, s.122: Possession, use, or dealing in identity documents for the purpose of contravening the Immigration Act constitute indictable offences. See s.123 for penalties.

Competition Act, s.52: A false or misleading representation made for the purpose of promoting a business interest constitutes a hybrid offence. This could apply to criminal businesses that purport to be trusted entities in order to lure people into providing their personal information, which is then used in identity fraud. Note: under s.74.01 of the Competition Act, false or misleading representations may also be treated as a "reviewable conduct", determined on a civil burden of proof and punishable by "administrative monetary penalties". Also, under s.36 of the Act, a person who has suffered loss or damage due to conduct contrary to s.52 may sue the wrongdoer for damages.

Anti-Spam/Online Protection Act (Bill C-28, Royal Assent Dec.15, 2010): New civil legislation expected to come into full effect by late 2011 prohibits false or misleading representations online, the installation of computer programs without consent, the altering of transmission data, and the sending of commercial electronic messages without consent. Under this law, the CRTC and Competition Tribunal can impose administrative monetary penalties of up to $1m on individuals and $10m on organizations for violations under their respective Acts, and those affected can sue for damages. The federal Privacy Commissioner can also take measures against computerized collection of personal information and unauthorized compiling or supplying of lists of electronic addresses. Individuals affected by violations of this Act can sue for damages. The obstruction of an investigation under this Act constitutes an offence.

Personal Information Protection and Electronic Documents Act: This civil law requires that organizations in the course of commercial activity obtain the informed consent of individuals to the collection, use and disclosure of their personal information, except in

specifically listed circumstances. It also requires that safeguards be established to protect personal information from loss, theft or unauthorized access. Proposed amendments (as of February 2011) would require that organizations that suffer a security breach exposing personal information to potential abuse notify affected individuals. The Act sets up a regime under which complaints of non-compliance can be made to the federal Privacy Commissioner, who investigates and renders non-binding findings. Complainants can then apply to Federal Court for a binding ruling and remedies as against the organization. It is an offence for an organization not to cooperate with the Privacy Commissioner in an audit or complaint investigation under the Act.

Privacy Act: This statute puts limits on the federal government's collection, use and disclosure of personal information. Unlike private sector data protection laws and some provincial public sector data protection laws, this outdated statute does not include a requirement for the government to take reasonable security precautions with respect to personal data in its possession.

Provincial legislation

Consumer protection legislation: Most provinces prohibit unfair and deceptive business practices, and treat them both as offences punishable by fine and/or imprisonment as well as civil wrongs actionable by consumers. Like the federal *Competition Act*, these laws are directed at legitimate businesses rather than criminals.

Credit reporting legislation: All provinces, other than New Brunswick and the three territories, have legislation regulating credit bureaus (e.g., Equifax and TransUnion). Although these laws vary by province, they generally apply the same duties to credit bureaus: accuracy of recorded data, basing personal credit information on the best evidence available, corroboration of unfavourable personal credit information, limits on disclosure of credit data, free provision of credit report to individuals upon request annually, procedure for correction of errors in report. It is an offence punishable by fine to supply false credit information or to otherwise violate the Act.

Privacy legislation: Alberta, British Columbia and Quebec each have their own private sector data protection legislation similar to the federal *Personal Information Protection and Electronic Documents Act* described above. These laws apply to provincially-regulated businesses only (PIPEDA applies to provincially regulated businesses in other provinces, and to federally regulated business across Canada). A key difference between PIPEDA and the three provincial private sector data protection laws is that the provincial Privacy Commissioners in Alberta, B.C. and Quebec can make binding orders against those violating the Act. Alberta's law (s.37.1) requires notification of affected individuals in the case of data security breaches.

All provinces and territories, like the federal government, have separate laws designed to protect data held by their governments. Such privacy statutes are typically combined with "access to information" provisions, and have titles such as *"Freedom of Information and Protection of Privacy Act"* or *"Access to Information and Protection of Privacy Act"*. Some provinces also have separate legislation governing the treatment of personal data in the health sector. In most cases, these laws include provisions requiring that government

institutions take reasonable security measures to protect personal data from theft, loss or unauthorized access. The health privacy laws in Ontario and Newfoundland & Labrador require that individuals be notified of security breaches involving their personal data.

2.6 International Context of Identity Crime

Identity crime knows no borders and is increasingly transnational in nature. International organized crime groups are known to engage in identity crime in order to conceal their identities as well as to earn profit for their other criminal activities. And the internet now permits criminals to gather, trade and fraudulently use identity information from victims anywhere in the world. This poses challenges for victims as well as for investigators and prosecutors.

There are many efforts underway at the international level to facilitate cross-border investigation and prosecution of identity crime. These include:

Consumer Sentinel Network: This is a secure investigative cyber-tool and complaint database, restricted for use by participating civil and criminal law enforcement agencies. Operated by the U.S. Federal Trade Commission, the database includes identity crime and other consumer-related complaints from Canada and other countries as well as the U.S. Members can use the network to search the complaint database and share complaints with other law enforcement agencies, as well as to learn how to work together with private sector companies and consumer organizations to combat identity fraud and other consumer complaints. See www.ftc.gov/sentinel

econsumer.gov: This initiative of The International Consumer Protection and Enforcement Network (ICPEN) allows consumers to lodge complaints about cross-border online fraud with consumer protection authorities in any of the 26 participating countries. Incoming complaints are shared via the Consumer Sentinel network with participating consumer protection law enforcers who may use the information to investigate suspect companies and individuals, uncover new scams, and spot trends in fraud. See www.econsumer.gov

IC3: The Internet Crime Complaint Centre receives, develops, and refers complaints about internet-based crime to relevant authorities, as long as either the victim or the offender is located in the United States. See www.ic3.gov

POLCYB: The Society for the Policing of Cyberspace – based in B.C., this international association of police, government, academics and industry works to enhance international partnerships among public and private professionals to prevent and combat crimes in cyberspace. See http://www.polcyb.org

INTERPOL: The International Criminal Police Organization is actively involved in combating payment card fraud, information technology crime, transnational organized crime and other criminal activity related to identity crime. Interpol assists domestic law enforcement agencies through operational support, database services (e.g., counterfeit payment card database) and police training. See http://www.interpol.int

Efforts to assist victims of identity crime recover their reputations tend to be national in scope. This makes sense given that remedial laws, policies and mechanisms are domestic.

- For a list of key resources for victims of identity crime in the U.S., see Appendix H.
- In the U.K., the website **www.identitytheft.org.uk** provides identity crime victims with contact information for relevant authorities and other useful information on how to prevent and deal with identity crime.

International organizations and initiatives can nevertheless offer guidance to states in developing appropriate, effective victim assistance at the domestic level.

The United Nations, through its Office on Drugs and Crime (UNODC), has been leading initiatives to address identity crime, including the needs of victims, at the international level. Starting with the release of a study on "Fraud and the criminal misuse and falsification of identity" in 2007 and on the basis of its mandates arising from ECOSOC resolutions 2004/26 and 2007/20, UNODC has launched a consultative platform on identity-related crime which aims to bring together senior public sector representatives, business leaders, international and regional organizations and other stakeholders to pool experience, develop strategies, facilitate further research and agree on practical action against identity-related crime. Part of this work involves developing tools to help Member States "adopt useful practices and efficient mechanisms for supporting and protecting victims of economic fraud and identity-related crime…"[16] Links to UNODC tools and resources on identity-related crime can be found on the following webpage: http://www.unodc.org/unodc/en/organized-crime/index.html?ref=menuside

2.7 International Law Relevant to Identity Crime

Various international agreements, conventions and other instruments oblige State Parties to take measures relevant to the prevention, detection, investigation, and prosecution of identity-related crime as well as to the treatment of victims. Canada is a State Party to many of these instruments. As a result, Canada is obliged to ensure that it can meet these obligations and may be required to pass domestic legislation or take other

domestic measures to implement or comply with the international agreement. While the international instrument is the ultimate source document for a given obligation, the more relevant document for Canadian law enforcement activities is the domestic law or policy implementing the international obligation. However, familiarity with the underlying international instruments is useful when dealing with foreign states in the investigation or prosecution of identity crime, especially if the foreign state is a party to the international agreement in question.

United Nations Convention Against Transnational Organized Crime: Identity crime is often part and parcel of transnational organized crime. Canada has signed and ratified[17] this

[16] ECOSOC Resolution 2009/22 of July 30, 2009.

[17] A State does not become Party to an international convention, and thus legally bound, until it ratifies the convention.

international convention, the purpose of which is "to promote cooperation to prevent and combat transnational organized crime more effectively". With respect to victims, Article 25 requires that State Parties take appropriate measures within their means to assist and protect victims of offences covered by the Convention, that they provide for compensation and restitution for such victims, and that they allow victims to present their views and concerns at appropriate stages of criminal proceedings. Article 14(2) requires that states "give priority consideration to returning the confiscated proceeds of crime or property to the requesting State Party so that it can give compensation to the victims of the crime or return such proceeds of crime or property to their legitimate owners."

United Nations Convention Against Corruption: Identity crime may also be committed in cases of corruption. Canada is a State Party to this convention, which focuses on international cooperation in the effort to prevent and combat corruption, and in asset recovery. Article 32 addresses the protection of witnesses, experts and victims, requiring among other things that each State Party "enable the views and concerns of victims to be presented and considered at appropriate stages of criminal proceedings against offenders…"

Council of Europe Convention on Cybercrime: Increasingly, identity criminals are using computer-based techniques to steal, trade and fraudulently use personal data. This international convention is designed to make investigations and prosecutions of computer-related crimes more effective, by for example facilitating the collection of electronic evidence in criminal investigations. Canada has signed but not yet ratified the *Cybercrime Convention*. Before it can ratify, Canada must amend the *Criminal Code* to provide for the expedited preservation of stored computer data, the collection of "traffic data", and other tools required by the convention. Such amendments are currently before Parliament.

The *Convention on International Civil Aviation* requires that the International Civil Aviation Organization (ICAO) adopt and amend from time to time international standards and recommended practices and procedures dealing with customs and immigration procedures, for purposes including the prevention and detection of travel document fraud. Annex 9 to this Convention sets out Standards and Recommended Practices (SARPs) for the clearance of aircraft and commercial traffic. Chapter 3 of this Annex obliges Contracting States to regularly update security features in new versions of their travel documents, and to guard against their misuse and to facilitate detection of cases where such documents have been unlawfully altered, replicated or issued. Another Standard requires States to establish controls on the lawful creation and issuance of travel documents. States are also now obliged to issue separate passports to all persons, regardless of age, and to issue them in machine readable form, in accordance with ICAO's specifications. States and airlines are required to collaborate in combating travel document fraud.

Taken together with relevant domestic laws and other international legal mechanisms such as mutual legal assistance treaties, these international conventions provide a solid framework for international cooperation in the investigation and prosecution of cross-border identity crime.

Module 3: Understanding Victims of Identity Crime

3.1 Range and Types of Identity Crime Victims

Anyone can be a victim of identity crime. Although lack of awareness can be a factor, individuals are often victimized even though they take every possible precaution to protection themselves. Moreover, there is no typical identity crime victim; individual victims of identity crime range across all demographics including age, gender, income, education, and ethnicity.

Identity crime may involve corporate and/or government targets as well as individual victims. As financial institutions increasingly offer "zero liability" fraud guarantees to consumers using their payment cards, the direct financial losses from such fraud are borne by those institutions rather than by individual victims. But corporations pass on these costs on to the general consumer base through higher prices or interest rates. Similarly, costs to governments from identity crime (in terms of financial losses as well as corrective and preventative efforts) are passed on to taxpayers.

In contrast to corporate and government targets, individual victims cannot pass on the costs of their crime to anyone else (other than the extremely rare case of a successful civil lawsuit against a perpetrator who is able to pay damages).

3.2 The Importance of Identifying and Reporting Identity Crime

In order to respond effectively to identity crime, we need to understand it. Information provided by identity crime victims is extremely valuable in this respect. Reports from victims of identity crime should therefore be identified as such and reported to the central agency responsible for statistics gathering and analysis, so that policy-makers can have access to comprehensive, accurate data on the problem.[18] The Canadian Anti-Fraud Centre (CAFC) is currently Canada's central repository for statistics on identity crime. A separate national centre for reporting unsolicited commercial email ("spam") is currently under development. Canada also participates in some international crime databases – see Module 6.2. *An important role of law enforcement agencies is to ensure that the incident reported to them is included in relevant national and international registries.*

Relatively few victims of identity crime in Canada report the incident to police.[19] Of

[18] Canada's Uniform Criminal Reporting (UCR) codes do not yet include codes for identity crimes.

[19] According to the 2008 MERC survey, only 13% of identity fraud victims in Canada report the offence to the police, and only 0.5% report to the CAFC: MeRC Working Paper #23. In the U.S., only 17% of identity crime victims surveyed in 2008 had reported the crime to law enforcement; this figure is lower (13%) for victims of payment card fraud and higher (26-28%) for victims of new account or other forms of identity fraud: US BJS 2008 survey. A higher proportion of victims reporting to the Consumer Sentinel database said that they had contacted police (35% in 2007 and 36% in 2008). This figure doubled to 72% in 2009, presumably reflecting successful public and victim education in the U.S. in recent years. See Federal Trade Commission, *Consumer Sentinel Network Data Book*, February 2010, p.12.

those who do, most are unsure of how their information was obtained by the criminal,[20] who perpetrated the crime, where the criminal is located, or even the extent to which they have been victimized. They may know very little about the crime, other than that they are being wrongly accused for debts incurred or crimes committed by another person. This does not make their report any less important or legitimate.

Often, third parties will report suspected identity crime based on a known security breach that exposed personal data, or identity documents discovered in suspicious circumstances. The individuals whose personal data has been so exposed should be immediately contacted. In the former situation, the organization or person responsible for the security breach should inform the individuals of the risk caused by the breach and of the measures that they can take to prevent or mitigate damage from consequent identity fraud. Reports of suspected or possible future identity crime should also be recorded and filed in a way that allows them to be easily referenced if/when victims come forward.

3.3 Impact of Identity Crime on Individual Victims

The impact of identity-related crime on individual victims varies widely depending on the nature and extent of the identity information compromised and the fraudulent activity in question. Personal account fraud (eg: fraudulent use of account information, PINs and passwords) is generally the least damaging to individual victims since account information can be changed easily, stopping losses upon detection and avoiding further account fraud. Moreover, direct losses as a result of account fraud are often covered by the service provider (e.g., credit card companies' zero liability policies).

Fraud involving one's personal information such as address, birth date, mother's maiden name, or government-issued identity documents (e.g., driver's license numbers, social insurance numbers and health card numbers) is much more difficult to resolve and tends to be more costly and of longer duration than mere account fraud.[21]

Victims can suffer any of the following kinds of harm:

- Direct financial loss (goods, services or cash obtained by the offender from misusing the victim's account or personal information);
- Indirect financial loss (costs incurred as a result of the crime, such as legal fees, bounced cheques, postage, phone calls, and other miscellaneous expenses);
- Lost income and opportunities due to tarnished reputation (e.g., inability to access credit or other benefits due to fraud or corrupted identity);
- Time and effort required to restore identity information and reputation;
- Harassment by creditors. debt collectors or law enforcement;
- Loss of family and social support as a result of the false accusations and reputational damage;

[20] *Ibid.* ; MERC Working Paper #23 (57% didn't know).

[21] ID Analytics, National Data Breach Analysis White Paper, 2006; cited in MeRC Working Paper #23, p.28. See also Javelin Strategy & Research, *2011 Identity Fraud Survey – Consumer Report.*

- Emotional and psychological trauma (as a result not only of the crime itself but of the difficulties encountered in remediation efforts).

Financial Loss – direct and indirect

Victims of credit card fraud are least likely to be held responsible by their service provider for the fraudulently incurred charges, assuming that they detect and report the fraud quickly. However, if the criminal gains access to the victim's bank or other accounts, victims will be held responsible unless they can convince the bank or service provider that the transactions were fraudulent.

If the criminal takes the next step and opens up new accounts or obtains loans in the victim's name, the financial damage starts to spiral and becomes more difficult to undo. Victims in such cases suffer not only direct financial losses, but the often greater indirect financial costs of a ruined credit rating, as well as time taken off work to deal with the stress and practicalities of recovering one's reputation. Victims of real estate fraud may lose title to their home.

Information on financial losses to victims from identity crime in Canada is limited but it is clear that the range of loss is wide depending on the type and extent of the crime. In October 2010, identity fraud victims reporting to the Canadian Anti-Fraud Centre reported an average of $2000 in losses.

Lost opportunities or privileges due to tarnished reputation

The most frustrating and damaging effects of identity crime on victims are those that are not easily quantifiable. Account fraud can leave the victim with a seriously damaged credit rating even if the service provider covers the direct losses. Damaged credit can leave victims unable to obtain credit or loans. Given that so many ordinary services in this day and age involve credit, the inability to access credit can deny victims access to basic services such as telephone, internet, home and automobile rental or purchase.

Time and effort in remediation efforts

Even if they do not incur direct losses due to the crime, individual victims often have to spend countless hours undoing the damage that the perpetrator has wrought to their records and reputations. In cases involving fraudulent use of identity documents (as opposed to accounts), the time and effort required is particularly significant. Remediation efforts are often frustrated by the lack of a simple process through which to certify that one is a victim and not the person who incurred the debts or engaged in the illegal activities in question. Police reports are extremely valuable to victims in this respect.

