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

POLICY APPROACHES TO IDENTITY THEFT

May, 2007

CIPPIC Working Paper No. 6 (ID Theft Series)

www.cippic.ca

CIPPIC Identity Theft Working Paper Series

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

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

Suggested Citation:

CIPPIC (2007), "Policy Approaches to Identity Theft", CIPPIC Working Paper No.6 (ID Theft Series), May 2007, Ottawa: Canadian Internet Policy and Public Interest Clinic.

Working Paper Series:

No.1: Identity Theft: Introduction and Background
No.2: Techniques of Identity Theft
No.3: Legislative Approaches to Identity Theft
No.4: Caselaw on Identity Theft
No.5: Enforcement of Identity Theft Laws
No.6: Policy Approaches to Identity Theft
No.7: Identity Theft: Bibliography

CIPPIC

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

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

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This paper reviews government and corporate sector initiatives that help to prevent, detect, and mitigate the effects of identity theft. Examples of collaboration and cooperation between various levels of government, between the public and private sectors, and within the international community are canvassed as well. The role of nongovernmental organizations in shaping the policy agenda for identity theft is also discussed, as these organizations play an important part in policy development, through their advocacy, research, and education activities. Law enforcement efforts are not addressed here as they are covered in the Working Paper “Enforcement of Identity Theft Laws”.

NOTE REGARDING TERMINOLOGY

The term "identity theft", as used in this Working Paper series, refers broadly to the combination of unauthorized collection and fraudulent use of someone else's personal information. It thus encompasses a number of activities, including collection of personal information (which may or may not be undertaken in an illegal manner), creation of false identity documents, and fraudulent use of the personal information.

Many commentators have pointed out that the term "identity theft" is commonly used to mean "identity fraud", and that the concepts of "theft" and "fraud" should be separated. While this suggestion has merit, we are using the term "identity theft" more broadly, in keeping with the norm that has developed in the literature on this subject. The issue of terminology is discussed further in the first paper in this series.

1. INTRODUCTION

Policies are a driving force behind identity theft prevention, detection, and mitigation initiatives. While good laws are crucial, they are only part of the solution. Their effectiveness is directly related to the way they are interpreted and the vigour with which they are applied and enforced. Appropriate policies, supported by adequate resources and sound management, and translated into effective programs and initiatives, give life to statutory objectives and requirements.

This Working Paper contains a select inventory of government and corporate policies relating to identity theft. Although the focus is on Canada, the section on "players" also identifies relevant U.S. and international organizations. This inclusion was necessary as Canadian governments, businesses, and nongovernmental organizations have established linkages with neighbouring countries. Similarly, international groups often influence the policy initiatives in Canada.

By addressing policy initiatives, this Paper highlights the contributions of both the public and private sectors in combating identity theft. Organizations are frequently criticized for policies and practices that can leave individuals vulnerable to the risk of identity theft. This criticism may be justified. That being said, there are also many examples of constructive policies that serve to prevent, detect, and mitigate identity theft.

This Paper also discusses nongovernmental organizations that are concerned about identity theft. These include consumer groups, advocacy groups, privacy and security organizations, technology associations, think-tanks, academic institutions, law firms, universities, and other organizations that are neither governmental nor business. While some might argue that they are not part of the policy agenda, they are in fact quite relevant to this discourse. This is because they can and do influence government and corporate sector policies. As well, their activities, which include public education, victim assistance, and technical and policy research, support and reinforce those of governments and businesses. There are many examples of collaboration and cooperation between government, business, and nongovernmental organizations.

This Paper takes a non-restrictive approach to defining policies. The distinction between policies, policy initiatives, programss and practices is not always clear. While the focus of this Paper is on true policies, relevant programs and practices are noted where they assist the analysis. Mechanisms for coordination, cooperation, and collaboration that flow from such policies are also mentioned, as are business codes relating to data security.

The Paper begins with an overview of the key Canadian organizations that play a role in combating identity theft. Mention is also made of U.S. and international organizations, to the extent that these form part of global networks relevant to Canadian organizations. Next, Canadian government and corporate policies relating to identity theft are reviewed, along with related activities and mechanisms for coordination and collaboration. Law enforcement and data security breach notification policies are not addressed here, as they are the subject of separate Papers in this series.

2. THE PLAYERS

Identity theft concerns many organizations here in Canada as well as those situated in other countries. By way of illustration, the links webpage of the Reporting Economic Crime On-Line initiative (RECOL) lists 45 organizations, of which 26 are Canadian.[1] The Consumers Measures Committee (CMC) consultation mentioned below extended to over 60 groups and organizations. Thirty Canadian business organizations participated in developing CMC's identity kit for businesses.[2]

Governments and businesses are the primary players in the policymaking process for identity theft. Each has strived in its own way to address the problem by formulating policies and by establishing mechanisms for information exchange, collaboration, and cooperation. Their efforts are reinforced by, and to some degree are influenced by, the numerous activities of the nongovernmental sector.