Harassment by creditors, debt collectors and others who assume that the victim is responsible

Victims of identity fraud sometimes become aware of the crime only when they are accused of failing to pay an overdue account. At this point, the account has typically been referred to collection, and the victim is unaware of it because bills have been sent to an address provided by the criminal, either through a change of address notice or when applying for

a new service under the victim's name. Debt collectors may refuse to accept the victim's explanation and instead continue to pester the victim. For victims of identity crime, this kind of harassment adds to the already significant damages that they suffer.

In some cases, the offender may use the victim's identity in the commission of other crimes. The victim may then face arrest and possible incarceration as a result of the fraud. It can be difficult for such victims to convince authorities that they are not the real criminal.

Emotional and Psychological Trauma

In more serious cases of identity crime, individual victims experience significant emotional trauma and a seemingly never-ending effort to regain their reputations. It can take hundreds of hours over a period of several months for a victim of serious identity crime to finally correct all corrupted records and restore their reputation. Most devastating can be the damage caused to family or social relationships as a result of the stress and frustrations of trying to regain control of one's identity information and financial reputation.

The symptoms of psychological trauma experienced by some identity crime victims are similar to those experienced by victims of violent crime.[22] Some victims report that the crime has had long-lasting, even permanent negative effects on their lives.[23] The psychological distress caused by the crime itself is heightened when victims encounter difficulties clearing their names.

Even in the case of deceased persons whose identities have been stolen and used fraudulently, the families of such victims may suffer emotional distress as a result of the reputational damage caused by the crime.

3.4 Understanding Individual Victims of Identity Crime

Like victims of other types of crime, identity crime victims have important needs for:

- **safety** (protection from ongoing victimization),
- **support** (referral to victim service professionals),
- **information** (about their rights and resources available to them, as well as about the status of investigation and prosecution involving their complaint),
- **continuity** (consistent information and support throughout their interaction with the justice system), and
- **justice** (a sense that law enforcement is working in their best interests by conducting a reasonably thorough investigation of the complaint and doing its part to hold the offender accountable.[24]

Some victims will be more capable than others of figuring out what they need to and of doing it themselves. Seniors and other vulnerable segments of the population need extra support and assistance. Police officers should listen to the victim to determine the level

[22] US BJS 2008 survey; Van Vliet and Dicks, University of Alberta, *Stolen Identities: A Qualitative Study on the Psychological Impact of Identity Theft*, unpublished draft paper, 2010.

[23] Identity Theft Resource Centre, Fact Sheet 301: Enhancing Law Enforcement and Identity Theft Victim Communications ["ITRC Fact Sheet 301"]

[24] See the "Seven Critical Needs of Victims Law Enforcement Must Address", chapter IV of U.S. Office for Victims of Crime, *Enhancing Law Enforcement Response to Victims: A 21st Century Strategy* (2009).

of support and advice needed, and should take the time to explain to the victim what he or she needs to do.

Victims of identity crime have particularly acute needs for information and advice on how to restore their reputations and protect themselves from further fraud. They are often double- shocked: first to learn about the violation, and second to find out that they are considered guilty by creditors, investigators and collection agents and that they bear the full burden of proving their innocence. They are further distressed to find that they have to do so separately with each creditor, document issuer, law enforcement and other affected agency, and that each has its own forms and procedures. It doesn't seem fair to them, especially if the crime was caused by someone else's negligence.

Once they realize that they are on their own in terms of remediation, victims are forced to become their own advocates. Some victims are tireless in their vigilance and determination to clear their names and see the perpetrator brought to justice. Some feel that they need to become the primary investigator in the case. These victims will put countless hours into their own investigation of the case, uncovering evidence that may or may not be useful to law enforcement.[25]

A frequent complaint of victims who contact the Identity Theft Resource Centre in the U.S. is that law enforcement doesn't treat the person as a victim and doesn't seem to care about the incident. Like other victims of crime, they need to feel that their criminal report is being taken seriously by law enforcement, that the police will back them up in their efforts to clear their names, and that they will continue to be part of the loop of any investigation. In cases of ongoing victimization, victims need to feel like they are doing something to "get the person to stop". [26]

3.5 Understanding Corporate and Government Victims

Corporations and governments are often targeted by identity criminals as sources of individual identity information that can then be used in identity fraud.
In such cases, the organization may be at fault for failing to take adequate security measures and could be sued by affected individuals. If the security breach is made public (this may be required by law depending on the breach), the organization can suffer reputational as well as financial damage.

In addition, organizations are susceptible to being defrauded by identity criminals in their roles as service providers and document issuers. Corporations may be fooled by criminals posing as customers accessing their accounts, or applying for loans or new accounts. Governments may be fooled by criminals posing as others in order to obtain financial benefits, insured health services, immigration status, tax refunds or other benefits. Governments may unwittingly allow criminals to enter the country on falsified passports, and law enforcement agencies may unwittingly arrest innocent victims whose identities have been misappropriated by criminals. As issuers of foundation identity documents (e.g., birth certificates, social insurance numbers, drivers licences, passports,

[25] ITRC Fact Sheets 301 and 302.
[26] ITRC Fact Sheet 301.

health cards), governments can also be targeted by criminals posing as others in order to obtain identity documents that they can then use to evade authorities and engage in further fraud.

Where identity criminals defraud the organization by posing as the victim, the organization may assume liability for financial losses due to the fraud, thus relieving the individual victim. On top of direct financial losses, reputational damage, and loss of goodwill, corporations and governments that have been targeted in this manner typically need to invest in system upgrades and staff training in an effort to avoid future incidents. However, the costs to corporations of such losses are ultimately passed on to the general customer base through higher prices or interest rates; likewise, the costs to governments of preventing, detecting and mitigating identity fraud are passed on to taxpayers.

In addition to the targeting described above, organizations may be directly victimized by identity criminals, when their corporate identity is misappropriated and then used to defraud individual victims. In such cases, the criminal poses as a trusted entity in order to lure the individual victim into providing their personal (e.g., account) information for use in identity fraud. Such "corporate identity fraud" can cause significant reputational damage to the victimized corporation (or government), not to mention the costs of efforts to prevent, detect and stop it. As a form of intellectual property crime, itmay be prosecuted as fraud, passing off, or other offences under the *Criminal Code*. It is also civilly actionable by the victimized corporation or government as trademark infringement under the *Trademarks Act*.

Module 4: Responding to Individual Victims of Identity Crime[27]

4.1 Role of Local Law Enforcement

The primary role of police officers and investigators is to detect and apprehend criminals. However, law enforcement also plays an important role in assisting victims of crime. By enhancing their response to victims, law enforcement agencies can increase the efficiency and effectiveness of investigations, help prevent re-victimization, and improve their reputation in the community. A commitment to assisting victims as part of policing does not require substantially more resources and benefits not only the victim but also the police force itself and the community at large. [28]

The *Canadian Statement of Basic Principles of Justice for Victims of Crime,* endorsed by all federal, provincial and territorial Ministers Responsible for Criminal Justice and incorporated in to some provincial victims' rights legislation, states among other things:

- "Information should be provided to victims about available victim assistance services, other programs and assistance available to them, and means of obtaining financial reparation" and
- "All reasonable measures should be taken to minimize inconvenience to victims".[29]

Pilot projects in the U.S. have found that by treating victims as a high priority, law enforcement agencies increase their efficiency and effectiveness through:

- expanded knowledge of and access to victims services and supports,
- greater willingness by victims to cooperate with investigation,
- potential for increased case clearance rates,
- better perception of community safety and increased confidence and trust in law enforcement,
- potential for improved crime reporting, and
- improved morale and job satisfaction.[30]

It is particularly important for police officers to build a strong working relationship with identity crime victims, who may have been financially and emotionally devastated by the effects of this crime and who present important opportunities for law enforcement in advancing the specific investigation as well as in learning more about how identity criminals operate.

In the past, law enforcement agencies have sometimes failed to respond adequately to reports of identity crime, either because the crime was not well understood, because

[27] This Module draws heavily on *Training Key #617* of the International Chiefs of Police, "Identity Crime Update: Part II (2008)". To order, see http://www.theiacp.org/idsafety/

[28] See U.S. Office for Victims of Crime, *Enhancing Law Enforcement Response to Victims: A 21st Century Strategy* (2009), ch.III: Benefits and Challenges of Enhancing Response to Victims ["US OVC *Enhancing Victim Response*"]

[29] See http://www.victimsfirst.gc.ca/serv/wvr-qdv.html

[30] US OVC, *Enhancing Victim Response.*

there was no law making identity theft a crime, or because police could not identify the venue in which the crime occurred or the perpetrator was operating. This attitude of law enforcement was frustrating to victims and damaging to the reputation of police in the community. Moreover, it failed to recognize that, in the case of identity crime, a single victim could be the tip of a large criminal iceberg.

Identity crime is now recognized as a major problem in Canada and elsewhere.[31] Now that the *Criminal Code* includes specific offences for identity theft, identity fraud, and other identity-related crimes,[32] police departments should be prepared to take identity crime complaints, initiate investigations, and lay charges or recommend charges for prosecution wherever possible.

But police should also be prepared to provide victims with the information they need to minimize the damage caused by the crime and to protect themselves from further victimization. This includes, above all, providing victims with a copy (or reference number) of the incident report.

The International Chiefs of Police *Model Policy on Identity Crime*, developed in the U.S. context, recognizes the importance of victim assistance in cases of identity crime, encouraging forces to adopt the following policy statement:

> "This law enforcement agency shall take the following measures to respond to identity crime:
> 1) record criminal complaints;
> 2) provide victims with necessary information to help restore their pre-crime status;
> 3) provide victims with copies of reports as required by federal law;
> 4) work with other federal, state, and local law enforcement and reporting agencies as well as financial institutions to solve identity crime cases;
> 5) seek opportunities to increase community awareness and prevention of identity crimes; and
> 6) provide identity crime training to officers." [33]

4.2 Communicating with the Victim[34]

It is important to manage the victim's expectations about what law enforcement can do for them and what they are responsible for doing themselves. Officers should be clear with victims about limits on their ability to investigate the crime, the time-intensive nature of fraud investigations, and the chances of a successful prosecution. They should make sure that victims understand the primary role of civil law as a mechanism for victim compensation and the limits of restitution in cases that are prosecuted. Victims need to know the hard facts up front.

---

[31] See Module 2

[32] See Module 2.4.

[33] The Model Policy goes on to provide specific procedures for completing identity crime reports, assisting the victim after the report is completed, and investigating identity crime. To obtain a copy of the Model Policy, see http://www.theiacp.org/idsafety/.

[34] See IRTC Fact Sheet 301, "Enhancing Law Enforcement and Identity Theft Victim Communications".

Victims of identity crime typically have limited information about the crime and are eager to find out how it happened, who did it, and how exposed they are to future identity fraud. Victims of identity crime involving financial institutions are often frustrated by the refusal of those institutions to provide information about the theft or fraud involving their personal information, and may press police officers to obtain such information and provide it to them.

Other than general data protection laws allowing individuals to access their personal information held by corporations and governments (see Module 7.1), Canada has no law entitling identity crime victims to information about the alleged fraudulent transactions. (This is in contrast to the U.S. where such a right exists.[35]) Nevertheless, victims should be advised to make a formal request for such information from the institution themselves, using their rights under privacy law if necessary.

Victim communication should be viewed as an ongoing part of any investigation, especially given the ongoing nature of much identity crime. Failure to maintain close contact with the victim could deprive the investigator of key new evidence in the case. It can also mean lost opportunities to improve community relations.

In cases involving large numbers of victims, efficient methods to deliver updates and solicit new evidence through secure communication channels need to be developed and used.

4.3 What Victims Need from Law Enforcement

When contacted by a victim of alleged identity crime, it is important that law enforcement move quickly - not just for investigatory purposes but also to help the victim limit the damage - by providing information, referrals and advice. See Appendix A for a printable one-page checklist for police taking identity crime complaints.

(1) The Police Report

The single most valuable thing that law enforcement can do for victims of identity crime is to provide them with a copy of the incident report (or at a minimum, with the report reference number).

A police report serves as some level of proof to creditors and others that the person is indeed a victim and is not fabricating the claim. It helps victims clear their credit reports of negative information resulting from the identity crime (e.g. bad debts) and avoid the long-term effects of a poor credit rating (e.g., being refused credit or insurance, or paying higher interest rates). A detailed police report also helps victims keep fraudulent debts from reappearing on their credit reports or ending up in the hands of a new debt collector.

Without a police report, victims may be unable to make progress clearing their name and restoring their reputations. If the police force is unwilling to provide the victim with a copy of the police report, the victim should be provided with the report number, and

[35] *Fair Credit Reporting Act*, s.609(e).

advised to provide the report number, together with contact information for the police, to credit bureaus and others.

If the victim requests a copy of the report, the officer should advise the victim that he or she may be able to obtain a copy of the report (likely redacted) by way of a formal access to information request, made under the *Privacy Act* (for RCMP) or the relevant provincial/territorial access to information law (for provincial/municipal police forces). The Information and Privacy Commissioner for their province or territory can provide further guidance on this.

See Module 4.4 and Appendix B for the information that should be included in an identity crime incident report.

(2) Advice

Law enforcement personnel should waste no time in referring victims to relevant victim support centres[36] and, if possible, in providing them with up-to-date information on what to do and who to contact in order to restore their pre-crime status. See the appendices to this manual for guides and information that police and others can provide to victims (see below).

Every hour that passes without the victim having taken mitigating measures is an hour during which the criminal may be draining accounts, running up bills, or otherwise damaging the victim's reputation. Although a victim support centre may be able to provide the victim with the same information and advice, police officers can use this opportunity to build community goodwill as well as to ensure that the victim acts quickly to stem the damage.

- See Appendix D for a three-page **Victim Self-Help Guide** that can be provided to victims. For a one-page summary version of the same guide, see Appendix DD.

- See Appendix C for an "**Identity Crime Victim Statement/Affidavit"** form that once completed by the victim, serves as a nice basis for the police report. The form is designed to provide all key information about the alleged crime. Victims should be advised to complete this form and make copies of the completed, signed and witnessed (or sworn) statement for use with creditors, document issuers and others.

Victims should also be advised, right away, to document all conversations and to preserve all documentation regarding the crime. This could be key evidence in a prosecution. They should be advised in particular to print or save electronic records that might change or disappear over time. Victims should also keep track of all expenses to which they are put in case they are able to make a restitution claim against the perpetrator.

[36] A national identity crime victim support centre for Canada is currently being established and is expected to be operational by 2012. In the meantime, victims should contact the Canadian Anti-Fraud Centre. See Appendix A for contact information.

- A useful approach for many victims is to record all actions, contacts, and other information regarding their efforts in a single journal for ease of reference. The one-page "**Identity Crime Victim Action Log**" in Appendix E is designed to help victims record their efforts and contacts made in the remediation process. More complicated cases will require more than one page.

- See Appendices I and J for **key victim resources in Canada and the U.S.** As of March 2011, a national support centre for victims of identity crime is in the process of being established – its website is expected to be operational by fall 2011 and its call centre by 2012. Its website will provide a comprehensive set of information and resources for victims of identity crime in Canada. The nation-wide call centre will provide real-time advice and counseling for identity crime victims. In the meantime, the Canadian Anti-Fraud Centre www.antifraudcentre.ca (tel: 1-888-495-8501) provides support to victims.

- **Prevention advice** for victims and the general public is available from many sources. Appendix FF is a one-page list of Prevention Tips. Appendix F is a more detailed, four-page list of Prevention Advice for victims as well as the general public.

Other useful guides for identity crime victims in Canada include:
- the RCMP's Identity Crime Victim Assistance Guide, available at www.rcmp-grc.gc.ca/scams-fraudes/victims-guide-victimes-eng.htm
- the International Chiefs of Police "Prevention toolkit" available at http://www.theiacp.org/idsafety/files/pdfs/prevention_toolkit.pdf
- the Consumer Identity Theft Kit available for reference and download at http://cmcweb.ca/eic/site/cmc-cmc.nsf/eng/fe00084.html. This Kit was developed in 2007 by a working group of government consumer professionals.

(3) An Understanding of What Happens Next in the Criminal Investigation

After taking the identity crime incident report, the police officer should explain to the victim what will happen to the report, including the likelihood that the incident will not be investigated further. The officer should explain the process that will be followed to investigate the crime (e.g., the report will be assigned to an investigative officer who will review the report and contact the victim with any follow-up questions, etc.), and how long it is likely to take. If the matter involves another jurisdiction, the victim should be advised of how that will be handled, and whether they should contact the law enforcement agency in the other jurisdiction.

The police officer taking the incident report should advise the victim that the incident report may (or will) be sent to other relevant law enforcement/ intelligence agencies and databases for their information and action as appropriate. If possible, specify the other agencies to which the report will be forwarded so that the victim is aware and can follow up with them. Knowing that their report is being shared with other law enforcement agencies communicates to victims that they are being taken seriously and builds victim confidence in the police.

Finally, if there is a chance that the matter will proceed to investigation, the victim should be provided with contact information for someone in the police force whom they can call to check on the status of the investigation.

(4) Impersonation Alert in Criminal Database File

In cases of "criminal identity theft", victims may be apprehended by law enforcement officers for crimes that they did not commit (rather, a criminal impersonating them did). Law enforcement agencies can help such victims by ensuring, after appropriate verification procedures (e.g., fingerprinting, comparison of photos with physical person, etc.) that their crime database records are flagged with an alert indicating that this individual's identity documents have been stolen and that a criminal may be impersonating the individual.

4.4 Information to Include in the Police Report

The police officer taking the initial incident report should obtain certain key information needed to assess the nature, severity and location of the crime and to make an informed determination about whether and how to proceed with an investigation. See Appendix B for a printable checklist.