In recent years, governments have responded to the evolution of identity theft as a serious crime and as a source of public concern by developing a variety of identity theft policies. Some of these policies are new; others have evolved from existing privacy and security initiatives and consumer protection policies. These policies relate to identity document security, consumer education, victim assistance, authentication practices, information collection, law enforcement, and other matters relevant to identity theft. These have, in turn, led to programs, legislative initiatives, and new institutional arrangements.

At the corporate level, banks, credit bureaus, retailers, and other financial institutions collect and hold great deal of personal information about individuals in the course of doing business. These institutions are targets for identity thieves, who commit economic fraud using a variety of techniques. These include using forged and stolen credit, debit and phone cards, committing mortgage fraud, and opening new accounts using a false identity. Financial institutions deal directly with individuals and their policies can be instrumental to protect individuals and to help mitigate the effects of identity theft.

Many international and domestic nongovernmental organizations have taken an interest in identity theft. These organizations, through research and lobbying, and by undertaking studies and public awareness initiatives, play an important if sometimes unacknowledged role in shaping the policymaking process. In some cases, existing organizations have expanded their mandate to respond to the rise of identity theft as a public concern. New organizations that focus on an identity theft have also been established.

[1] Reporting Economic Crime On-Line, Canadian and International Links, online: <https://www.recol.ca/linkspage.aspx>.
[2] Consumer Measures Committee, Identity Kit for Business, online: <http://cmcweb.ca>.

2.1. Canada

2.1.1. Federal and Provincial Governments

2.1.1.1. Federal

Several federal departments and agencies have responsibilities relating to identity theft. These departments include central agencies such as the Treasury Board Secretariat and the Privy Council Office, other government departments, the Royal Canadian Mounted Police (RCMP), and Crown corporations such as Canada Post. They are involved with a number of interdepartmental, federal/provincial/territorial, binational, and international organizations and initiatives relating to identity theft, which are discussed later in this Paper.

The Treasury Board and the Privy Council Office have broad responsibilities, which include government-wide policymaking, resource allocation, and security. These responsibilities encompass identity theft. The Treasury Board recently became chair of an important interdepartmental initiative aimed at ensuring a consistent approach to identity management throughout the federal government.

Industry Canada has important roles relating to identity theft. Its E-Commerce Branch is the lead federal agency in the growing area of electronic commerce, which encompasses internet privacy and issues related to authentication. The Branch chairs a public/private sector working groups to develop principles for electronic authentication. Its officials also represent Canada in international organizations concerned with identity theft, such as the Organization for Economic Cooperation and Development (OECD) and the Asia-Pacific Economic Cooperation forum (APEC).

The Office of Consumer Affairs within Industry Canada acts as a federal focal point for consumer protection and awareness issues, of which identity theft is but one. This office also co-chairs the Consumer Measures Committee (CMC), a federal/provincial/territorial body created under Chapter 8 of the Agreement on Internal Trade (AIT). The CMC provides a forum for national cooperation to improve the marketplace for Canadian consumers through harmonization of laws, regulations, and practices, and through actions to improve public awareness. This committee recently turned its attention to identity theft. In July 2005, it released a Discussion Paper seeking stakeholder input on a number of possible policy approaches to identity theft.[3]

The Competition Bureau, which reports to Parliament through the Minister of Industry, has an interest in fraud prevention. It recently joined forces with the RCMP on fraud awareness initiatives and provides tips for consumers on its website.

The RCMP, as the lead federal law enforcement agency, plays a role in the detection and prosecution of identity theft and public education. Its role and that of other law

[3] Consumer Measures Committee, Working Together to Prevent Identity Theft: A Discussion Paper (Ottawa: Industry Canada, 6 July 2005), online: <http://cmcweb.ca>.

enforcement agencies is discussed in the Paper entitled "Enforcement of Identity Theft Laws". The Canadian Border Services Agency also has an important detection and enforcement role. The Department of Public Safety (formerly Solicitor General of Canada) is Canada's lead department for public safety. Its mandate is to develop and implement policies for national security, including crime prevention and law enforcement. Identity theft is a component of their mandate.

As well as researching identity theft offences, the Department of Justice is relevant as it recommends amendments to existing laws and develops new legislation in response to government direction. For example, in 2003, the Criminal Law Policy Section initiated a Consultation on Proposals to Amend the *Criminal Code* on the topic of identity theft.[4]

The Passport Office (a Special Operating Agency that was formerly part of the Department of Foreign Affairs), Human Resources Development Canada, and Citizenship and Immigration all issue foundation documents. Foundation documents are important government-issued identity documents that are of great value to identity thieves. The Canada Revenue Agency also collects and holds sensitive personal and financial information about Canadians. The data security measures taken by these departments are highly relevant to identity theft protection, given identity thieves' interest in accessing personal information held by the governments.

The mail security policies of Canada Post, a Crown corporation, are critical to identity theft prevention. For example, identity thieves commonly attempt to redirect mail by fraudulently completing change of address forms.

The federal Privacy Commissioner and her provincial and territorial counterparts are independent bodies that oversee privacy laws, respond to public complaints, conduct investigations and raise public awareness. Identity theft is an issue of increasing interest to the Commissioners. It has also become a topic for debate in the Standing Committee on Access to Information, Privacy and Ethics' ongoing five-year review of the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[5] The CIPPIC White Paper on approaches to security breach notification was prepared for this purpose.[6] The Standing Committee has recently initiated a study on identity theft.

2.1.1.2. Provincial

Provincially, the relevant ministries or departments are those concerned with consumer and corporate affairs and government services. This study focuses on Ontario and has not looked at territorial government arrangements. Ministries that are responsible for issuing

[4] Department of Justice, Consultation Document on Identity Theft (Ottawa: Department of Justice, October 2004) and Identity Theft: Consultation on Proposals to Amend the *Criminal Code* (Ottawa: Department of Justice, June 2006).

[5] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5 (PIPEDA). The website for the federal Office of the Privacy Commissioner is <http://www.privcom.gc.ca>.

[6] Canadian Internet Policy and Public Interest Clinic (CIPPIC), Approaches to Security Breach Notification: A White Paper (Canadian Internet Policy and Public Interest Clinic: Ottawa, 9 January 2006), online: <http://www.cippic.ca>.

foundation documents, such as driver's licenses and birth certificates, are also important players. So too is the Ministry of Health, responsible for issuing health cards, which are often targeted by identity thieves. While not cast as identity documents *per se*, these cards, like those issued by the federal government, often serve in practice as proof of identity.

In recent years, identity theft has figured to an increasing degree in the activities of provincial police forces. Police forces are one of the first organizations involved following an instance of identity theft. They investigate these crimes, track down identity thieves, and lay charges where appropriate. The Paper on law enforcement refers to specific initiatives by the Ottawa, Winnipeg, and Vancouver forces with respect to training and interjurisdictional cooperation and coordination. The Ontario Provincial Police (OPP) is also interested in identity theft, working in cooperation with the RCMP and other forces and holding annual conferences on the matter. The Canadian Association of Chiefs of Police has also addressed identity theft at its annual conferences.

2.1.2. Corporations

Policies and practices of financial service providers that issue credit cards, debit cards, telephone cards, and digital certificates have a major impact upon fraud prevention, detection, and mitigation. So too do the policies and practices of individual retail vendors, Canadian banks, and internet service providers. Furthermore, all these actors have a strong interest in identity theft prevention and customer awareness. The three national credit bureaus, also known as consumer reporting agencies, Equifax, TransUnion, and Northern Credit Bureau, are significant as a negative credit report is a common outcome of identity theft. These bureaus therefore have considerable control over the financial situation of individuals and play a crucial role in prevention and detection, as well as victim assistance.

National organizations representing the business community have been active in identity theft policy development, advocacy, and education. These include the Canadian Bankers Association, Insurance Bureau of Canada, Canadian Association of Internet Providers (CAIP), Interac Association, and Advanced Card Technology Association of Canada.

Consumer groups such as the Canadian Council of Better Business Bureaus, Consumers Association of Canada, Consumers Council of Canada, and Retail Council of Canada are also active players on the policy front. Identity theft has captured the attention of pollsters such as Ipsos Reid and EKOS. These companies have included identity theft in national consumer surveys, testing awareness and highlighting concerns relating to identity theft, victim experiences, and expectations.[7]

[7] See, for example, Ipsos-Reid, EDS Canada Privacy and Identity Management Survey (31 January 2005), online: <http://www.ipsos-na.com/news/pressrelease.cfm?id=2543>. Surveys are also discussed in the Introduction and backgrounder, the first Paper in this series.

2.1.3. Non-Governmental Organizations

A number of Canadian non-governmental organizations have taken an interest in identity theft polices. This project is but one example of the efforts of the Canadian Internet Policy and Public Interest Clinic (CIPPIC) to influence policy development. The British Columbia Freedom of Information and Privacy Association (BCFIPA) published a report on identity theft legislation and policies in 2005, with a focus on the adequacy of PIPEDA in preventing identity theft.[8] In 2003, the Public Interest Advocacy Centre (PIAC) released a report on identity theft and consumers.[9] Both these reports were written with the aim of informing governments and influencing policies.

Other consumer groups, such as the Canadian Association of Retired Persons (CARP), have started advising their members on how to protect themselves, and in some cases, have made recommendations to governments on improving laws and policies.[10]

Another group working on identity theft policy is the Public Policy Forum, an Ottawa-based national, not-for-profit organization with a mandate to promote better public policy and better public management through dialogue among leaders from the public, private, labour, and voluntary sectors. In 2003, it hosted a roundtable on identity theft at which government, law enforcement, and business sector representatives discussed how to improve collaboration and cooperation.[11]

Universities, academics, and private research groups have also begun to take an interest in identity theft. Some Canadian law firms provide legal information and updates on privacy and identity theft issues as part of their day-to-day outreach services.[12] Lawyers have written on different aspects of the problem, such as data security breach notification.[13] The Canadian Bar Association has prepared position papers on various aspects of identity theft, including criminal law considerations and data breach notification.[14] The Law Society of Upper Canada website contains information on mortgage fraud and other identity theft topics.[15] The research and advocacy of these

[8] British Columbia Freedom of Information and Privacy Association (BCFIPA), PIPEDA and Identity Theft (30 April 2005), online: <http://www.fipa.bc.ca>.