Be sure to identify the type of identity crime (credit card, debit card, existing account, new account, loan, etc.) at the top of the report – this is helpful to creditors who need to review the police report in order to respond to the victim.

An in-person meeting with the victim should be set up as soon as possible by the investigating officer. Meeting the victim face-to-face is important because it allows the officer or investigator to assess the authenticity of the victim's claims more effectively. It also provides an opportunity to review and gather documentation of the crime, and to establish a good working relationship with the victim.

The victim should be instructed, in advance, to bring with them all identity documentation, all documentation about the alleged crime including any notes they have made, and a chronological log of their efforts to date in investigating the crime and mitigating damage.

A useful tool for gathering relevant victim information is the "Identity Crime Victim Statement/Affidavit" form (Appendix C). The victim should be instructed to complete this form and bring it with them, along with all supporting documentation, to the meeting.

The initial identity crime report has two purposes:
(1) for law enforcement, as the basis on which to launch an investigation, and
(2) for the victim, as a document that helps them to convince creditors and others of their innocence in their remediation efforts.
In the first meeting with the victim, or if necessary over the phone, the interviewing officer should take down the following information (see Appendix B for printable checklist):

- Identifying and contact information for each victim as necessary depending on the nature of the crime;

- Details of the suspected crime:
  - when and how it was discovered,
  - documents or information used by the criminal,
  - how the victim's information was or may have been taken,
  - location of fraudulent activity,
  - financial institutions or other organizations involved,
  - fraudulently incurred debts or other damages, etc.

- Accounts known to have been fraudulently accessed or opened by the suspect (advise the victim to get a copy of their credit report from both Equifax and TransUnion in order to identify any fraudulent accounts);

- Whether the victim authorized anyone to use their name or personal information and if so for what purposes and in what circumstances;

- Any identity information and/or personal authentication information (e.g., SIN, birth certificate, driver's licence, passport, health card, credit card, debit card, account numbers) that has been lost, stolen or potentially misappropriated and used by the criminal;

- Whether the victim is aware of any circumstances in which their personal information may have been compromised (e.g., burglary, auto theft, loss of wallet, suspicious transaction, etc.);

- Any knowledge or belief about the identity of the suspected criminal and the basis for such belief;

- Names and contact information of customer service representatives or others who have provided information to the victim about the crime;

- Any additional information or documentation that the victim can provide to assist in the investigation;

- Consent of the victim to disclose the existence of their complaint and/or the police incident report to organizations requesting confirmation of the complaint;

- Whether the victim has filed a report of the crime with any other law enforcement agency (if so, get details);

- The type of identity crime (theft, fraud, existing account, new account, credit card, debit card, etc.) – this should be specified at the top of the report to facilitate statistics gathering and reviews of the report by creditors.

The interviewing officer should be able to assess the authenticity of the victim's claims on the basis of this meeting or conversations. Unless there are strong grounds on which to suspect that the complaint is fraudulent, the officer should provide the victim with the incident report number (and if possible, a copy of the incident report) and the matter should proceed to investigation.

More information can be obtained from the victim in a second interview, after the case has been referred to investigation.

4.5 Working with Individual Victims in the Investigation of Identity Crimes

Victims of identity crime are important partners in the process of investigation and prosecution of the crime. It is natural for identity crime victims to feel a strong need to be actively involved in the investigation – after all, it is their reputation that has been damaged and their finances turned upside down. Investigators should give victims evidence-gathering tasks that will be helpful to the case.

Important evidence that the victim should obtain (or have) includes:

- A copy of their credit report from each credit reporting agency (Equifax and TransUnion), with fraudulent accounts on the report identified;
- From the credit report or creditors, addresses associated with the fraudulent accounts (to help determine where the suspect lives);
- A list of creditors and merchants where the suspect has opened accounts in the victim's name;
- A journal with the time and date of all contacts with creditors, collection agents, and others in their remediation efforts;
- A record of the impact of the crime (financial, reputational, emotional, psychological) on them and their family (for future use in the victim impact statement).

Victims should be advised to gather electronic documentation of the crime, such as screen shots, emails, chat logs, links to websites, images etc. immediately, before they are deleted.

4.6 Working with Individual Victims in the Prosecution of Identity Crimes

Once the matter proceeds to prosecution, victims can take advantage of victim assistance programs depending on the jurisdiction. In all provinces and territories, victims have the right to information about the proceeding and to a reasonable opportunity to have the impact of the offence on them brought to the attention of the court (usually via a victim impact statement as part of the sentencing process). Prosecutors should ensure that victims of the identity crime in question are so informed and offered the opportunity to submit victim impact statements to the court. Information for victims on victim impact statements can be found here:
http://www.justice.gc.ca/eng/pi/pcvi-cpcv/pub/statem-declar/index.html
http://www.crcvc.ca/docs/VictimImpactStatements.pdf
http://www.courtprep.ca/en/witnessTips/vis.asp
http://www.victimsweek.gc.ca/res/r58.html

Individual victims may be valuable witnesses in trials of identity criminals. The same rules and principles apply to identity crime victims as to others in this respect: they will need

to be briefed on court process, properly prepared for examination and cross-examination and provided with protective testimonial aids if necessary. In large scale identity crimes involving hundreds or thousands of individual victims, it can be very useful to have one or two individual victims testify as to the impact of the crime on them. This can be done most efficiently through victim impact statements.

In cases involving victims in foreign jurisdictions, it will be necessary to work with law enforcement agencies and possibly prosecutors in the foreign jurisdiction to identify and obtain evidence from those victims. Advance consideration should be given to the manner in which this evidence is obtained, with a view to ensuring its admissibility in court. See Module 6.4 for more on cross-border victim assistance.

If the offender is convicted under ss.402.2 or 403 of the *Criminal Code* (Identity Theft or Identity Fraud), the victim is entitled to restitution for financial losses attributable to the crime as well as for expenses incurred to re-establish their identity. Eligible expenses include those incurred to replace identity documents, and to correct one's corrupted credit history and credit rating (see s.738(1) of the *Criminal Code*). Victims should be made aware of the need for documentation in order for such expenses to be reimbursed, and of the limited nature of this remedy

Victims should also be advised that convicted criminals will be required to pay a fee called a "victim surcharge", but that this money does not go directly to the victim — rather, it is placed in a special fund in the province or territory (sometimes called the Victim Assistance Fund) and is used to provide services and assistance to victims of crime in general.

If the perpetrator is convicted and sentenced to a term of imprisonment, victims may be able to access funding from the federal Department of Justice, Policy Centre for Victim Issues, in order to attend Parole Board hearings. See http://www.justice.gc.ca/eng/pi/pcvi-cpcv/attend-audience.html

In large scale identity crimes involving more than a few victims (e.g., major corporate or government data breaches), it is obviously impossible to treat each individual victim in the manner suggested above. In such cases, law enforcement and prosecutors must work with the corporate (or government) victim to ensure that individual victims are provided with an opportunity to contribute useful evidence to the investigation, to provide victim impact statements, to obtain restitution in the event of successful prosecution, and to attend parole board hearings where applicable.

Module 5: Responding to Institutional Victims of Identity Crime

A given instance of identity crime typically involves two different kinds of victims: the *individual* whose personal or account information has been stolen and/or fraudulently used, and the *institutions* that have been burgled and/or defrauded. Sometimes you will be contacted first by a business or government agency reporting the theft of personal data in its possession, or the fraudulent use of its trade-mark in a phishing or other scheme designed to steal identity information from unsuspecting individuals. The following are guidelines for responding to and working with institutional victims of identity crime.

5.1 Fraudulent Use of Corporate or Government Trademark

If the case involves fraudulent use of a corporate or government trademark (e.g., logo, website), it constitutes *intellectual property crime* and may be a candidate for prosecution as such. It may also constitute an offence under the *Competition Act* (false or misleading representations). Victims of such offences have a statutory right to sue for damages even if the matter is not prosecuted. Law enforcement officials should

1. Direct the corporation or government to:

a) the RCMP's online guide entitled "Reporting Intellectual Property Crime: A Guide for Victims of Copyright and Trademark Infringement", available at http://www.rcmp-grc.gc.ca/fep-pelf/ipr-dpi/guide-eng.htm

b) the Competition Bureau to report the matter and for more information on offences and remedies under the *Competition Act:* http://www.competitionbureau.gc.ca

50 Victoria Street
Gatineau, Quebec
K1A 0C9
Telephone: 819-997-4282
Toll-free: 1-800-348-5358 (Canada)
Fax: 819-997-0324

2. Gather the information listed in the above RCMP Guide (under "Checklist for Reporting Copyright and Trademark Offences") from your corporate/government victim contact, and contact the RCMP's intellectual property crime coordinator in your region to determine whether/how to proceed with an investigation. For a list of contacts by region, see: http://www.rcmp-grc.gc.ca/fep-pelf/ipr-dpi/cont-eng.htm

3. Contact the Competition Bureau to determine whether it plans to investigate the matter, and to ensure that investigations of the same matter are coordinated.

5.2 Theft of Personal Information from Corporate/ Government Holdings

If the case involves suspected theft of customer or citizen records, it may be the first step of a potentially larger case of identity crime. It is essential that mitigating measures be taken immediately by the affected body in order to prevent identity fraud based on the stolen information. Law enforcement and prosecutors should:

1. Inform the affected (or reporting) entity that it has a responsibility to take immediate measures to prevent both further theft of data and identity crime based on the information that was or may have been stolen. This common sense responsibility is set out in various privacy-related statutes, sometimes explicitly and sometimes implicitly. Refer them to the Privacy Commissioner for their jurisdiction for further direction on their responsibilities under privacy legislation to notify affected individuals and other authorities of the breach.

2. Take down a full incident report, and file it in such a way that it can be linked to incidents of identity crime in the future. This could be relevant investigatory information if the stolen information is indeed used to commit further identity crimes.

3. Ask the reporting entity to inform you immediately if it receives information of any sort suggesting that identity crimes may occur, be occurring or have occurred based on the stolen information.

4. Keep in touch with the reporting entity and update the report accordingly.

Best Practice: *Develop a system for linking reports of identity crime over time and across jurisdictions. As part of this effort, establish a national database of lost, stolen and fraudulent identity documents.*

5.3 Working with Institutional Victims in the Investigation and Prosecution of Identity Crime

Many identity crimes involve theft of personal information from public or private sector institutions, and/or fraudulent use of corporate identities (e.g., trade-marks) to lure individuals into providing their personal information. In such cases, police officers and investigators will need to work closely with the organization in question to identify individual victims and ensure that they are properly notified and advised, as well as to investigate and prosecute the case generally.

Most identity crimes involve fraudulent use of the victim's financial accounts or fraudulent creation of financial accounts in the victim's name. In such cases, the creditors/banks/ merchants in question must be contacted to determine how the accounts were opened and to gather relevant evidence including:

- if the account was opened or accessed via the internet, relevant IP addresses;
- if the account was accessed via the telephone, any telephone number captured;

- if the account was accessed or opened in person, the employee/witness who opened the account or conducted the transaction;
- all other information about the suspicious accounts and transactions: customer records, signatures, transaction history, application forms, videos or photographs, etc.
- statements from witnesses regarding the transactions and the suspect.

Organizations may be reluctant to disclose facts about the incident, such as obvious security failures, that put them in a bad light. They may insist that certain information be treated as confidential and not disclosed to individual victims. However, the organization should be advised that they may be required by law to notify authorities and/or affected individuals of the breach,[37] and that in any case individuals are entitled to information about their accounts under privacy/access to information legislation.[38]

[37] See s.37.1 of the Alberta *Personal Information Protection Act*; and Bill C-29, proposed amendments to the federal *Personal Information Protection and Electronic Documents Act* as of March 2011.

[38] See *Personal Information Protection and Electronic Documents Act*, Schedule 1, Principle 4.9 and similar rights under provincial and territorial data protection legislation requiring that organizations provide individuals with access to their personal information held by the organization, upon request.

Module 6: Coordinating Victim Response with Other Agencies

6.1 Roles, Responsibilities and Best Practices in Identity Crime Victim Remediation

It is important that all parties understand their roles and responsibilities in the process of victim remediation. As discussed in Modules 4 and 5,

- *individual and institutional victims* are primarily responsible for taking the steps necessary to mitigate damage to themselves and to restore their pre-crime status;
- *institutional victims* are additionally responsible for limiting damage to those individual victims whose information or accounts were compromised as a result of the crime; and
- *law enforcement agencies* play an important role in educating and assisting victims in their remediation efforts.

The following is a summary of roles and responsibilities (best practices as well as legal obligations) in victim remediation, by party. Note that this does not the many preventative measures that should be taken by all parties as a matter of course.

Police

- Investigation and reporting
  - record all complaints alleging identity crime
  - ensure that the incident report is forwarded to appropriate authorities for further investigation and possible linkage to other reports
  - ensure that information from the incident is entered into relevant databases for future reference as well as statistical purposes
  - investigate the alleged crime, working with victims to gather evidence and with law enforcement agencies in other jurisdictions as necessary
  - assist other law enforcement agencies with information and cooperation in connection with identity crime investigations that they are conducting
- Victim assistance
  - provide incident report number (or copy of report) to victim for use in remediation efforts
  - if possible, provide victim with information on how to restore their pre-crime status (e.g., copy of Appendices to this Manual)
  - refer victim to the appropriate victim support centre for further advice and assistance
  - in cases that are clearly the sole responsibility of another law enforcement agency, refer victim to the appropriate law enforcement agency
  -

Other law enforcement agencies *(e.g., Competition Bureau, Consumer Protection Agencies, Canadian Border Security Agency)*

- Investigation and reporting

- identify complaints of identity crime and enter into relevant databases for statistical purposes as well as future law enforcement reference
- to the extent possible, ensure that complaints of identity crime are investigated
- cooperate with police and other law enforcement agencies in the investigation of identity crime (domestic and cross-border)

• Victim assistance
- refer victim to police for purposes of criminal incident report, as appropriate
- provide victim with information on how to restore their pre-crime status
- refer victim to the appropriate victim support centre for further advice and assistance

Individual Victims

• Damage detection, prevention and mitigation
- notify banks, creditors, service providers, document issuers, Canada Post (as appropriate) and cancel all compromised payment cards immediately upon discovering the theft or fraud
- obtain copy of credit reports and notify credit bureaus (Equifax and Transunion) + relevant creditors of any fraudulent transactions
- have fraud alert placed on credit files and monitor credit report for fraudulent activity
- if possible and desired, obtain "credit freeze" directing the credit bureau not to provide your credit information to anyone other than existing creditors without your express consent to each such disclosure
- keep identity information and documents secure and monitor accounts in order to prevent and detect further fraud

• Remediation and compensation
- take steps necessary to obtain new identity documents
- pursue rights and remedies under civil law to eliminate or reduce liability for fraudulent transactions and to obtain compensation for losses (See Module 7.1 and/or Appendix I)
- document all remediation efforts and expenses incurred
- monitor progress of investigation and prosecution, and request restitution in the event of successful prosecution

• Investigation and reporting
- report to relevant law enforcement and regulatory agencies
- cooperate with law enforcement

Corporate and Government Victims

• Assistance and Damage Mitigation re: individual victims
- identify and notify affected individuals of security breaches involving their personal information and advise them on steps to take to avoid or mitigate damages
- do not hold individuals liable for losses due to fraud beyond their control

- Investigation and reporting
  - report to relevant law enforcement and regulatory agencies
  - cooperate with law enforcement
- Remediation and compensation
  - if possible, sue criminal for civil damages

Identity document issuers and government benefits providers

- Victim assistance
  - provide claimants (victims) with a fair and expeditious process for establishing the veracity of their claims and obtaining new identity documents
- Investigation
  - cooperate with other law enforcement agencies in identity crime investigations
  - investigate and track reports of lost, stolen or corrupted identity documents

Creditors, Financial Institutions, Service Providers, Utilities

- Victim Assistance and Damage Mitigation
  - take proactive measures to monitor accounts for fraudulent activity and notify account-holders immediately of suspicious activity
  - notify affected individuals of security breaches involving their personal data and advise them on steps to take to avoid or mitigate damages
  - notify consumers of any adverse decision made on the basis of their credit report and assist consumers in obtaining a copy of their credit report
    if a fraud alert appears on a consumer's credit file, do not approve the application for credit without due diligence
  - take extra precautionary measures when approving applications or issuing credit where there are any claims or evidence of identity fraud
  - cease attempting to collect debts from consumers where reason to believe that they have been the victim of identity fraud
  - cease providing information from fraudulent transactions to credit bureaus
  - provide victim with information about fraudulent transactions involving their personal information
  - upon request by victim, provide information about fraudulent transactions directly to law enforcement
  - provide victim with information and advice on how to limit damages and recover their pre-crime status (e.g., a victim recovery toolkit)
  - refer victim to the appropriate victim support centre

Credit Bureaus

- Victim assistance
  - inform victims of their rights and remedies with respect to credit reporting
  - provide victims with information and advice on how to recover their pre-crime status (e.g., a victim recovery toolkit), as well as referral to the appropriate victim support centre

- provide victims of identity crime with free access to their credit file without delay
- provide victims with information on sources of information in their credit file

- Damage Mitigation
  - corroborate unfavourable information about consumers before including it in the consumer's credit file
  - place fraud alerts on consumer credit files immediately upon request by a consumer
  - notify creditors of allegedly fraudulent transactions involving them
  - upon request by a consumer, freeze the consumer's credit such that only specified creditors have access to the report without transaction-specific approval by the consumer
  - block the reporting of information where the consumer provides evidence that it was a result of identity fraud
  - expunge credit records that have been proven to be based on fraudulent transactions
  - notify furnishers of allegedly fraudulent credit information of the fraud claim

Debt Collectors

- Damage Mitigation
  - notify creditors of alleged fraud
  - cease attempting to collect debts from consumers who formally attest they have been a victim of identity fraud

Prosecutors

- Victim assistance
  - ensure that victims are aware of their right to information and participation in the case, as well as to restitution
  - if requested, provide the victim with updates on the case, an opportunity to participate via a victim impact statement, and an opportunity to claim restitution
- Prosecution
  - cooperate as necessary with other law enforcement agencies and prosecutors in order to obtain admissible evidence (e.g., victim impact statements) from victims regardless of their location

6.2 Coordinating with Other Government/Law Enforcement Agencies to Assist Victims

There are numerous federal and provincial government agencies that may be involved in any particular incident of identity crime. Coordination among these agencies is necessary for victim assistance as well as for national statistics gathering and the investigation of overlapping criminal and regulatory offences.