[9] The Public Interest Advocacy Centre (PIAC), Identity Theft: The Need for Better Consumer Protection (November 2003), online: <http://www.piac.ca>.

[10] CARP, for example, made a submission to the 2005 Consumer Measures Committee consultation exercise. See Consumer Measures Committee, *supra* note.4.

[11] Public Policy Forum, Public Policy Forum Roundtable on Identity Theft and Identity Fraud (Ottawa, 26 June 2003), online:< http://www.ppforum.ca>.

[12] See for example the website of Gowlings Lafleur Henderson, online: <http://www.gowlings.com>. In the U.S., some firms have taken a special interest in data security breach notification.

[13] Fraser, Mark Hayes, "Responsibility for Security Breaches: Towards a Workable Standard", Privacy Centre of Excellence *et. al*., *supra* note 4. There is also a considerable volume of articles in various U.S. law journals on identity theft.

[14] Email from Mark Hayes (19 January 2007) and Canadian Bar Association, "CBA Says Deficiencies in PIPEDA must be Addressed in Five-Year Review" (11 December 2006), online: <http://www.cba.org/CBA/News/2006_Releases/2006-12-11_pipeda.aspx>.

[15] The Law Society of Upper Canada, online: <http://www.lsuc.on.ca>.

professional associations and individuals are a useful resource for policymakers and may be reflected in their decisions.

2.2. United States

2.2.1. Federal and State Governments

In contrast to Canada, the U.S. government has delegated responsibility for identity theft reporting and policymaking to one central agency. Under the *Identity Theft and Assumption Deterrence Act of 1998*, the Federal Trade Commission (FTC) develops public education programs, serves as the central reporting point for identity theft, compiles statistics, assists victims, and coordinates enforcement efforts with other agencies.[16] Other important federal players include the Federal Bureau of Investigation (FBI) and the U.S. Postal Service.

In addition to its traditional role in aiding law enforcement, the U.S. Department of Justice is also responsible for developing a national strategy for identity theft law enforcement and for public education. In 2003, the department conducted a survey to determine the preparedness of major police associations. This was followed by national consultations with law enforcement officials, victims, prosecutors, and the business community, which formed the basis for a national strategy to combat identity theft.[17] The Fraud Section of the Criminal Division investigates business crimes, including various forms of economic fraud (e.g. insurance, securities, international crime, internet fraud, mortgage scams). More recently, it has added crimes targeting consumers to its mandate.

State agencies with a particular focus on identity theft include the State and Consumer Services Agency, the Department of Consumer Affairs, and the Office of Privacy Protection. In California, as in many other states, identity theft is a high-profile issue. The California state government has led the way, not only in enacting progressive legislation, but also in its outreach and public education initiatives. Perhaps not surprisingly, it is also home to some of the most active and prominent privacy and identity theft advocacy groups. Since 2005, the Governor has sponsored an annual identity "summit". The summit attracts a wide range of participants from government, law enforcement, and the corporate sector.[18]

2.2.2. Corporations

As in Canada, the American financial sector – banks, credit issuers, credit bureaus, internet service providers, and privacy and security companies – has developed policies aimed at combating identity theft. Umbrella organizations such as the U.S. Better Business Bureau have also engaged in policy development, advocacy,k and education.

---

[16] See <http://www.ftc.gov>.

[17] U.S. Department of Justice, *A National Strategy to Combat Identity Theft* (Department of Justice: Washington, February 2006).

[18] California District Attorneys Association, *Teaming Up Against Identity Theft: Proceedings of the Summit on Solutions, Los Angeles, 2006* (Los Angeles: 23 February 2006) and *Locking Up the Evil Twin: Proceedings of the Summit on Identity Theft Solutions, Sacramento, 2005* (Sacramento: 1 March 2005).

2.2.3. Non-Governmental Organizations

The U.S. is home to a number of very influential advocacy groups. The Identity Theft Resource Center**,** based in California, is a major advocacy group that plays an active role in public awareness and victim assistance. The Privacy Rights Clearinghouse, another national advocacy and public education group based in California, is concerned with a wide variety of issues relating to privacy and consumer rights, including identity theft. Other key groups active in working with government and business to propose policy reforms include the National Consumers' League and the Electronic Privacy Information Centre (EPIC).

2.3. International Organizations

In recent years, international organizations have started to develop policies and related initiatives in the area of identity theft, including governmental, business, and consumer organizations. Canada plays an active role in many of these inter-governmental initiatives.