The Criminal Intelligence Service of Canada (CISC) is tasked with facilitating the timely production and exchange of criminal information and intelligence within the Canadian

law enforcement community. See http://www.cisc.gc.ca. At the international level, Interpol works to improve collaboration among law enforcement agencies. For a model bilateral police co-operation agreement, see http://www.interpol.int/Public/ICPO/LegalMaterials/cooperation/Model.asp

As of March 2011, federal and provincial law enforcement and government agencies are working on a National Identity Crime Strategy that should improve victim assistance in part through more effective coordination among government agencies. In the meantime, law enforcement can assist by:
a) ensuring that all relevant statistics-gathering, investigatory and prosecutorial agencies are informed of the reported incident;
b) coordinating efforts and sharing information with other investigatory agencies as appropriate; and
b) directing victims to the appropriate agencies for reporting and assistance.

Databases to which the incident should be reported

In addition to the local police force database, the complaint should be reported to other relevant national and international databases for use in cross-border investigations and statistics-gathering. In some cases such as the CAFC, , victims can report their complaint directly to the agency; in others, such as Interpol databases, the report must be made by a law enforcement official.

Canadian Anti-Fraud Centre – national repository of mass market fraud complaints
Box 686 North Bay, Ontario P1B 8J8
Telephone (toll-free): 1 (888) 495-8501
Local or outside Canada/US: 1 (705) 495-8501
Fax: 1 (888) 654-9426
Email for law enforcement only: le@antifraudcentre.ca
Email for victims and public: info@antifraudcentre.ca

Interpol - Counterfeit Payment Cards Database
See http://www.interpol.int/Public/CreditCards/Default.asp

Consumer Sentinel Network – international database of identity theft and consumer fraud complaints for use by registed law enforcement agencies only
See https://register.consumersentinel.gov/ or call the Consumer Sentinel HelpLine at 1.877.701.9595

Internet Crime Complaint Centre – takes complaints about internet-based crime directly from victims via an online form and refers them to relevant authorities, as long as either the victim or the offender is located in the United States.
www.ic3.gov

Econsumer.gov – a web portal for individual victims to report complaints about online and related transactions with foreign companies and to have their complaints shared with consumer protection authorities in the other jurisdiction. Complaints lodged with

econsumer.gov are automatically shared with the Consumer Sentinel Network.
www.econsumer.gov

Agencies that may assist in investigation or prosecution

Canada Post Security – if mail theft or redirection suspected
1-800-267-1177 (for public)

Competition Bureau – re: misrepresentations in the commercial context
Monday - Friday, 8:30 a.m. to 4:30 p.m., Eastern Time.
Toll-free: 1 800 348-5358
TDD (for hearing impaired): 1 800 642-3844
Fax: (819) 997-0324

Canadian Border Security Agency – re: immigration fraud
Border Watch toll-free line: 1-888-502-9060
Local criminal investigation units:
http://www.cbsa-asfc.gc.ca/contact/investigation/contact-eng.html
Criminal intelligence (immigration fraud): nat-nt-fraud@cbsa-asfc.gc.ca
Criminal intelligence (human trafficking): cbsa-humantraffic@cbsa-asfc.gc.ca

Citizenship and Immigration Canada – re: immigration fraud
1-888-242-2100
TTY services: 1-888-576-8502

Privacy Commissioner – if involves government or private sector breach

> **Privacy Commissioner of Canada** (federal government or private sector)
> Toll-free: **1-800-282-1376**
> Local or outside Canada: **(613) 947-1698**
> Fax: **(613) 947-6850**
> TTY: **(613) 992-9190**
> http://www.priv.gc.ca/
>
> **Provincial/Territorial Information and Privacy Commissioner** (prov/terr government, or private sector in Alberta, B.C., or Quebec). For contact information, see http://www.priv.gc.ca/resource/prov/index_e.cfm

Provincial Consumer Protection authorities – re: misrepresentations/fraud in the consumer context. See http://www.consumerhandbook.ca/en/contacts/provincial-territorial-offices

Agencies providing assistance to individual victims

Canadian Identity Theft Support Centre – not yet established; will provide information, advice and support to victims of identity crime across Canada via a website (expected fall 2011) and national call centre (expected 2012)

Canadian Anti-Fraud Centre – SeniorBusters - offers assistance and support to Canadian seniors who are victims of mass marketing fraud
http://www.antifraudcentre-centreantifraude.ca/english/cafc_seniorbusters.html
Box 686 North Bay, Ontario P1B 8J8
Telephone (toll-free): 1 (888) 495-8501
Local or outside Canada/US: 1 (705) 495-8501
Fax: 1 (888) 654-9426
Email for victims: info@antifraudcentre.ca
Email for law enforcement only: le@antifraudcentre.ca

Federal Ombudsman for Victims of Crime – information and guidance to victims of crime generally
http://www.victimsfirst.gc.ca/abt-apd/wwa-qsn.html
P.O. Box 55037, Ottawa, Ontario K1P 1A1
Telephone (toll-free): 1-866-481-8429
Local or outside Canada: 613-954-1651
TTY (Teletypewriter): 1-877-644-8385
E-mail: victimsfirst@ombudsman.gc.ca
Fax: 613-941-3498

Policy Centre for Victim Issues, Justice Canada – directs victims generally to local victim support services and offers funding for victims to attend parole board hearings
http://www.justice.gc.ca/eng/pi/pcvi-cpcv/index.html
Department of Justice Canada
284 Wellington Street
Ottawa, Ontario
Canada K1A 0H8
Fax: (613) 952-1110
E-Mail: webadmin@justice.gc.ca

6.3 Coordinating with the Private Sector to Assist Victims

The private sector plays an important role in victim assistance generally, and in the case of financial identity crime, that role is critical. Corporations targeted in a particular incident or set of incidents (ie: corporate victims) are responsible for notifying individual victims, advising them how to minimize damage, and covering losses in many cases. However, other corporations also play important roles in victim assistance. See Module 6.1 for a list of responsibilities by type of organization.

In specific cases, law enforcement agencies can help by directing the victim to organizations that can assist the victim to restore the victim's pre-crime status. If private sector organizations require confirmation that a consumer has been a victim of identity crime, the police should confirm incident report to the organizations upon request.

More generally, law enforcement agencies need to build ongoing collaborative relationships with the private sector with a view to streamlining victim assistance as well as investigations of identity crime. Current initiatives in this respect include:

- the Private Sector Liaison Committee of the Canadian Chiefs of Police
- The Society for the Policing of Cyberspace (POLCYB) – an international association of police, government, academics and industry representatives that works to enhance international partnerships among public and private professionals to prevent and combat crimes in cyberspace; based in B.C.; see http://www.polcyb.org

6.4 Dealing with Inter-jurisdictional Challenges in Victim Assistance

Where the identity crime involves more than one jurisdiction (within Canada or internationally), coordination with other law enforcement agencies and/or regulatory authorities is required to investigate and prosecute the alleged crime. But coordination may also be required for effective victim assistance: victims may need to contact document issuers, credit reporting agencies and other organizations in the other jurisdiction in order to prevent further damage and to restore their reputations. As well, victims may be able to obtain help from victim assistance organizations in the other jurisdiction.

The first step is to determine which jurisdictions are involved. This can be difficult when the location of the perpetrator is unknown, as is often the case with computer-based identity crime. Computer forensic investigations may be required.

Once all engaged jurisdictions have been identified, the relevant law enforcement agencies should be contacted and a determination made about which agency should take the lead in investigating the crime. That agency should then contact the victim(s) and ensure that they are aware of their rights and have taken appropriate preventative and corrective actions.

A number of regional inter-agency partnerships exist for the purpose of coordinating law enforcement response to certain types of cross-border fraud.[39] Depending on the case, one or more of these partnerships could be helpful in coordinating law enforcement response to victims.

Interpol provides a model police co-operation agreement on its website. See http://www.interpol.int/Public/ICPO/LegalMaterials/cooperation/Model.asp

In cases that proceed to prosecution, it may be necessary for prosecutors to arrange for the giving (or receiving) of testimony by victims remotely (video-conferencing). If this assistance is required from outside of Canada, mutual legal assistance can generally be arranged by contacting:

[39] E.g., Atlantic Partnership (re: US-Atlantic Canada fraud); Toronto Strategic Partnership (re: Ontario-U.S. fraud); C.O.L.T. (Centre of Operations Linked to Telemarketing fraud); Alberta Partnership Against Cross-Border Fraud; Project Emptor (B.C.-U.S. deceptive marketing scams); Vancouver Strategic Alliance (B.C.-U.S. fraud and deceptive marketing).

Director-General
International Assistance Group
Department of Justice Canada
284 Wellington Street
Ottawa, Ontario K1A 0H8
Tel. 613-957-4832
Fax. 613-957-8412

Module 7: Identity Crime Victim Rights and Remedies

7.1 Legal rights and remedies for identity crime victims in Canada

Identity crime victims in Canada have certain legal rights and remedies that may assist them in detecting the problem, mitigating damages, restoring their reputation, and obtaining redress. Many of these legal rights and remedies are provided under provincial law and therefore vary by jurisdiction. See Appendix I for this information in tabular form.

Detection and Mitigation

Especially where the victim's information was obtained from a third party, it is important that victims are notified and that the third party takes reasonable steps to prevent fraudulent use of that information. The federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA") and similar provincial legislation require that organizations protect personal information under their control "by security safeguards appropriate to the sensitivity of the information".[40] It can be argued that implicit in this general requirement are duties to detect and report suspected fraud, as well as to take extra precautions to authenticate individuals where evidence of identity fraud exists. However, only Ontario and Manitoba explicitly require the latter, and only in situations where a fraud alert has been added to a consumer credit file.[41]

Most identity crime involves financial fraud. In addition to common law duties of care, all provinces but New Brunswick have consumer reporting legislation requiring that credit bureaus take reasonable measures to ensure that the information they report on consumers is accurate, complete, based on the best evidence available, and corroborated if unfavourable.[42] Data protection legislation applicable in all provinces also requires that organizations take reasonable measures to ensure the accuracy of personal information they hold, and affected individuals can pursue enforcement and redress under most regimes.[43]

Alberta is the only jurisdiction so far to have enacted a general legislative duty to notify individuals of security breaches involving their personal data.[44] Under the Alberta law,

---

40 PIPEDA Schedule 1, Principle 4.7; Alberta *Personal Information Protection Act*, s.34; B.C. *Personal Information Protection Act*, s. 34; Quebec *Act Respecting the Protection of Personal Information in the Private Sector*, ss.10, 20.

41 Ontario *Consumer Reporting Act*, ss.12.1-12.3; Manitoba *Personal Investigations Act*, s.12.1.

42 B.C. *Business Practices and Consumer Protection Act*; Alta *Fair Trading Act (Credit and Personal Reporting Reg);* Sask *Credit Reporting Act;* Man *Personal Investigations Act;* Ont. *Consumer Reporting Act; Civil Code of Quebec;* NS *Consumer Reporting Act;* NL *Consumer Reporting Agencies Act;* PEI *Consumer Reporting Act.*

43 PIPEDA Schedule 1, Principle 4.6; Alberta *Personal Information Protection Act*, s.33; B.C. *Personal Information Protection Act*, s. 33; Quebec *Act Respecting the Protection of Personal Information in the Private Sector*, ss.11.

44 Alberta *Personal Information Protection Act*,s.37.1.

organizations must notify the Privacy Commissioner first, and must notify affected individuals only if so required by the Commissioner. Ontario and Newfoundland require notification of data security breaches involving health information only.[45] Bill C-29, currently before Parliament,[46] would add a security breach notification requirement to PIPEDA. If passed, organizations subject to PIPEDA will be required to notify the Commissioner of any "material breaches" of security affecting their holdings of personal information, and to notify affected individuals if it is "reasonable" in the circumstances to "believe that the breach creates a real risk of significant harm to the individual".[47]

Credit bureau practices are critical in mitigating damages due to financial identity fraud. Ontario and Manitoba are the only jurisdictions in Canada to require that credit bureaus place fraud alerts on consumer files upon request by the consumer or otherwise.[48] Canadian credit bureaus do, however, voluntarily offer fraud alerts in other provinces.

Most provinces requires that credit reporting agencies give consumers the right to one free copy of their credit report per year,[49] and credit bureaus offer the same in those jurisdictions where it is not legislatively required. This allows consumers to detect identity crime. Additional credit monitoring services are offered by credit bureaus and other commercial entities for a fee.

Liability for Fraudulently Incurred Debts

Although not required to do so by law, credit card companies in Canada have voluntarily adopted zero liability policies for "card not present" transactions, and limited liability in other situations. The *Canadian Code of Practice for Consumer Debit Card Services*[50] encourages banks not to hold consumers liable for fraudulent debit card transactions where reasonable precautions were taken, but actual bank practices vary in this regard, and the code does not (yet) apply to electronic banking.

Real estate and mortgage fraud is a growing problem, and some jurisdictions have legislated protection for homeowners in this regard after highly-publicized cases in which unsuspecting homeowners lost title to their homes as a result of identity fraud.[51]

Compounded Victimization

One of the most frustrating problems for victims of identity crime is the often compounded nature of their victimization. Not only do they need to repair their finances and reputations,

---

45 Ontario *Personal Health Information Protection Act*, ss.12(2), 16(2); Newfoundland & Labrador, *Health Information Act*, ss.15, 20(3).

46 40th Parliament, 3rd Session.

47 Proposed new sections 10.1 and 10.2.

48 Ontario *Consumer Reporting Act*, ss.12.1-12.3; Manitoba *Personal investigations Act*, ss.12.1-12.4.

49 Except in BC where there is no provision with respect to access, credit reporting laws in all other provinces specify that a consumer has the right to access their credit report. Some provinces state that the report shall be provided free of charge (SK, ON, NS, NL and PEI). A report requested in Alberta must be provided free of charge once a year, and "reasonable fees"' may be charged for additional reports. In Manitoba, credit bureaus may charge $5 per report.

50 See http://www.fcac-acfc.gc.ca/eng/industry/RefDocs/DebitCardCode/DebitCardCode-eng.pdf

51 See for example *Ontario Consumer Protection and Service Modernization Act, 2006*; Alberta *Land Titles Amendment Act, 2006.*

but they often find themselves treated like criminals and subjected to repeated harassment by debt collectors. Most provinces and territories have legislation governing debt collectors and proscribing overly aggressive debt collection practices. But only seven of the thirteen provinces and territories prohibit collection agencies from continuing to attempt collection where the consumer claims that they are not the debtor (and/or states that they would prefer for the matter to be taken to court).[52]

Restoration of Reputation

Most but not all provincial credit reporting laws require that credit bureaus notify those to whom they have disclosed incorrect information of the inaccuracy. The time period for such notification ranges from 60 days to one year. Similar duties to notify apply to corrected data under data protection laws, but only where "appropriate" in most jurisdictions.

Compensation

The *Criminal Code* (s.738(1)(d)) allows victims of identity crime to claim restitution for expenses incurred "to re-establish their identity, including expenses to replace their identity documents and to correct their credit history and credit rating" in addition to general restitution for direct losses due to the crime. However, restitution is applicable only in the small proportion of cases that are prosecuted and result in convictions, and where the criminal has the means to pay restitution. Restitution may therefore be helpful for a few victims of identity crime, but it is unlikely to be a meaningful remedy for the vast majority of victims.

In the event that the perpetrator is convicted and sentenced to a term of imprisonment, victims of identity crime may be eligible for funding to attend Parole Board hearings involving the perpetrator. Call 1-866-544-1007 or see http://www.justice.gc.ca/eng/pi/pcvi-cpcv/attend-audience.html

There are a number of common law causes of action that could be used by victims to sue identity criminals and/or facilitators of identity crime for damages. However, Canadian courts are reluctant to award damages for "pure economic loss", making such actions risky. Statutory rights of action are therefore more promising.

Under PIPEDA, individuals can ultimately take complaints of privacy violations to Federal Court and can obtain damages for humiliation as well as actual expenses incurred.

However, as noted above, the Federal Court has stated that an award of damages should only be made under PIPEDA "in the most egregious situations."[53]

Alberta and B.C. consumer protection and data protection legislation include private

[52] B.C. *Business Practices and Consumer Protection* Act, ss.116(4); Alberta *Trade Practices Act, Collection and Debt Repayment Practices Regulation,s.12(1)(k)*; Manitoba *Consumer Protection Act*, s.98; Ontario *Collection Agencies Act*, Regulation 103/06, s.22; New Brunswick, *Collection Agencies Act*, s.14(1)(l); Quebec *Act respecting the collection of certain debts*, s.3(2.1); N.W.T. *Consumer Protection Act, Debt Collection Practice Regulations*, ss.11, 13. Note: under Ontario and NB legislation, the debtor must provide notice to the collection agency by registered mail in order for this provision to have effect.