The Organization for Economic Co-operation and Development (OECD), for example, has established a Working Party on Information Security and Privacy (WPISP),[19] in which Canada participates through Industry Canada and the federal Privacy Commissioner. The WPISP is developing guidelines for electronic authentication and may be considering the issue of data security breach notification. It is also considering revisions to the 2002 OECD Guidelines for the Security of Information Systems and Networks.[20]

The Asia Pacific Economic Cooperation forum (APEC) works to harmonize policy in the area of online privacy and security through the Security and Prosperity Steering Group (SPSG) of its Telecommunications and Information Group.[21] Industry Canada participates on the SPSG, as well as on APEC's Electronic Commerce Steering Group, and was involved in the development of APEC's Privacy Framework.[22]

The United Nations has also been active in studying identity theft policies, laws, and trends, specifically those related to fraud, criminal misuse, and falsification of identity. The U.N. Crime Commission Intergovernmental Expert Group on Fraud and the Criminal Misuse and Falsification of Identity Crime Commission are undertaking a survey of

---

[19] OECD Working Party on Information Security and Privacy (WPISP), online: <http://www.oecd.org/document/46/0,2340,en_2649_34255_36862382_1_1_1_1,00.html>.

[20] OECD, "Guidelines for the Security of Information Systems and Networks" (2002). The OECD has also produced a document entitled "Guidelines on the Protection of Privacy and Transborder Flow of Data" (1980).

[21] Asia Pacific Economic Cooperation (APEC), Security and Prosperity Steering Group (SPSG), online: <http://www.apec.org/apec/ministerial_statements/sectoral_ministerial/telecommunications/2005/annex_e.html.>

[22] Asia Pacific Economic Cooperation (APEC), Press Release on the Privacy Framework, online: <http://www.apec.org/apec/news_media/fact_sheets/apec_privacy_framework.html>.

member state governments, of which Canada is one, with the aim of developing guidelines for prevention, investigation, and prosecution.[23]

In 2005, Canada, the U.S. and Mexico launched the Security and Prosperity Partnership (SSP), which aims to increase economic integration and security cooperation between these three countries. A Framework of Common Principles for Electronic Commerce has been signed, under which work programs for electronic authentication, privacy protection, and consumer protection in the online marketplace have been established.[24]

International nongovernmental organizations concerned with identity theft policies include: the Anti-Phishing Working Group, an industry association focused on eliminating the identity theft and fraud that results from phishing and email spoofing;[25] the Trans Atlantic Consumer Dialogue (TACD),[26] which is developing a Resolution on Identity Theft, Phishing and Consumer Confidence for consideration by the European Commission and the U.S. government; and Liberty Alliance.[27]

3. CANADIAN FEDERAL AND PROVINCIAL GOVERNMENT POLICIES FOR PREVENTING AND COMBATING IDENTITY THEFT

This section of the Paper provides examples of federal and provincial government policies directed at preventing, detecting, and mitigating the effects of identity theft. Many of these policies are concerned with the integrity of government-issued identity documents and the security of the personal information it collects.

3.1. Identity Management Policy Development

The federal government has been undertaking a review of its numerous, diverse and often segmented policies, with the aim of creating one integrated, streamlined, and consolidated policy infrastructure. Known as the "Policy Suite Renewal," and led by the Treasury Board, this process has resulted in efforts to rationalize the policy process and encourage better coordination between departments and programs.[28]

---

[23] U.N. Crime Commission, Intergovernmental Expert Group on Fraud and the Criminal Misuse and Falsification of Identity, U.S. Questionnaire, online: <http://www.usdoj.gov/criminal/fraud/UNOCDCQuestionnaireUSGResponseFinal.pdf>.

[24] Security and Prosperity Partnership of North America, online:< http://www.cbsa-asfc.gc.ca/agency-agence/spp-psp-e.html>.

[25] Anti-Phishing Working Group, online: <http://www.antiphishing.org/>.

[26] Trans Atlantic Consumer Dialogue (TACD), online: <http://www.tacd.org>.

[27] Liberty Alliance is a global consortium of more than 150 companies, nonprofit and government organizations, including technical experts, academics, and private sector organizations such as financial service companies. Its goal is to develop an open standard for federated network identity that supports all current and emerging network devices. In 2005, it formed the Identity Theft Prevention Special Interest Group (SIG). The SIG provides a forum to discuss definitional issues, make recommendations, and document best practices. Liberty Alliance has produced a number of documents on policy, practices, prevention, and legislation and has sponsored multidisciplinary workshops on identity theft. See: Liberty Alliance, online: <http://www.projectliberty.org>.

[28] Canada, Policy Suite Renewal Initiative (October 2004), online: <http://www.tbs-sct.gc.ca/prp-pep/index_e.asp>.

Consistent with this new approach, the federal government is attempting to develop a conceptual framework for identity management across the government. Treasury Board is chairing an interdepartmental committee, which to date has focused on developing Identity Principles to guide departments in their information collection and sharing activities. As proper information management lies at the heart of preventing identity theft, this initiative has potentially significant implications for the way in which the federal government approaches this issue.

3.2. Security of Identity Documents

Governments issue important identity documents to individuals, known in law enforcement as "foundation documents". Federally, these include Social Insurance Numbers (SINs), passports, and permanent resident cards. Provincially, they include driver's licenses, birth and marriage certificates, and health cards.

These documents are widely used to prove identity in ways that go beyond their primary purposes. They are therefore prime targets for identity thieves, who can forge or use stolen documents to commit financial fraud or impersonate the rightful owner to obtain benefits or shield themselves from the law.