[53] *Randall v Nubodys Fitness Centres, 2010 FC 681 (CanLII), para.55.*

rights of action for damages as a result of violations of statutory provisions such as those applicable to credit bureaus. Other provinces, however, do not provide for such private rights of action in their relevant legislation.

Justice

Identity crime victims quite understandably usually want to see their perpetrators brought to justice and appropriately sentenced. Under ss.402.2 and 403 of the *Criminal Code*, identity criminals may be sentenced to imprisonment of up to five years for identity theft and ten years for identity fraud. Theft from mail (s.356), and trafficking in forged documents (s.368) are also subject to a maximum ten year sentence, while trafficking in identity documents is subject to a maximum five year sentence (s.56.1).

In the event that the offender is prosecuted, identity crime victims have the same rights as other victims of crime to information about and participation in criminal proceedings. Under s.722 of the *Criminal Code,* victims are entitled to file and read a Victim Impact Statement at the time of sentencing an offender. Under the *Corrections and Conditional Release Act*, victims are entitled to disclosure of certain information about the offender.[54] As well, all provinces have laws providing victims with similar rights to information about the offender and formally recognizing the needs of victims (e.g., legislating the Canadian Statement of Basic Principles of Justice for Victims of Crime).[55] Through the Policy Centre for Victim Issues (Justice Canada), victims may be able to obtain funding to attend Parole Board hearings involving their offenders.[56]

7.2 Legal Gaps in the Canadian Approach to Victims of Identity Crime

Compared to laws in the United States, Canadian law lacks a comprehensive set of rights and remedies for victims of identity crime, leaving victims without information or effective recourse that could otherwise be made available. See Appendix I for a table setting out existing legal rights and remedies under Canadian law, along with corresponding provisions under U.S. law, by issue. Below is a description of the gaps in Canadian law relating to consumer protection and victim assistance with respect to identity crime.

Awareness

Legal rights and remedies are of limited use if individuals are unaware of them. For this reason, U.S. legislators require that credit bureaus provide identity crime victims with a "Statement of Rights" approved by the Federal Trade Commission ("FTC").[57] As well, the FTC is legislatively tasked with the duty to maintain a central internet and telephone-based service providing information and assistance (e.g., complaint referrals) to victims of identity crime.[58] No such initiatives have been taken in Canada, legislatively or otherwise.

---

54 See ss.26(1) and 142(1).

55 These statutes are typically entitled "Victims of Crime Act", "Victims Bill of Rights" or "Victim Services Act".

56 See http://www.justice.gc.ca/eng/pi/pcvi-cpcv/attend-audience.html

57 U.S. *Fair Credit Reporting Act* ["FCRA"], 15 USC 1681, s.609(d)

58 *Identity Theft Assumption and Deterrence Act*, s.5.

Detection and Mitigation

Although there is widespread support for mandatory data breach notification laws in Canada, Alberta is the only jurisdiction so far to have enacted such a law applicable across sectors.[59] Almost all U.S. states now require notification of data security breaches to authorities and affected individuals.[60]

In the U.S., consumers have the right to place fraud alerts on their credit files, and indeed to have this done by all three credit bureaus through a single request.[61] Creditors are required to take extra steps to authenticate applicants where a fraud alert appears. As noted above, Ontario and Manitoba are the only jurisdictions in Canada to legislate such requirements.

Of more value to many identity crime victims than fraud alerts are credit freezes, which, as the name suggest, stop the reporting of consumer credit information unless approved by the consumer on a transaction-specific basis. Such freezes are far more effective in both preventing and detecting identity fraud, since they do not rely on creditors to take extra precautionary measures (as in the case of fraud alerts), but simply deny access to the credit report. Almost all U.S. states now require that credit freezes be offered to identity crime victims. [62] Yet, no Canadian jurisdiction requires this and credit bureaus do not voluntarily offer it in Canada.

In the U.S., federal legislation entitles every consumer to a free copy of their credit report annually, and to additional copies in the case of identity crime victims.[63] Although most provinces give consumers the right to one free copy of their credit report per year, not every province has legislated this as a consumer right.[64] Moreover, credit bureaus interpret this as allowing one free *hard copy* report, which must be ordered or obtained in person. Credit bureaus charge for electronic access to one's credit report (which may be necessary in order for the victim to act in a timely way), and for more than one hard copy per year.

Liability for Fraudulently Incurred Debts

Identity crime victims in Canada have no legislated protections from liability for losses due to identity fraud beyond their reasonable control. In contrast, the U.S. *Fair Credit Billing Act* protects consumers from liability for fraud in the case of "card-not-present" transactions, and limits consumer liability to $50 in cases of lost or stolen cards as long as the consumer has notified the company of the loss promptly upon discovery.[65] In addition, the U.S. *Electronic Fund Transfers Act* limits consumer liability for fraudulent electronic fund transfers, depending on how quickly the loss is reported.[66] Furthermore, most states have legislation limiting consumer liability for new accounts that have been fraudulently established.[67]

---

59 *Personal Information Protection Act*, s.37.1.
60 See http://www.ncsl.org/default.aspx?tabid=13489
61 FCRA, s.605A
62 See http://www.ncsl.org/default.aspx?tabid=12516
63 FCRA, ss.612(a), (c) and (d).
64 See Footnote 51.
65 15 USC 1666, ss.161-162.
66 15 USC 1693ff and 12 CFR 205.
67 See http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/rights.html under "Limiting Your Loss From Identity Theft".

Although some provinces (e.g., Ontario, Alberta) have legislated consumer protections against losses due to real estate and mortgage fraud, not all have done so.

Compounded Victimization

As noted above, most provinces and territories have legislation proscribing overly aggressive debt collection practices. However, unlike U.S. law, there is no Canadian law requiring debt collectors to notify the creditor of alleged fraud once made aware, nor is there any requirement for creditors not to send accounts to collection when they have been notified that the account resulted from identity fraud.[68]

Credit bureaus can play an important role in stemming the damage to victims of identity crime by stopping the reporting of alleged fraudulent transactions, and by notifying their credit-granting customers of alleged fraudulent transactions. Although they are required to do so under U.S. law,[69] there is no similar explicit statutory duty in Canada.

In the U.S., an entire industry has built up around serving those victimized or fearful of being victimized by identity crime. While some of the services offered are worthwhile for victims, many charge high prices for services that are free and easily accessed directly by victims themselves. Without proper self-help guidance, those who have suffered identity crime can thus be further victimized by unscrupulous entrepreneurs.[70] This new industry is unregulated in both the U.S. and Canada.

Restoration of Reputation

Identity crime victims need, above all, to restore their reputations. In order to do so, they need to be able to prove that they are victims of fraud. And in order to do that, they need documentation regarding the fraudulent transaction(s) in question. But other than a general right under data protection laws to access their personal information held by organizations, Canadians have no rights to information regarding transactions conducted

fraudulently in their names. Nor has any program or process been established in Canada to facilitate the restoration of identity crime victims' reputations.

In the U.S., identity crime victims have statutory rights to obtain information from businesses and debt collectors about alleged fraudulent transactions, and the right to have such information provided directly to police or other governmental authorities.[71] U.S. authorities have also established a process to facilitate the issuance of detailed police reports in identity crime cases.[72] As explained in Module 4, this is the single most important service that law enforcement can provide to victims of identity crime, as it provides the basis on which victims can convince creditors to correct their records.

Some U.S. states have also established "Identity Fraud Passport" programs for victims of

---

68 FCRA, s.615(f)

69 FCRA, s.615(g)(1)

70 See Privacy Rights Clearinghouse, Fact Sheet 33: "Identity Theft Monitoring Services".

71 FCRA, s.609(e)

72 See FTC *Guidebook for Assisting Identity Theft Victims*, s.II B, "The Primary Tools to Show that the Victim is Not Responsible for the Fraud and to Correct Credit Reports", <http://www.idtheft.gov/probono/docs/i.%20Table%20of%20Contents.pdf>

criminal identity fraud. Under such programs, victims concerned about being arrested for crimes they did not commit can apply for a "passport" certifying that they are victims of identity fraud.[73] Australia has also adopted a process for the issuing by a court magistrate of "victim's certificates" to individuals who can demonstrate that they are the victim of identity theft and likely to be impersonated in the commission of an offence.[74]

No such programs exist in Canada. In 2008, the joint civil/criminal section working group on Identity Theft of the Uniform Law Conference of Canada reviewed the potential for "victim assistance options for erroneous criminal justice records" in Canada and identified a number of obstacles to adopting victim certification or related processes in the Canadian context. They concluded that more research and analysis was needed before any such programs could be recommended for Canada.[75]

Moreover, creditors are required, under U.S. law, to expunge fraudulent accounts under certain conditions.[76] No such legislative requirement exists in Canada, although it could be argued that the general duty to ensure accuracy of personal information under Canadian data protection laws encompasses such measures.

Several U.S. states now have laws requiring that inaccurate information in the criminal records of identity crime victims be expunged or corrected.77 No such laws exist in Canada.

Compensation

Criminal injuries compensation legislation applies only to victims of violent crime and therefore does not assist identity crime victims.

As noted above, s.738(1) of the *Criminal Code* allows victims of identity crime to claim restitution for expenses incurred "to re-establish their identity, including expenses to replace their identity documents and to correct their credit history and credit rating", in addition to general restitution for any direct losses due to the crime. It is not clear whether "costs of re-establishing one's identity" include the value of time spent by victims in remediation efforts; this will be a matter for courts to determine. In contrast, U.S. legislation expressly permits restitution for the value of time reasonably spent by the victim in remediation efforts, in addition to out-of-pocket expenses incurred in the restoration process.[78]

While victims of identity crime can sue identity criminals and/or facilitators of identity crime (if it is possible to identify them) for damages, few provinces explicitly provide for rights of action relevant to identity crime victims, and even in the event of success, there is no guarantee of a damage award sufficient to justify the expense of a lawsuit. In contrast,

---

73 See http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/state-crim-passport.html
74 *Criminal Code Act 1995*, Part 9.5 – Identity Crime, Division 375 – Victims' certificates.
75 Uniform Law Conference of Canada, *Report of the Joint Criminal/Civil Section Working Group on Identity Theft: A Progress Report* (August 2008).
76 FCRA, s.611(a)(5), s.623(b)
77 See http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/state-crim-expunge.html
78 *Identity Theft Enforcement and Restitution Act*, 18 USC 3663(b)(6) and 3663(c)(1)(A)

the U.S. *Fair Credit Reporting* Act includes statutory rights of action wilful or negligent non-compliance with the Act.[79] In addition, a number of U.S. states have specific statutory rights of action for identity crime, some permitting treble damages and attorney fees.[80]

Justice

Maximum sentences for convicted identity criminals in the U.S. are higher than in Canada where certain other offences are involved: under the *Identity Theft Assumption and Deterrence Act*, the maximum sentence is 10, 15 or 20 years, depending on the nature of the crime.[81] As well, under the *Identity Theft Penalty Enhancement Act,* offenders convicted of identity theft during and in relation to other crimes are not eligible for probation, must serve sentences for each crime consecutively, and cannot have one sentence reduced to take into account the other sentence.[82]

Conclusion: Legislative Gaps

Clearly, victims of identity crime in Canada would benefit from law reform designed to provide them with both additional protection (through more specific obligations on credit bureaus and others handling their personal information) and rights to information and assistance in the remediation process. The U.S., having recently gone through a policy process designed to achieve just that, offers a useful model for Canadian policy-makers.[83]

7.3 Policy Gaps in the Canadian Approach to Victims of Identity Crime

National Statistics on Identity Crime

The first step in responding effectively to identity crime is to understand it. This requires the gathering and reporting of national statistics on the nature and incidence of identity crime and its impact on victims in Canada. Canada has very little in the way of publicly reported data on identity crime. The Canadian Centre for Justice Statistics *Uniform Crime Reporting Survey,* which gathers official crime statistics from police forces, does not yet track identity crimes as such.[84] Moreover, Statistics Canada has noted that better measurement of fraud in Canada could be obtained through a survey of businesses rather than police.[85] There is an obvious need for the systematic gathering of Canadian data on identity crime and its impact on individual victims.

---

79 Ss.616, 617.

80 See Jeffrey Dion and James Ferguson, "Civil Liability for Identity theft", (Feb 1, 2007); online at http://goliath.ecnext.com/coms2/gi_0199-6285492/Civil-liability-for-identity-theft.html

81 18 USC 1029

82 18 USC 1028A

83 See President's Identity Theft Task Force Report (Sept.2008), www.idtheft.gov

84 See http://www.statcan.gc.ca

85 Statistics Canada, *A Feasibility Report on Improving the Measurement of Fraud in Canada, 2005* (April 2006), Catalogue no. 85-569.

Inter-jurisdictional coordination among law enforcement agencies

Another gap in Canada's response to identity crime is limited coordination among law enforcement agencies in the investigation and prosecution of identity criminals who operate across jurisdictions. On top of all their other challenges in achieving remediation, victims in such cases face the challenge of dealing with law enforcement agencies in different jurisdictions, who may be unwilling to share information with each other or to coordinate investigations. Current efforts to improve coordination among law enforcement agencies need to be expanded in order to deal effectively with the growing proportion of crime that is trans-provincial and trans-national in nature.

A National Strategy on Identity Crime

In June 2010, the RCMP undertook to lead the development of a National Identity Crime Strategy. This Strategy is being developed through broad consultation with private and public sector stakeholders that are directly affected by identity crime. It focuses on preventing identity crimes, whether through information provided to Canadians or through more robust processes and systems. As of March 2011, the Strategy has three priority areas: Criminal Intelligence and Analysis; Prevention, Awareness and Victim Assistance; and, Effective Enforcement, Disruption and Prosecution. As victim assistance is a component of the Strategy, it is anticipated that stakeholders representing the consumer and victim perspective will be included in the development of the Strategy and that a plan will be developed to address gaps in Canadian law relating to consumer protection and victim assistance.

At the same time, various Canadian public and private sector institutions are working on initiatives to combat identity crime and to assist identity crime victims. For example, privacy commissioners, consumer protection agencies, law enforcement agencies, financial institutions, credit bureaus, and others are all engaged in their own consumer/victim awareness efforts. The Identity Theft working group of the Consumer Measures Committee, a federal/provincial/territorial committee established under the Agreement on Internal Trade, published "Identity Theft" information kits for consumers and businesses in 2007[86] and is now working on harmonization of credit reporting laws. Some but not all provinces have moved forward with law reforms designed to assist identity crime victims. The Private Sector Liaison Committee of the Canadian Chiefs of Police is working to improve the coordination and sharing of fraud prevention and awareness information among stakeholders. The Federal Victims Strategy - led by the Policy Centre for Victim Issues (Justice Canada) and including partners in Public Safety Canada, the Public Prosecution Service of Canada, Correctional Service Canada, and the Parole Board of Canada - is researching victim needs and funding national initiatives with respect to identity crime victims. It is hoped that these and other related initiatives will be coordinated under the new National Strategy.

[86] See http://cmcweb.ca/eic/site/cmc-cmc.nsf/eng/fe00084.html

Appendices

Appendix A. Guide for Police Officers Receiving Identity Crime Complaints
Appendix B. Information to Include in the Police Report
Appendix C. Identity Crime Victim Statement/Affidavit form
Appendix D. Identity Crime Victim Self-Help Guide – detailed version
Appendix DD. Identity Crime Victim Self-Help Guide – summary version
Appendix E. Identity Crime Victim Action Log
Appendix F. Identity Crime Prevention Tips – detailed version
Appendix FF. Identity Crime Prevention Tips – summary version
Appendix G. Resources for Identity Crime Victim in Canada
Appendix H. Resources for Identity Crime Victims in the USA
Appendix I. Legal Rights and Remedies for ID crime victims in Canada (Table)
Appendix J. References

APPENDIX A

Guide for Police Officers Receiving Identity Crime Complaints

- ❑ Take a formal report about the incident.
  - Give the report number to the victim.
  - If possible, give the victim a copy of the report.

    Victims need to be able to refer creditors to your report in order to clear debts and other fraudulent transactions made in their name.

- ❑ See separate checklist for information to include in your report.
  - If possible, have the victim provide you with a completed *Identity Crime Victim Statement/Affidavit* (Appendix C) and attach it to your report.

- ❑ Advise victims that they are responsible for remediation and should keep a complete diary of their efforts and expenses, as well as all evidence regarding the crime.

  Victims of identity crime may be suffering severe psychological distress and may need support in order to take appropriate steps.

- ❑ Give individual victims a copy of the following documents or refer them to www.icclr.law.ubc.ca, from where they can download the forms and documents:
  - Identity Crime Victim Self-Help Guide (Appendix D or E)
  - Identity Crime Victim Log of Steps Taken (Appendix F)
  - Identity Crime Victim Statement /Affidavit form (Appendix C)
  - Prevention Tips (Appendix G or H)
  - Resources for Identity Crime Victims in Canada (Appendix I)

- ❑ Advise victims to complete the Identity Crime Victim Statement/Affidavit (Appendix C) and to make copies of the completed form for use with creditors, credit bureaus, and any other agencies who need proof of the crime.

- ❑ Advise victims to contact the Canadian Anti-Fraud Centre (1-888-495-8501) (refer victims to the new Canadian identity crime victim support centre once operational)

- ❑ If the victim is from the U.S. or if the crime appears to have taken place in the U.S.,
  - give the victim a copy of Resources for ID Crime Victims in the U.S. (Appendix J)
  - forward your incident report to the appropriate U.S. agency.

- ❑ If the crime appears to have taken place in another country, forward your incident report to the appropriate law enforcement authority or to Interpol for forwarding

- ❑ Refer corporate and government victims to:
  - the RCMP Guide for Victims of Intellectual Property Crime (for trademark infringement) available via the RCMP's website (www.rcmp-grc.gc.ca)
  - the Competition Bureau (for misleading representations)
  - the Office of the Privacy Commissioner of Canada (security breaches)

- ❑ Ensure that information about the incident is included in all relevant databases (domestic and international) for statistical and investigatory purposes. See Module 6.2 for a list of relevant databases.

APPENDIX B

Identity Crime Checklist: Information to include in the police report

*NOTE: The **Identity Crime Victim Statement/Affidavit** form provides an efficient way for the victim to provide this information. See Appendix C to this Manual.*

- ❑ Identifying and contact information for each victim: date of birth, telephone, email and postal addresses, prior addresses.
- ❑ Details of the suspected crime:
  - when and how it was discovered,
  - documents or information used by the criminal,
  - how the victim's information was or may have been taken,
  - location of fraudulent activity,
  - financial institutions or other organizations involved,
  - fraudulently incurred debts or other damages, etc.
- ❑ Accounts known to have been fraudulently accessed or opened by the suspect (advise the victim to get a copy of their credit reports from both Equifax and TransUnion in order to identify any fraudulent accounts);
- ❑ Whether the victim authorized anyone to use their name or personal information and if so for what purposes and in what circumstances;
- ❑ Any identity information and/or personal authentication information (e.g., SIN, birth certificate, driver's licence, passport, health card, credit card, debit card, account numbers) that has been lost, stolen or potentially misappropriated and used by the criminal;
- ❑ Whether the victim is aware of any circumstances in which their personal information may have been compromised (e.g., burglary, auto theft, loss of wallet, suspicious transaction);
- ❑ Any knowledge or belief about the identity of the suspect and the basis for such belief;
- ❑ Names and contact information of customer service representatives or others who have provided information to the victim about the crime;
- ❑ Any additional information or documentation that the victim can provide to assist in the investigation;
- ❑ Consent of the victim to disclose the existence of their complaint and/or the police incident report to organizations requesting confirmation of the complaint;
- ❑ Whether the victim has filed a report of the crime with any other law enforcement agency (if so, get details).
- ❑ Specify the type of identity crime (theft, fraud, existing account, new account, credit card, debit card, etc.) at the top of the report - this will facilitate statistics gathering and reporting.

APPENDIX C

Victim's Name _____ Phone Number _____

IDENTITY CRIME VICTIM STATEMENT/AFFIDAVIT

This is a voluntary form for victims of identity crime to use when dealing with police, creditors, credit reporting agencies, and others in an effort to clear their records. The form is available online at www.icclr.law.ubc.ca

Before completing this form:
1. Place a fraud alert on your credit reports, and review the reports for signs of fraud.
2. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.

I, _____ , state as follows:
(name)

About You (the victim)

1. My full legal name is: _____
First Middle Last Suffix
2. My commonly-used name *(if different from above)* is: _____
First Middle Last
3. My date of birth is (y/m/d): _____/____/____
4. My address is: _____

   City: _____ Province/Territory: _____ Postal Code: _____
5. I have lived at this address since: _____
6. My home phone number is: _____ cell _____
7. My business phone number is: _____
8. I prefer to be contacted by phone at: _____
9. My email address is: _____
10. My identity document numbers are:
    *(*leave this blank until you provide this form to someone with a legitimate business need, such the police or a credit reporting agency, and only provide the information requested).*

    Social Insurance Number: _____

    Drivers Licence Number: _____

    Health Card Number: _____

At the Time of the Fraud *(Skip this section if your information has not changed since the fraud)*

11. My full legal name was:_____
First Middle Last Suffix

12. My address was: _____

13. My phone numbers were: _____
Home Business

14. My email address was: _____

Declarations

15. I ❑ did/ ❑ did not authorize anyone to use my name or personal information to seek the money, credit, loans, goods or services , or for any other purpose, as described in this statement.

16. I ❑ did/ ❑ did not receive any benefit, money, goods or services as a result of the events described in this statement.

17. I ❑ am/ ❑ am not willing to work with law enforcement if charges are brought against the person who committed the fraud.

18. If you answered "did" to question 15 or 16 above, explain here:

_____

_____

_____

_____

Identity Verification

19. I can verify my identity and address with the following documents (check all that apply):
    - ❑ Passport
    - ❑ Driver's Licence (with photo)
    - ❑ government-issued health card with photo
    - ❑ Other valid, government-issued photo ID (specify) _____
    - ❑ Birth Certificate
    - ❑ Official school record showing enrolment and legal address (if under 16 and no photo ID)
    - ❑ Proof of residency during the time the disputed charges occurred, the loan was made, or other event took place (e.g., a copy of a rental/lease agreement in my name, a utility bill, or an insurance bill)

Information about the Incident

This information notifies companies that an incident has occurred and it allows them to investigate your claim. Depending on the details of your case, each company may need to contact you with further questions.

20. I became aware of the incident through: _____

21. My identification document(s) (eg: driver's licence, passport, SIN card, birth certificate, health card) were:
    - ❑ lost on or about (y/m/d) _____/____/____
    - ❑ stolen on or about (y/m/d) _____/____/____
    - ❑ never received

    Additional information (e.g. which cards, circumstances): _____

22. I believe the following person used my information or identification documents to open new accounts, use my existing accounts, or commit other fraud: *(enter the information that you know)*

    Name: _____
    First Middle Last Suffix

    Address: _____

    Phone numbers: _____

    Additional information about this person: _____

23. Additional Comments (for example, a description of the incident, what information was used or how a possible identity thief gained access to your information): *Attach additional sheets as necessary*

About the Information and/or Accounts

24. The following personal information (e.g., my name, address, SIN, date of birth, etc.) in my credit report is inaccurate as a result of the identity crime:

    (A) _____

    (B) _____

    (C) _____

25. Credit inquiries from these companies wrongly appear on my credit report as a result of this identity crime:

    Company Name: _____

    Company Name: _____

    Company Name: _____

Below are the details about the different frauds committed using my personal information:

Name of Institution — Contact Person — Phone — Extension Account Number — Routing Number — Affected cheque number(s) Account Type: ☐ Credit ☐ Bank ☐ Phone/Utilities ☐ Loan ☐ Government Benefit ☐ Internet or Email ☐ Other Select One: ☐ This account was opened fraudulently. ☐ This was an existing account that someone tampered with. Date Opened or Misused (mm/yyyy) — Total Amount Obtained ($)	26. If there were more than three frauds, copy this page blank, and attach as many additional copies as necessary. Enter any applicable information that you have, even if it is incomplete or just an estimate. If the thief committed two types of fraud at one company, list the company twice, giving information about the two frauds separately.
Name of Institution — Contact Person — Phone — Extension Account Number — Routing Number — Affected cheque number(s) Account Type: ☐ Credit ☐ Bank ☐ Phone/Utilities ☐ Loan ☐ Government Benefit ☐ Internet or Email ☐ Other Select One: ☐ This account was opened fraudulently. ☐ This was an existing account that someone tampered with. Date Opened or Misused (mm/yyyy) — Total Amount Obtained ($)	**Contact Person:** Someone you dealt with and whom the police or other investigator can call about this fraud.
Name of Institution — Contact Person — Phone — Extension Account Number — Routing Number — Affected cheque number(s) Account Type: ☐ Credit ☐ Bank ☐ Phone/Utilities ☐ Loan ☐ Government Benefit ☐ Internet or Email ☐ Other Select One: ☐ This account was opened fraudulently. ☐ This was an existing account that someone tampered with. Date Opened or Misused (mm/yyyy) — Total Amount Obtained ($)	**Account Number:** The number of the credit or debit card, bank account, loan, or other account that was misused. **Amount Obtained:** For instance, the total amount purchased with the card or withdrawn from the account.

27. *If the incident involved a mortgage, provide the following information:*

Lender's Name and Address: _____

Date of Registration: _____

Legal Description of Property: _____

Municipal Address of Property: _____

Registration Number of Mortgage: _____

Documentation of the Fraud

28. I can provide the following documentation as proof of the fraud: *(identify any supporting documentation that you can provide that helps to establish the fraudulent nature of the transactions in question. Attach legible copies – not originals – to this statement.)*

- ❑ A copy of the incident report completed by the police or other law enforcement agency
- ❑ Other supporting documentation (describe): _____

_____

_____

_____

_____

Law Enforcement Report

Having the police complete an incident report about your complaint will make it easier for you to convince creditors of the fraud and to clear your records. Ask a police officer to witness your signature on this Statement. Be sure to get the reference number for the police report. When sending this statement to creditors and credit reporting agencies, attach a copy of any confirmation letter or official police report that you are able to get.

29. I ❑ have / ❑ have not reported the events described in this document to the Police

30. The Police ❑ did / ❑ did not complete a report.

31. I filed my complaint with the police:
    - ❑ in person (location: _____)
    - ❑ by telephone
    - ❑ by email, fax, mail, or other method (specify: _____)

If you have contacted the police or other law enforcement agency, complete the following:

Law Enforcement Agency _____ Name of Officer _____

Report number _____ Badge Number _____

Date of Report_____ Phone Number _____

Protecting Your Privacy

I agree that companies and agencies to whom I provide this Identity Crime Statement may use and share the personal information in it **only for the purposes of** investigating the incident described in the Statement, prosecuting the person(s) responsible and preventing further fraud or theft. The companies may disclose the information to law enforcement agencies for these purposes,

The companies to whom I provide this Identity Crime Statement agree that this information may not be used or disclosed for any other purposes except as authorized by law. If this document or information contained in it is requested in a law enforcement proceeding (e.g. before a court or tribunal), the company may have to provide it or disclose it.

Signature

All statements I have made on this form are true and complete in every respect to the best of my knowledge and belief, and are made in good faith. I understand that this Statement may be made available to federal, provincial or municipal law enforcement authorities for such action within their jurisdiction as they deem appropriate. I understand that knowingly submitting false information in this Statement could subject me to criminal prosecution.

_____ _____

Signature Witness

_____ _____

Printed name Printed name

_____ _____

Date Date

_____

Telephone number

Affidavit

Some companies or authorities may require that your statement be sworn (i.e., provided in the form of an Affidavit). If so, you will need to sign and swear that the contents of your statement are true, in the presence of a Notary Public or Commissioner of Oaths. DO NOT SIGN in advance.

_____ _____

Signature Notary Public or Commissioner of Oaths

_____ _____

Printed name Printed name

_____ _____

Date Date

_____

Telephone number

APPENDIX D

Identity Crime Victim Self-Help Guide (detailed version)

If you discover that you have been the victim of identity theft or fraud, you need to take steps immediately to minimize the damage and prevent further fraud.

Document everything, *including notes on who you talked to (name, title, contact info.), when, and what they said. Print off copies of electronic records. These records could be invaluable if you have a disagreement with a creditor, as proof of your victimization if the identity fraud persists, or as proof of the time and effort you spent should you ever be able to claim compensation for these efforts. Use a table such as that provided at the end of this checklist to keep track of all this information.*

- ❑ Identify all lost, stolen or compromised payment cards, cheques, account information and/or identity documents. Review your bank account, credit card, and other suspect account records and identify all unauthorized transactions. Determine if you are missing any account statements normally received by mail.

- ❑ **If your debit card, credit card, or other financial instrument has been compromised, contact the financial institution and report the theft/ fraud.** Call the telephone number on the back of the card if you have it. Have them cancel the compromised cards and issue new ones. If you don't report lost, stolen or compromised debit or credit cards immediately, you may be liable for fraudulent transactions. Put a "stop payment" on any stolen cheques.

- ❑ Contact each of Canada's main credit reporting agencies:
  Trans Union Canada at www.tuc.ca (1-866-525-0262 Québec 1-877-713-3393)
  Equifax Canada at www.equifax.ca (1-866-779-6440)
  - **Request a copy of your credit report** – this report will show accounts that have been opened in your name, and creditors who have made inquiries about you because you, or someone pretending to be you, applied for credit from them. You will need to provide proof of your identity to the credit bureau in order to get a copy of the report. The report should be free of charge if ordered by mail or in person. Online credit monitoring is available but subject to charge.
  - **Request that a fraud alert be placed on your file, alerting creditors that they need to take extra precautions to verify identity before granting credit to someone purporting to be you** – confirm with the credit bureau how long the fraud alert will be left on your file, and what effect it will have on creditors.
  - **If you want to stop all issuing of credit in your name without your transaction-specific approval, ask the credit bureau if it will provide such a "credit freeze" to you.** Credit bureaus in the U.S. provide this service.

- ❑ **If an account (bank, utility, telephone, etc.) has been fraudulently accessed or set up in your name, contact the service provider and have the account cancelled and closed.**
  - Ask what address is on the account and note any addresses that are not yours. Contact Canada Post regarding any fraudulent addresses (see below).
  - Ask that any new requests for service first be confirmed with you.
  - Have the service provider note on the account that it was closed at your request because of identity fraud.

- **If the service provider provided the criminal with unauthorized credit, money, information, goods or services in your name, ask them to investigate the occurrence. Find out:**
  - What information does the company need to start an investigation?
  - Has the company already started a criminal investigation? If so, with which police force? What is the report number?
  - What do you need to do to have your losses reimbursed?

❑ If you are missing mail and suspect that it has been redirected to another address, contact Canada Post at www.canadapost.ca (1-800-267-1177)

*Use the **Identity Crime Victim Statement** (online at www.icclr.law.ubc.ca) to notify financial institutions, creditors, service providers, document issuers, police, etc. of the fraud, to establish your innocence, to get replacement documents, and to provide the information they need to start an investigation.*

❑ **Report the crime to your local police force.**
- Provide the police with all relevant information and documentation as requested. The Identity Theft Statement form is useful in this respect.
- **Request a copy of the police report** to show creditors and document issuers so that they will believe that you are a victim of identity crime. If you can't get a copy of the report, at least get the report number.
- **Take down the name and title of the police officer** whom you should contact with additional information about the crime.
- If the crime involves another country, your local police force will report the incident either to the law enforcement in the other country or to Interpol who will forward the request for assistance or information to the relevant foreign law enforcement agency.

❑ **Once you have a copy of your credit report, review it carefully.** Note any accounts that appear to have been fraudulently opened in your name, and any inquiries by creditors to whom you did not apply for a service. **Contact each of those creditors and follow the steps set out above for dealing with fraudulent accounts.**

❑ **Report and replace any government-issued identity cards** (e.g., SIN, birth certificate, health card, drivers licence) by contacting Service Canada at 1-800-O-Canada (1 800 622-6232) or TTY: 1 800 926-9105. An agent will be able to direct to the appropriate federal or provincial organization to replace each of your cards.
- For information on replacing your **Social Insurance Number** due to fraud, see http://www.servicecanada.gc.ca/eng/sc/sin/index.shtml
- If your **passport** has been lost or stolen, contact Passport Canada at
  1-800-567-6868 TTY services: 1-866-255-7655
  Outside Canada and the United States: 819-997-8338
  http://www.passport.gc.ca
- If your **immigration documents** have been lost or stolen or if you suspect that someone is using them fraudulently, contact Citizenship and Immigration Canada at
  1-888-242-2100 TTY services: 1-888-576-8502
  http://www.cic.gc.ca

- ❑ Report the theft or fraud to the **Canadian Anti-Fraud Center** by going to their website or by calling **1-888-495-8501.** The CAFC is the central agency in Canada for information and criminal intelligence on identity crime. The CAFC provides valuable assistance to law enforcement agencies all over the world by identifying connections among seemingly unrelated cases. Your information may provide the piece that completes the puzzle.

- ❑ For advice on privacy issues related to the identity crime, contact the Privacy Commissioner of Canada (1-800-282-1376 or www.priv.gc.ca). The Office of the Privacy Commissioner can investigate data breaches by corporations or governments which may lead to personal information being used to commit identity crime. Some provinces have adopted their own private-sector privacy laws, which are enforced by provincial privacy commissioners:
  - Quebec http://www.cai.gouv.qc.ca
  - Alberta http://www.oipc.ab.ca
  - British Columbia http://www.oipc.bc.ca

- ❑ Monitor your credit report, bank statements, and mail with a view to detecting any additional fraud, mail diversion or other criminal activity. Consider setting up an online alert to monitor any online activity in your name - see http://www.google.com/alerts

APPENDIX DD

Identity Crime Victim Self-Help Guide (short version)

- ❑ If your debit card, credit card, or other financial instrument has been compromised, contact the financial institution and report the theft/ fraud immediately.

- ❑ **Contact both of Canada's national credit reporting agencies:**
  Trans Union Canada at www.tuc.ca (1-866-525-0262 Québec 1-877-713-3393)
  Equifax Canada at www.equifax.ca (1-866-779-6440)
  - Request a copy of your credit report
  - Ask that a fraud alert be placed on your file

- ❑ Identify all lost, stolen or compromised payment cards, cheques, account information and/or identity documents. Review your bank account, credit card, and other suspect account records and identify all unauthorized transactions. Determine if you are missing any account statements normally received by mail.

- ❑ **Once you have a copy of your credit report, review it carefully.** Note any accounts that appear to have been fraudulently opened in your name, and any inquiries by creditors to whom you did not apply for a service.

- ❑ **Report the crime to your local police force.**
  - Give the police all the information you have about the crime.
  - **Get the report number** so that you can refer creditors to it.

- ❑ **Complete the Identity Crime Victim Statement/Affidavit form,** make copies, and provide a copy to each creditor whose records need to be corrected.