Bearing this in mind, governments have introduced policies to strengthen the integrity of key identity documents. In the case of birth certificates and immigration/citizenship documents, the federal government works with provincial governments to improve the accuracy and security of these documents.[29]

3.2.1. Tighter Procedures for Obtaining Driver's Licenses and Birth Certificates

Driver's licenses are generally available with few authentication checks. In 2005, the Ontario government increased penalties for making false statements in driver's license applications to between $400 and $5000.[30] In addition, drivers are legally required to register any change of address with the License Bureau. That being said, a person applying for a driver's license only needs to show one piece of identification as proof of signature.[31]

In 2002, Ontario introduced new rules designed to protect the integrity of birth certificates. Citizens must report lost, stolen or destroyed birth certificates, which will then be deactivated. Information will be shared with other government programs, including the Passport Office. Only one birth certificate will be issued at one time for an individual. Fines for applicants providing false information have increased.[32]

---

[29] Public Policy Forum, *Public Policy Forum Roundtable on Identity Theft and Identity Fraud, Ottawa, 2003* (Ottawa: Public Policy Forum, 26 June 2003) at 22.
[30] Ontario, *Transportation Statute Law Amendment Act, 2005.*
[31] CNW Group, *Province Continues Improvements To Driver's Licence Security*: online <http://www.newswire.ca/en/releases/archive/March2006/17/c3302.html>.
[32] Ontario, *Vital Statistics Statute Law Amendment Act (Security of Documents), 2001.*

3.2.2. More Secure Delivery of Identification Documents

Driver's licenses and Canadian passports are still delivered by regular mail. This makes them prone to theft. As an indication of the severity of the issues surrounding mail theft, the Government of Alberta, in consultation with its partners, is currently reviewing the regular mail delivery method of the new driver's license.[33]

3.2.3. Using "Non-Tamper Proof" Identity Documents

At the federal level, identity cards for immigrants to Canada with permanent resident status now have high-tech security features to hamper forgery.[34] Provincially, the Alberta government has recognized the problems associated with identification documents that can be easily counterfeited. To combat this problem, it has introduced a new driver's license, one which uses a laser-embedded photograph, raised lettering and a gradually diminishing graphic containing the driver's name and birth date.[35]

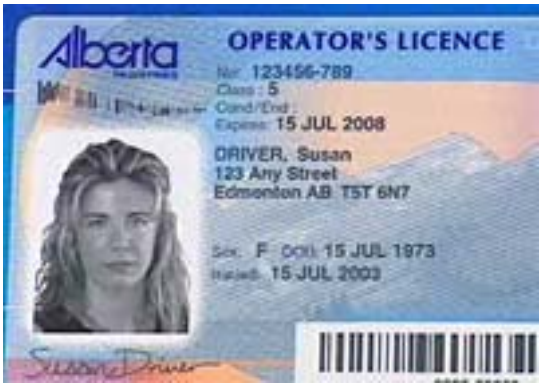

Figure 3.1 - Alberta driver's licence

3.2.4. Tighter Security for Social Insurance Numbers (SINs)

The federal government, in response to recommendations by the Auditor General of Canada, has tightened security for SINs in ways that have the potential to decrease their value to identity thieves. Only original documents are now accepted as proof of identity and citizenship. Any SIN that has not been used for five years is deactivated. Furthermore, SINs for people who are not Canadians or permanent residents expire after a certain period of time.

---

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

[34] Canada Online, Canadian ID Cards and Documents, online: <http://canadaonline.about.com/od/idcards/Canadian_ID_Cards_and_Documents.htm>.

[35] CBC News, *Alberta launches 'most secure' driver's licence*, June 4, 2003: online <http://www.cbc.ca/story/news/national/2003/06/04/Consumers/driverlicence_030604.html>.

3.2.5. Biometric Passports

In response to pressure from the U.S. and as part of an international policy initiative of the International Civil Aviation Organization (ICAO) of the United Nations, the federal government is planning to introduce biometric passports with the goal of improving national security.

Currently, new Canadian passports include security features such as digital photos, holograms, special ink, digital printing, a "ghost" photo, and a machine-readable zone. All of these features have been designed to minimize the ease of forgery and tampering. In 2006, the federal government amended the *Canadian Passport Order* to give the Passport Office the ability to convert any personal information on a passport, including a photograph, into a "digital biometric format".[36] The Canadian Border Services Agency has taken a step in this direction already through its CANPASS initiative. Under CANPASS, some major airports have kiosks that take digital pictures of a person's eye as a means of identification. At this point, registration for CANPASS is purely voluntary.

3.2.6. National Identification Cards

Past federal governments have discussed the concept of national identity cards. The federal Privacy Commissioner, as well as civil liberties advocacy groups, and the Canadian public have expressed serious concerns about introducing such devices. As with biometric passports, the issue is laden with ethical, human rights, and technological issues.

3.2.7. Security of the Postal System

Identity thieves often use the postal system to steal personal information. Methods include stealing mail from homes, mailboxes or delivery boxes, or by completing a fraudulent change of address form in order to redirect mail to another location. Canada Post has long been engaged in preventing identity theft, and has recently improved security measures for change of address requests. It also has an active public education and awareness initiative.