- ❑ If you are missing mail and suspect that it has been redirected to another address, contact Canada Post at www.canadapost.ca (1-800-267-1177)

- ❑ Report and replace lost or stolen government-issued identity cards (e.g., SIN, birth certificate, health card, drivers licence) by contacting Service Canada at 1 800 622-6232 or TTY: 1 800 926-9105. An agent will direct to the appropriate federal or provincial organization to replace each of your cards.
  - If your passport has been lost or stolen, contact Passport Canada at 1-800-567-6868 TTY: 1-866-255-7655
  - If your immigration documents have been lost or stolen, contact Citizenship and Immigration Canada at 1-888-242-2100 TTY: 1-888-576-8502

- ❑ Report the theft or fraud to the **Canadian Anti-Fraud Center** by going to their website or by calling **1-888-495-8501.**

APPENDIX E

Identity Crime Victim Action Log

Use this form to record the steps you've taken to report the fraudulent use of your identity or accounts.

Credit Bureau	Phone number	Date contacted	Contact Person	Comments
Equifax	1-866-779-6440			
TransUnion	1-866-525-0262 1-877-713-3393 (Que)			

Creditor	Address and Phone number	Date contacted	Contact Person	Comments

Law Enforcement Agency/Dept	Phone number	Date contacted	Contact Person	Report Number	Comments

APPENDIX F

Identity Crime Prevention Advice (detailed version) For Victims and Other Individuals

Staying Alert

Once resolved, most cases of identity theft stay resolved. But occasionally, some victims have recurring problems. To help stay on top of the situation, continue to monitor your credit reports and read your financial account statements promptly and carefully. You may want to review your credit reports once every three months in the first year of the theft, and once a year thereafter. Stay alert for other signs of identity theft, such as:

- ❑ failing to receive bills or other mail. Follow up with creditors if your bills don't arrive on time. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks.
- ❑ receiving credit cards that you didn't apply for.
- ❑ being denied credit, or being offered less favourable credit terms, like a high interest rate, for no apparent reason.
- ❑ getting calls or letters from debt collectors or businesses about merchandise or services you didn't buy.

What Everyone Should Do Now

- ❑ Place passwords on your credit card, bank, and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SIN or your phone number, or a series of consecutive numbers. When opening new accounts, you may find that many businesses still have a line on their applications for your mother's maiden name. Ask if you can use a password or customized question/answer instead.

- ❑ Ensure that documents with personal information are secured in your home, especially if you have housemates, employ outside help, or are having work done in your home.

- ❑ Ask about information security procedures in your workplace or at businesses, doctor's offices or other institutions that collect your personal information. Find out who has access to your personal information and verify that it is handled securely. Ask about the disposal procedures for those records as well. Find out if your information will be shared with anyone else. If so, ask how your information can be kept confidential.

Maintaining Vigilance

- ❑ Don't give out personal information on the phone, through the mail, or on the Internet unless you've initiated the contact or are sure you know who you're dealing with. Identity criminals are clever, and have posed as representatives of banks, Internet service providers (ISPs), and even government agencies to get people to reveal their SIN, mother's maiden name, account numbers, and other identifying information. Before you share any personal information, confirm that you are dealing with a legitimate organization. Check an organization's website by typing its URL in the address line,

rather than cutting and pasting it. Many companies post scam alerts when their name is used improperly. Or call customer service using the number listed on your account statement or in the telephone book. For more information, see ***How Not to Get Hooked by a 'Phishing' Scam,*** a publication from the U.S. Federal Trade Commission.

❑ Treat your mail and trash carefully:

- Deposit your outgoing mail in post office collection boxes or at your local post office, rather than in an unsecured mailbox. Promptly remove mail from your mailbox unless it is locked. If you're planning to be away from home and can't pick up your mail, call Canada Post at 1-866-607-6301 or go online to http://www.canadapost.ca/tools/pg/manual/PGholdmail-e.asp to request a vacation hold.

- To thwart an identity thief who may pick through your trash or recycling bins to capture your personal information, tear or shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you're discarding, and credit offers you get in the mail.

❑ Don't carry your SIN card, birth certificate or other unnecessary identity documents with you; instead, store them in a secure place.

❑ Carry only the identification information and the credit and debit cards that you'll actually need when you go out.

❑ Give your SIN out only when required by law (i.e., for income and tax reporting purposes). Ask to use other types of identifiers instead.

A Special Word About Social Insurance Numbers
Your employer and financial institutions will need your SIN for wage and tax reporting purposes. Other businesses may ask you for your SIN to do a credit check if you are applying for a loan, renting an apartment, or signing up for utilities. Sometimes, however, they simply want your SIN for general record keeping. If you are asked for your SIN, ask:

- Why do you need my SIN?
- How will my SIN be used?
- How do you protect my SIN from being stolen?
- What will happen if I don't give you my SIN?

Getting satisfactory answers to these questions will help you decide whether you want to share your SIN with the business. The decision to share is yours.

NOTE: It is illegal for businesses in Canada to refuse to provide you with a service or benefit simply because you won't provide your SIN to them, unless they have a legitimate need for the SIN (See the federal Personal Information Protection and Electronics Document Act, Schedule 1, Principle 4.3).

❑ Be cautious when responding to promotions. Identity thieves may create phony promotional offers to get you to give them your personal information.

❑ Keep your purse or wallet in a safe place at work; do the same with copies of administrative forms that have your sensitive personal information.

- ❑ When using credit or debit cards, never let them out of your sight. Key in personal identification numbers privately when you use direct purchase terminals, bank machines, or telephones.

- ❑ When ordering new cheques, pick them up from the bank instead of having them mailed to an unsecured home mailbox.

- ❑ Review the cardholder agreement for your debit and credit cards and confirm the level of protection from fraudulent transactions that they offer you. Shop around for a better deal if you are not satisfied with the protection that they offer.

The Doors and Windows Are Locked, But . . .

If you store your SIN, financial records, tax returns, birth date, and bank account numbers on your computer, you are at a higher risk of identity theft. These tips can help you keep your computer - and the personal information it stores – safe:

- ❑ Update your virus protection software regularly (set it to update automatically every week). Install patches for your operating system and other software programs to protect against intrusions and infections that can lead to the compromise of your computer files or passwords. The Windows XP operating system can be set to automatically check for patches and download them to your computer.

- ❑ Never open files sent to you by strangers, or click on hyperlinks or download programs from people you don't know. Be careful about using file-sharing programs. Opening a file could expose your system to a computer virus or a program known as "spyware," which could capture your passwords or any other information as you type it into your keyboard. For more information, see ***File Sharing: Evaluate the Risks*** and ***Spyware,*** publications from the U.S. Federal Trade Commission.

- ❑ Use a firewall program, especially if you use a high-speed Internet connection like cable, DSL or T-1 that leaves your computer connected to the Internet 24 hours a day. The firewall program will allow you to stop uninvited access to your computer. Without it, hackers can take over your computer, access the personal information stored on it, or use it to commit other crimes.

- ❑ Use a secure browser - software that encrypts or scrambles information you send over the Internet -to guard your online transactions. Be sure your browser has the most up-to-date encryption capabilities by using the latest version available from the manufacturer. You also can download some browsers for free over the Internet. When submitting information, look for the "lock" icon on the browser's status bar to be sure your information is secure during transmission.

- ❑ Try not to store financial information on your laptop unless absolutely necessary. If you do, use a strong password a combination of letters (upper and lower case), numbers and symbols. A good way to create a strong password is to think of a memorable phrase and use the first letter of each word as your password, converting some letters into numbers that resemble letters. For example, "I love Felix; he's a good cat," would become 1LFHA6c. Don't use an automatic log-in feature that saves your user name and password, and always log off when you're finished. That way, if your laptop is stolen, it's harder for a thief to access your personal information.

- ❑ Before you dispose of a computer, delete all the personal information it stored. Deleting files using the keyboard or mouse commands or reformatting your hard drive may not be enough because the files may stay on the computer's hard drive, where they may be retrieved easily. Use a "wipe" utility program to overwrite the entire hard drive.

- ❑ Look for website privacy policies. They should answer questions about maintaining accuracy, access, security, and control of personal information collected by the site, how the information will be used, and whether it will be provided to third parties. If you don't see a privacy policy - or if you can't understand it - consider doing business elsewhere.

APPENDIX FF

Identity Crime Prevention Tips (summary version)

- ❑ Minimize the risk. Be careful about sharing personal information or letting it circulate freely. When you are asked to provide personal information, ask how it will be used, why it is needed, who will be sharing it and how it will be safeguarded.

- ❑ Give out no more than the minimum, and carry the least possible with you.

- ❑ Never carry your birth certificate, SIN, or passport with you unless necessary.

- ❑ Be particularly careful about your SIN; it is an important key to your identity, especially in credit reports and computer databases. Provide other identifiers if you have the option.

- ❑ Don't give your credit card number on the telephone, by electronic mail, or to a voice mailbox, unless you know the person with whom you're communicating or you initiated the communication yourself, and you know that the communication channel is secure.

- ❑ Be suspicious of all email messages you were not expecting. Don't open attachments or click on links in electronic messages from people you don't know.

- ❑ Ensure that your computer is protected by virus/security software that is updated weekly.

- ❑ Pay attention to your billing cycle. If credit card or utility bills fail to arrive, contact the companies to ensure that they have not been illicitly redirected.

- ❑ Guard your mail. Promptly remove mail from an unsecured mailbox after delivery. Ensure mail is forwarded or re-routed if you move or change your mailing address.

- ❑ Notify creditors immediately if your identification or credit cards are lost or stolen.

- ❑ Access your credit report from a credit reporting agency once a year to ensure it's accurate and doesn't include debts or activities you haven't authorized or incurred.

- ❑ Ask that your accounts require passwords or customized question/answer challenges before any inquiries or changes can be made. Choose difficult passwords – not your mother's maiden name. Memorise them and store them in a non-obvious location.

- ❑ Key in personal identification numbers privately when you use direct purchase terminals, bank machines, or telephones.

- ❑ Find out if your cardholder agreements offer protection from fraudulent transactions; shop around for a better deal if you are not satisfied with the level of protection offered.

- ❑ Burn or shred personal financial information such as statements, credit card offers, receipts, insurance forms, etc. Insist that businesses you deal with do the same.

APPENDIX G

Resources for Identity Crime Victims in Canada

Canadian Identity Crime Victim Support Centre (expected to be operational by 2012)
Once fully established, this centre will provide identity crime victims across Canada with information, advice and support in recovering their reputations and avoiding repeat victimization. Its website is expected to be operational by fall 2011 and its national call centre by early 2012.

Canadian Anti-Fraud Centre and SeniorBusters
www.antifraudcentre.ca
1 (888) 495-8501
Overseas and Local: 1 (705) 495-8501
In addition to providing information and advice to individual victims through its call centre, the CAFC gathers and reports statistics on reported fraud in Canada, and makes victim evidence available to law enforcement agencies. A joint project of the Ontario Provincial Police, the RCMP and Canada's Competition Bureau, CAFC engages in public education on fraud, and offers a volunteer-driven service to assist Canadian seniors who have become victims of fraud ("SeniorBusters").

General Victim Services in Canada

Victim Services in Canada
http://www.victimsfirst.gc.ca/serv/vsc-svc.html

Online directory pointing victims to services in their area
http://canada.justice.gc.ca/eng/pi/pcvi-cpcv/vsd-rsv/index.html

Provincial/Territorial Victim Services and Laws:
http://canada.justice.gc.ca/eng/pi/pcvi-cpcv/prov.html

Federal Ombudsman for Victims of Crime
http://www.victimsfirst.gc.ca/index.html

Guides for Victims of Crime and other resources:
http://canada.justice.gc.ca/eng/pi/pcvi-cpcv/pub2.html#crim
http://www.publicsafety.gc.ca/prg/cor/nov/voc-gd-06-2010-eng.aspx

Canadian Statement of Basic Principles of Justice for Victims of Crime
http://www.victimsfirst.gc.ca/serv/wvr-qdv.html#sec3

See also Appendix H, Resources for Victims of Identity Crime in the USA

APPENDIX H

Resources for Identity Crime Victims in the USA

Federal Trade Commission (FTC)

The FTC is the federal agency for identity theft complaints. The FTC website provides identity crime victims with full information on their rights and remedies under US law as well as complaint forms, an affidavit form, a sample letter to send to reporting companies, and other useful information.
1-877-IDTHEFT (438-4338)
http://www.ftc.gov/bcp/menus/consumer/data/idt.shtm

Department of Justice Office for Victims of Crime

This site provides links to a services for victims of identity crime.
http://www.ojp.usdoj.gov/ovc/help/it.htm

Identity Theft Resource Center

This California-based nonprofit group provides information and support for individual victims of identity crime.
(858) 693-7935 or 1 (888) 400-5530 (US-only)
http://www.idtheftcenter.org

Privacy Rights Clearinghouse

Another California-based nonprofit organization with information for victims of identity crime.
http://www.privacyrights.org/Identity-Theft-Data-Breaches

National Crime Victim Law Institute (NCVLI)

In addition to offering training and education, engaging in public policy advocacy, and intervening in legal cases, this university-based service links victims with legal clinics and attorneys in the U.S. who can provide them with free legal representation.
http://www.lclark.edu/law/centers/national_crime_victim_law_institute/

U.S. Credit Reporting Bureaus

TransUnion
1-800-680-7289
www.transunion.com
Equifax
1-800-525-6285
www.equifax.com
Experian
1-888-EXPERIAN (397-3742)
www.experian.com

APPENDIX I

LEGAL RIGHTS AND REMEDIES FOR IDENTITY THEFT/FRAUD VICTIMS IN CANADA

Issue	Legal Rights/ Remedies	Existing Canadian Law	Proposed Canadian Law[1]	U.S. Legislation[2]
1. Detection & Mitigation				
Delayed detection and/or notification by third parties	Responsibility of organizations to detect and report suspected fraud	PIPEDA – Principle 4.7 (Security Safeguards) + similar provision in provincial data protection laws (public and private sector) Credit reporting legislation[3] – duty of accuracy; best evidence rule; duty to corroborate unfavourable information Common law: e.g., negligence, breach of confidence, breach of contract,	OPC recommendation for security provision in federal *Privacy Act*	Common law duties of care Statutory rights of action in some states (see below) *Fair Credit Reporting Act* ("FCRA"), s.607(a), (b)

[1] This includes proposals made by government and government agencies.
[2] For a complete listing of relevant U.S. federal statutory provisions, see Appendix E of the FTC's Guide for Assisting Identity Theft Victims, online at http://www.idtheft.gov/probono/index.html
[3] All provinces except New Brunswick (and the three territories) have legislation governing credit bureaus (see note 7). This legislation varies by province, but there are significant similarities. Most include requirements that reasonable procedures be in place to ensure accuracy and completeness of information in a consumer's file (all but Man and NL), that the information be based on the best evidence available, and/or that unfavourable information be not be included unless reasonable efforts have been made to corroborate the information (all but Que).

Issue	Legal Rights/ Remedies	Existing Canadian Law	Proposed Canadian Law[1]	U.S. Legislation[2]
	Duty of organizations to notify affected individuals of data security breach	Alberta *Personal Information Protection Act*, s.37.1 Ontario *PHIPA*, ss.12(2), 16(2) NL *Health Info Act*, ss.15, 20(3)	Bill C-29	45 State laws[4]
	Duty of creditors to notify consumer of adverse decision based on credit report			FCRA, s.615(a)
Stopping further fraud	Fraud Alerts on Credit Reports + duty of creditors to take extra precautions to authenticate where fraud alert appears	Ontario *Consumer Reporting Act*, ss.12.1ff: right to fraud alert (no time limit) + duty of user to take care Manitoba *Personal Investigations Act*,, s.12.1 Voluntarily offered by both credit bureaus elsewhere in Canada[5]	Consumers Measures Committee (?)	FCRA, s.605A: right to free initial 90 day fraud alert upon request, + to 7 yr alert upon proof of victimization ("IDTheft Report"), + to one-call service for all credit bureaus; duty of creditors to confirm transaction with consumer or take extra steps to authenticate where fraud alert appears [6]
	Credit Freezes	none	none	48 state laws + voluntarily offered in rest of US[7]

[4] See http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm
[5] See http://www.transunion.ca/ca/personal/fraudidentitytheft/aboutfvad_en.page and www.equifax.com (select "Canada")
[6] 15 USC §§ 1681-1681x. You can obtain an extended credit alert, which lasts for seven years, if you provide evidence to a credit bureau that you have been a victim of identity theft. If you decide you want to remove a fraud alert before the expiration date, request removal in writing and provide information to the credit reporting company to verify your identity.
[7] See http://www.consumersunion.org/campaigns/learn_more/003484indiv.html

Issue	Legal Rights/ Remedies	Existing Canadian Law	Proposed Canadian Law[1]	U.S. Legislation[2]
	Free Access to Credit File	Credit reporting legislation:[8] most provinces give consumers the right to free copy of report once per year[9] Credit bureaus offer one free report by mail per year; charge for online access or electronic copy	none	FCRA, s.612(a): right to free copy of credit report annually FCRA, s.612(c),(d): IDT victims have additional right to a free copy of report when they initially place a fraud alert, and during 12 mos after an extended alert has been placed
	Credit Monitoring Services	Offered for a fee by credit bureaus and other private agencies	none	Offered for a fee by credit bureaus and other private agencies
	Duty of credit bureaus to block reporting of information where consumer provides evidence of fraud	PIPEDA Principle 4.7	none	FCRA, s.605B(a)
	Duty of credit bureaus to notify furnishers of allegedly fraudulent information, once notified by victim	PIPEDA Principle 4.7		FCRA, s.605B(b)
	Duty of creditors to cease providing information from fraudulent transactions to credit bureaus	PIPEDA Principle 4.7		FCRA, s.623(a)

[8] B.C. *Business Practices and Consumer Protection Act*, Part 6: Credit Reporting; Alberta *Fair Trading Act*, Part 5: Credit and Personal Reporting; Saskatchewan *Credit Reporting Act;* Manitoba *Personal Investigations Act;* Ontario *Consumer Reporting Act;* Quebec *Act respecting the Protection of Personal Information in the Private Sector;* Nova Scotia *Consumer Reporting Act*, PEI *Consumer Reporting Act;* NL *Consumer Protection and Business Practices Act*, Part VI.