3.3. Collection and Management of Personal Information

3.3.1. Secure Online Service

Since 1999, the federal government has been working on a government wide system to secure online transactions beyond tax return filings, which have had the benefit of a secure system for some time. The "Secure Channel" aims to protect the privacy of online transactions between Canadians and the government. A central registry, built on authentication technology and using secure encryption, will enable individuals to obtain a

[36] Canada, *Order Amending the Canadian Passport Order*, P.C. 2006-529 June 15, 2006 at s.8 (1) and (2), online: <http://www.ppt.gc.ca/publications/order_06-95.aspx?lang=e>.

range of government services through a "single window". The system currently remains in the development phase.[37]

3.3.2. Electronic Personal Health Information

A study of identity theft in the health care sector has noted that electronic health records, which include identifying information about the patient, are consistently a source of risk for identity theft.[38] For example, in some electronic systems, when a pharmacist accesses a patient's record, all of the patient's information is displayed and can be viewed by everyone behind the counter.[39]

The lack of appropriate access controls and privacy safeguards for the use of electronic health records increases the risk of identity theft. In the U.S., the Department of Health and Human Services has created a program to devise solutions to problems surrounding the security and privacy of patient data.[40]

3.3.3. Information Sharing

Different levels of government can provide a faster and more consistent response to problems associated with identity theft by coordinating their efforts through information-sharing initiatives. One such example is Canshare, an internet-based information-sharing system developed by, and for the use of, federal and provincial consumer law enforcement agencies.[41]

3.3.4. Procurement Policies

The federal government is trying to ensure that contractors who handle sensitive information adhere to privacy laws. A good example is the bidding process for the multi-billion dollar Canada student loan program. Bidders on the new 2006 contract had to demonstrate that they could impose tight security measures to prevent students' private financial and personal information from being compromised. This requirement is based in part on a concern that the information might fall into the hands of U.S. security agencies.[42]

---

[37] Ottawa Citizen, "Clumsy online service forced on PS", 23 January 2006 and "Online security program called clumsy", 24 January 2006 at A6.

[38] Gordon Atherley, *Identity Theft in Healthcare A White Paper*, Greyhead Associates, January 2006, online: <http://www.teranet.ca/corporate/publications/Identity_Theft_In_Healthcare.pdf> at p. 10.

[39] *Ibid*.

[40] Government Health IT, *States sign on to HHS privacy program*, 23 May 2006: online <http://www.govhealthit.com/article94617-05-23-06-Web>.

[41] Consumer Measures Committee, *Cooperative Enforcement - Working Group (completed)*, 21 December 2005: online: <http://strategis.ic.gc.ca/epic/internet/incmc-cmc.nsf/en/fe00030e.html>.

[42] Ottawa Citizen, "Student loan bidders must protect data", 13 March 2006 at A3.

3.4. Authentication

The federal government is leading an effort to develop improved principles for authentication. Further to, and in support of its international activities relating to authentication, Industry Canada chairs the Canadian Authentication Principles Working Group, which has members from various levels of government, industry, and consumer groups.[43] In 2004, the Working Group released a set of Principles for Electronic Authentication. These principles are in the process of being reviewed.

3.5. Public Education, Awareness and Assistance

By informing consumers of risks and preventative measures, promoting good privacy practices to businesses, and assisting victims, governments can help reduce the risks and impact of identity theft. There is considerable activity on this front on the part of both levels of government in Canada.

In recent years, the federal government and many of the provinces have implemented policies for informing individual consumers about measures they can take to protect themselves from identity thieves, and steps to take in the event they are victims. Federal departmental websites, including those of the RCMP, Public Safety Canada (formerly Public Safety Emergency Preparedness Canada), the Competition Bureau, and the Privacy Commissioner, provide a wealth of information for individuals seeking to reduce their exposure to identity theft. Provincially, the Ontario Ministry of Government Services regularly updates a website with tips for consumers.[44] The Alberta Government Services Consumer Information Centre maintains a similar website, with a toll-free number to call for advice.[45]

The Working Paper entitled "Enforcement of Identity Theft Laws" refers to Phonebusters, a policy initiative that is a source of information, advice and reporting for identity theft.[46] A joint effort of the RCMP, Competition Bureau, and Ontario Provincial Police, Phonebusters has proven to be a credible focal point for receiving reports of identity theft, informing individuals, and assisting victims. Phonebusters also provides victims with an "Identity Theft Statement" which can be used to report an incident to different organizations.[47]

The federal government also has a policy of alerting citizens to phishing scams. For example, in December 2006, the Department of Finance placed a warning on its website that emails were being sent to some Canadians, claiming to be from the department, promising a tax refund if an appended form is completed. The form asked for personal information such as credit card number and SIN. Recipients were advised to delete the email and contact law enforcement authorities.

---

[43] Industry Canada, *Principles for Electronic Authentication* (Ottawa: 2004).
[44] Email from Randy Hopkins (23 January 2007).
[45] Alberta, Government Services Consumer Information Centre, online: <http://www.governmentservices.gov.ab.ca>.
[46] Phonebusters, online: <http://www.phonebusters.com/>.
[47] Consumer Measures Committee, *The Identity Theft Statement*: *Frequently Asked Questions*, 14 January 2004, online: <http://cmcweb.ca/epic/internet/incmc-cmc.nsf/en/fe00077e.html>.