[9] Except in BC where there is no provision with respect to access, credit reporting laws in all other provinces specify that a consumer has the right to access their credit report. Some provinces state that the report shall be provided free of charge (SK, ON, NS, NL and PEI). A report requested in Alberta must be provided free of charge once a year, "reasonable fees"' may be charged for additional reports. In Manitoba, credit bureaus may charge $5 per report.

Issue	Legal Rights/ Remedies	Existing Canadian Law	Proposed Canadian Law[1]	U.S. Legislation[2]
	Duty of organizations to take precautionary measures where evidence of fraud	PIPEDA Principle 4.7 Ontario *Consumer Reporting Act*, s.12.3; Manitoba *Personal Investigations Amendment Act*, see above under "Fraud Alerts"		FCRA – various specific duties as set out above/ below, e.g., s.605A
2. Awareness				
Being made aware of one's rights + remedies	Duty of organizations to inform victims of rights & remedies	none identified	none	FCRA s.609(d) – credit bureaus must provide victims with FTC-approved "Statement of Rights"
	Duty of government to create central information, assistance, and complaint-referral service for victims of ID crime	none	none	*Identity Theft Assumption and Deterrence Act of 1998* ("IDTADA"), s.5 - FTC so tasked by law[10]
3. Liability for Fraudulently Incurred Debts				

[10] Public Law 105-318, 105th Congress; 112 Stat.3007

Issue	Legal Rights/ Remedies	Existing Canadian Law	Proposed Canadian Law[1]	U.S. Legislation[2]
	Limits on consumer liability for fraud where due diligence exercised	Credit cards – voluntary zero liability policies (VISA, Mastercard) Debit cards – Code of conduct limits liability,[11] but practices vary.[12] E-banking – no statutory protection	E-banking – proposals to expand Debit Card Code to cover E-banking.[13]	*Fair Credit Billing Act* – zero liability for credit card-not-present fraud, $50 max liability where card lost.[14] *Electronic Fund Transfers Act* (2009) – mandates disclosures and limits consumer liability for electronic funds transfers, depending on how quickly the loss is reported.[15] Most state laws limit consumer liability for fraudulently created new accounts5[16]
	Protection of land titles in cases of real estate/ mortgage fraud	Ontario *Consumer Protection and Service Modernization Act, 2006* Alberta *Land Titles Act*		
4. Compounded Victimization				

[11] *Canadian Code of Practice for Consumer Debit Card Services*
[12] See http://www.ic.gc.ca/eic/site/oca-bc.nsf/vwapj/EKOS_eng.pdf/$FILE/EKOS_eng.pdf
[13] See http://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca01750.html
[14] 15 USC 1693(g)
[15] 15 USC 1693ff
[16] See http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/rights.html under "Limiting Your Loss From Identity Theft".

Issue	Legal Rights/ Remedies	Existing Canadian Law	Proposed Canadian Law[1]	U.S. Legislation[2]
Harassment by debt collectors	Proscribed debt collection practices	Provincial debt collection/ consumer protection laws[17]	CMC- harmonization of debt collection practices (2003)	*Fair Debt Collection Practices Act*, s.805(c), 809(b)
	Duty of debt collectors to notify creditor of alleged fraud once made aware	none		FCRA, s.615(g)(1)
	Duty of creditors not to send account to collection where notified that it resulted from identity fraud	none		FCRA, s.615(f)
Credit reporting based on inaccurate or incomplete information	Duty of credit bureaus: a) to ensure accurate information	Provincial consumer reporting laws (all but MN and NL) PIPEDA Principle 4.6 BC, AB PIPA; QC Act		FCRA, s.607(b)
	b) to corroborate unfavourable information	Provincial consumer reporting laws (all but QC) PIPEDA Principle 4.7		FCRA, s.611
	c) to include consumer explanation/dispute/ protest in report	Provincial consumer reporting laws (all but QC)		FCRA, s.611

[17] Some provincial debt collection legislation prohibits collection agencies from continuing to attempt collection where the consumer claims that they are not the debtor and/or states that they would prefer for the matter to be taken to court. See B.C. *Business Practices and Consumer Protection Act*, ss.116(4); Alberta *Trade Practices Act, Collection and Debt Repayment Practices Regulation,s.12(1)(k);* Manitoba *Consumer Protection Act*, s.98; Ontario *Collection Agencies Act*, Regulation 103/06, s.22; New Brunswick, *Collection Agencies Act*, s.14(1)(l); Quebec *Act respecting the collection of certain debts*, s.3(2.1); N.W.T. *Consumer Protection Act, Debt Collection Practice Regulations*, ss.11, 13. Note: under Ontario and NB legislation, the debtor must provide notice to the collection agency by registered mail in order for this provision to have effect.

Issue	Legal Rights/ Remedies	Existing Canadian Law	Proposed Canadian Law[1]	U.S. Legislation[2]
	d) to notify those to whom report given[18] of the dispute + resolution	Provincial consumer reporting laws (AB, SK, MN, ON, NS, PEI, NL)		FCRA, s.611
	e) to notify credit-granting customers of alleged fraudulent transactions			FCRA s.605B(b); s.611
	f) to stop reporting of alleged fraudulent accounts	PIPEDA Principle 4.7		FCRA, s.605B(a)
Inability to prove that one is a victim, not a fraudster	See below, under "Restoration"			
Exploitation by commercial ID Theft services industry	Regulation of private ID Theft services industry	none	none	none - but FTC provides Fact Sheet[19]
5. Restoration of Reputation				
Proving that one is a victim, not a fraudster	Getting a report from police re: alleged theft/ fraud	none	none	

[18] within a specified period of time: 60 days (NS, ON, MN, PEI), 6 months (AB, SK), or one year (NL). BC and QC have no such provision.
[19] See http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt05.shtm

Issue	Legal Rights/ Remedies	Existing Canadian Law	Proposed Canadian Law[1]	U.S. Legislation[2]
	Right to information from businesses re: alleged fraudulent transactions	PIPEDA Principle 4.9 + ss.8-10	none	FCRA, s.609(e)
	Right to have such information provided directly to police or other government authority	None	none	FCRA, s.609(e)(1)B, C
	Right to information from debt collectors re: alleged debt	PIPEDA Principle 4.9 + ss.8-10	none	FCRA, s. 615(g)(2)
	Right to info from credit bureaus on sources of information	All provincial credit reporting laws		
	Process for being certified as an identity theft victim	none	none	"Identity Fraud Passport" programs in numerous states;[20] victims have right to apply for "passport" certifying their status
	Right to information from health care providers re: disclosures of personal health information			*Health Insurance Portability and Accountability Act*, - Privacy Rules:[21] one free accounting per year upon request
Restoring foundation documents				

[20] See http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/state-crim-passport.html
[21] 45 C.F.R. para.164.528

Issue	Legal Rights/ Remedies	Existing Canadian Law	Proposed Canadian Law[1]	U.S. Legislation[2]
Restoring credit files and ratings	Duty of credit bureaus to correct records + to notify those to whom they disclosed of the correction/ notation	Provincial credit reporting laws (all but BC and QC) PIPEDA Principle 4.6 – Accuracy; Principle 4.9.5 – must notify customers of correction "where appropriate" BC PIPA – must provide corrected info to recipients within past year AB PIPA – must provide corrected info to past recipients "to extent reasonable to do so"		FCRA, s.611
	Duty of creditors to expunge fraudulent accounts	PIPEDA Principle 4.6 - Accuracy		FCRA s.611(a)(5), s.623(b)
Restoring criminal records	Process for establishing criminal innocence	none	None	Several states have laws requiring expungement and correction of inaccurate information from the records of identity theft victims.[22]
6. Compensation				
Recovering losses as a result of fraud	See above, under "Liability for fraudulently incurred debts"			

[22] See http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/state-crim-expunge.html

Issue	Legal Rights/ Remedies	Existing Canadian Law	Proposed Canadian Law[1]	U.S. Legislation[2]
	Criminal Injuries Compensation programs	Provincial legislation + funds – but only applies to victims of violent crime. E.g., B.C. *Crime Victim Assistance Act*		
	Specific Victim Compensation Funds	Ontario Land Titles Assurance Fund (victims of real estate fraud)		
Recovering the costs of restoration (+ losses)	Common law rights of action for damages	against perpetrators: fraud, misrepresentation, nuisance, trespass, defamation, intentional infliction of mental distress, against facilitators: negligence, breach of contract, breach of confidence * but Cdn courts reluctant to award damages for "pure economic loss"		Some successful actions in U.S. against facilitators[23]

[23] Dion and Ferguson, "Civil Liability for Identity Theft" (Feb.1, 2007), online at http://goliath.ecnext.com/coms2/gi_0199-6285492/Civil-liability-for-identity-theft.html

Issue	Legal Rights/ Remedies	Existing Canadian Law	Proposed Canadian Law[1]	U.S. Legislation[2]
	Statutory rights of action for damages	PIPEDA ss.14, 16 – for breach resulting in damages BC PIPA s.57 AB PIPA s.60 BC *Business Practices and Consumer Protection Act*, s.171 - right of action for damages; s.192 – compensation where conviction Alta *Fair Trading Act*, s.50	*Anti-Spam/Online Protection Act,* S.C.2010, c.23: ss.47ff: for spam/spyware; s.51: actual or statutory damages; ss.52, 53: vicarious liability; directors and officers liability	Calif, Conn, Iowa, Louis, NJ, Penn have statutory rights of action for ID theft/fraud, some permitting treble damages + attorney fees.[24] FCRA, ss.616 (wilful non-compliance), 617 (negligent non-compliance)
	Restitution in criminal/ quasi-criminal sentencing	Crim Code s.738(1) – for direct financial losses and expenses attributable to restoration of identity (unclear if victim could claim for time spent) BPCPA s.192 - compensation for pecuniary losses up to Small Claims Ct. max Alta FTA, s.159(2)(b) – redress; (d) rescission of transaction; (e) restitution of property or funds;		*Identity Theft Enforcement and Restitution Act* – restitution for costs of restoration including attorney fees, + the value of time reasonably spent by victim in attempt to remediate.[25]
7. Justice				

[24] Ibid.
[25] 18 USC 3663(b)(6) and 3663A(c)(1)(A).

Issue	Legal Rights/ Remedies	Existing Canadian Law	Proposed Canadian Law[1]	U.S. Legislation[2]
Seeing perpetrators brought to justice	Criminal offences + penalties	Crim Code ss.402.1, 403: up to 5 or 10 years imprisonment depending on offence		*IDTADA* – up to 25 yrs, depending on nature of ID crime;[26] special considerations in sentencing[27] *Identity Theft Penalty Enhancement Act* (2004) – mandatory 2 yr min. sentence for "Aggravated IDTheft", in addition to regular sentence; see 18 USC 1028A
	Non-criminal offences	Provincial consumer protection laws and credit reporting laws, eg: BC BPCPA s.164ff, s.189 Alta FTA, s.161 Ont CRA, s.23 NS CRA, s.3 PIPEDA, s.28: obstructing an investigation or audit BC PIPA AB PIPA	*Anti-Spam/Online Protection Act*, S.C.2010, c.23 - s.20: administrative monetary penalties; s.41: injunctions; ss.42-46: offences (for spam/phishing, spyware)	FCRA, s.621
	Criminal law enforcement + sentencing	challenging		U.S. Sentencing Commission – Sentencing Guidelines for ID Theft[28]
	Consumer protection law enforcement	minimal		

[26] 18 USC 1029
[27] 28 USC 994(p)
[28] See President's Identity Theft Task Force, *Combating Identity Theft*, vol.II: Supplemental Information, p.47, online at http://www.idtheft.gov/reports/VolumeII.pdf

APPENDIX J

References

Canadian Statistics

Canadian Anti-Fraud Centre, annual, quarterly and monthly statistical reports, www.antifraudcentre.ca

Susan Sproule and Norm Archer, *Measuring Identity Theft in Canada: 2008 Consumer Survey* – MeRC Working Paper #23, http://www.merc-mcmaster.ca/working-papers/23.html

Susan Sproule and Norm Archer, *Measuring Identity Theft in Canada: 2006 Consumer Survey* – MeRC Working Paper #21, http://www.merc-mcmaster.ca/working-papers/21.html

Canadian Reports and Guides

Canada-US Cross-Border Crime Forum, Mass-Marketing Fraud Subgroup, I*dentity-Related Crime: A Threat Assessment - A Report to the Attorney General of the United States and the Minister of Public Safety of Canada* (November 2010) http://www.publicsafety.gc.ca/prg/le/oc/ircta-cciem-eng.aspx

Bi-National Working Group on Cross-Border Mass Marketing Fraud, *Report on Identity Theft: A Report To The Minister of Public Safety Canada And The Attorney General of The United States* (October 2004), http://www.publicsafety.gc.ca/prg/le/bs/report-eng.aspx

Criminal Intelligence Service Canada, *Report on Organized Crime 2008,* "Feature Focus: Identity Theft and Identity Fraud in Canada", and *Report on Organized Crime 2010,* http://www.cisc.gc.ca

Canadian Internet Policy and Public Interest Clinic, Identity Theft Working Paper Series and other resources on Identity Theft, 2006-2008, www.cippic.ca.

K. Jessica Van Vliet and Janice M. Dicks, University of Alberta, *Stolen Identities: A Qualitative Study on the Psychological Impact of Identity Theft,* unpublished draft paper, 2010.

James K. Hill, *Working with Victims of Crime: A Manual Applying Research to Clinical Practice, second edition* http://canada.justice.gc.ca/eng/pi/pcvi-cpcv/pub/res-rech/toc-tdm.html

United States Statistics

Federal Trade Commission, *Consumer Sentinel Network Data Book,* February 2010. http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf

United States Department of Justice, Bureau of Justice Statistics, V*ictims of Identity Crime, 2008, National Crime Victimization Supplement* (December 2010). http://bjs.ojp.usdoj.gov/content/pub/pdf/vit08.pdf

Information Security Media Group, *The Faces of Fraud - Fighting Back; 2010 Survey Results*, December 2010. http://www.bankinfosecurity.com/surveys.php?surveyID=9

Javelin Strategy and Research, *2011 Identity Fraud Survey Report: Consumer Version*, February 2011, https://www.javelinstrategy.com/research/Brochure-208 (see 2010 and earlier reports as well).

United States Reports and Guides

Federal Trade Commission, *Guidebook for Assisting Identity Theft Victims*, http://www.idtheft.gov/probono/docs/i.%20Table%20of%20Contents.pdf

Federal Trade Commission, various resources, reports and guides on identity crime, http://www.ftc.gov/bcp/edu/microsites/idtheft/

United States Department of Justice, Office of Community Oriented Policing Services, A *National Strategy to Combat Identity Theft* (June 2006)
http://www.cops.usdoj.gov/files/RIC/Publications/e03062303.pdf

United States Department of Justice, Office of Community Oriented Policing Services, Problem-Oriented Guides for Police: Problem-Specific Guides Series No.21: *Cheque and Card Fraud* (undated), and No. 25: *Identity Theft* (June 2004), both by Graeme R. Newman.
http://cops.usdoj.gov/RIC/ResourceDetail.aspx?RID=26
http://cops.usdoj.gov/RIC/ResourceDetail.aspx?RID=111

United States Department of Justice, Office for Victims of Crime and International Association of Chiefs of Police, *Enhancing Law Enforcement Response to Victims* (4 vols: 1. *A 21st Century Strategy*, 2. *Implementation Guide*, 3. R*esource Toolkit*, 4. *Training Supplemental)*, 2009.
http://www.responsetovictims.org/

International Association of Chiefs of Police, downloadable resources for Law Enforcement Agencies re: identity crime: http://www.theiacp.org/idsafety

- *Online ID Crime Toolkit for Investigators*
- *Model Policy – Identity Crime*, May 2008
- *Prevention Toolkit*
- *Recovery Toolkit*
- *Training Keys #616 and 617: Identity Crime Update: Parts I and II*, 2008.

Identity Theft Resource Centre, Fact Sheets No.112: *Enhancing Identity Theft Victim and Investigator Communications*, and No.301: *Enhancing Law Enforcement and Identity Theft Victim Communications*, both datecAug.21, 2009. http://www.idtheftcenter.org/law_enforcement.shtml (click on "Law Enforcement Victim Communications" or "Document Catalogue".

President's Identity Theft Task Force, Strategic Plan (2007) and Progress Report (2008), http://www.idtheft.gov

International Reports

United Nations Office on Drugs and Crime, Study on "Fraud and the criminal misuse and falsification of identity", April 2007; see Report to the Secretary General, Document E/CN.15/2007/8 and Appendices, available online at http://www.unodc.org/unodc/en/organized-crime/index.html?ref=menuside

United Nations Office on Drugs and Crime, *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* (2010), chapter 10: Cybercrime. http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf

Philippa Lawson, *Identity-Related Crime Victim Issues: A Discussion Paper,* International Centre for Criminal Law Reform and Criminal Justice Policy, February 2009. http://www.icclr.law.ubc.ca/files/2010/Identity-Related%20Crime%20Victim%20Issues.pdf