3.6. Supporting Research on Identity Theft

As well as undertaking independent research, governments have funded the identity theft initiatives of academics and nongovernmental organizations. The results of such research have informed and supported government initiatives. The Ontario government, for example, funds research into electronic commerce issues, including identity theft. The Ontario Research Network for Electronic Commerce (ORNEC) has provided funding for this research project.

The federal Privacy Commissioner has also funded research on identity theft, such as that conducted by the British Columbia Freedom of Information Association.[48] A joint effort of the University of Toronto and the London School of Economics, also funded by the Privacy Commissioner, is examining national identity policies with a view to developing a policy framework for managing multiple identity.[49]

4. STANDARDS AND CODES

4.1. Standards

The establishment of standards for preventing identity theft has been organized at the national level, influenced in large part by movement on the international scene. For example, ISO 17799 is an international security standard that covers different aspects of information system security. Among the topics covered is System Access Control, which includes controlling access to information, preventing unauthorized access to information systems, and detecting unauthorized activities. Another topic covered is physical and environmental security.[50]

In 2004, the Ontario Information and Privacy Commissioner participated in a proposal to establish a Privacy Technology Study Group (PTSG) to examine the need for developing a privacy technology standard. The Ontario Information and Privacy Commissioner also leads a project called PETTEP, which develops testing and evaluation criteria for privacy information technology and information systems. PETTEP acts as an official liaison organization to the ISO PTSG.

At the 26th International Conference on Privacy and Personal Data Protection held on September 14, 2004, it was recommended that ISO develop global privacy standards and specifically, a privacy technology standard. The standard would support the implementation of legal rules on privacy and data protection where they exist and the formulation of such rules where they are still lacking.[51] Examples of other, more specific standards, are outlined below.

---

[48] B.C. Freedom of Information Association, *supra* note .

[49] This initiative is known as the Information Policy Research Program.

[50] The ISO 17799 Information Security Portal, *ISO 17799: What Is It?*, online: <http://www.computersecuritynow.com/what.htm>.

[51] Resolution on a Draft ISO Privacy Framework Standard, 26th International Conference on Privacy and Personal Data Protection, Wroclaw, 14 September 2004, online:

4.1.1. Collection and Management of Personal Information

Although there is much progress still to be made, some promising practices have been adopted by the business community. These include methods for securing highly sensitive data by encrypting it, not just while in transit but also in its place of storage. In addition, businesses are creating fraud detection software and online security programs (such as those of VISA Canada), as well as other new technologies for security. For example, TPM chips assign a unique and permanent identifier to every computer before it leaves the factory. One's identity must be proven every time the computer is used.[52] Laptop computers with built-in encryption are being manufactured and sold.

4.1.2. Limiting the Use of Sensitive Unique Identifiers

The use of certain personally identifiable information, such as driver's licenses and SINs, to identify accounts increases the risk of identity theft. Many companies continue to use these identifiers[53] while other organizations are making a conscious effort to decrease their use of SINs as an identifier.[54]

4.1.3. Authentication

4.1.3.1. Two Factor Authentication

A majority of businesses still use only single factor authentication. This means that users only need one password to access workstations and other computing resources. The use of two factor authentication, such as the use of a secure token combined with a password, improves security and reduces the risk of data being compromised. For example, banks have introduced improved authentication procedures in the form of two or more question identification with passwords for online banking.

4.1.4. Credit Card Security Measures

Credit card issuers have introduced a variety of policies and measures to curb identity theft. VISA and Mastercard each have a zero tolerance liability policy for fraud.

<http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/806742/1056984/36N1231_Resolution_on_a_Draft_ISO_Privacy_Framework_Standard.pdf?nodeid=5023875&vernum=0> at p. 3.

[52] MSNBC, "Let's see some ID, please" (13 December 2005), online: <http://www.msnbc.msn.com/ID/10441443/priont/1/displaymode/1098/>.

[53] Information Technology Association of Canada (ITAC), ITAC comments on CMC Discussion Paper (September 2005), online: <http://www.itac.ca/Library/PolicyandAdvocacy/CyberSecurityandPrivacy/05Sept15IDTheft.pdf> at p. 2.

[54] Business.ca, "Privacy experts call for tougher penalties", 13 April 2006, online: <http://www.itbusiness.ca/it/client/en/home/DetailNewsPrint.asp?id=39048>.

4.1.4.1. Credit Card Security Number

Many businesses that accept credit cards have long had a policy of truncating, or partially blocking out, credit card numbers on electronic receipts. However, credit card security numbers are a fairly new security feature. The security number is a random number printed on the back of the card by the credit card issuer. When the card is used to make a purchase by phone or over the internet, the security number must be entered for the transaction to go through. If someone only skims the card, it cannot be used online or by phone unless he or she can also capture the security number.

4.1.4.2. Account Monitoring

Calling card issuers usually monitor client accounts for suspicious activity. For example, if a client has a calling card and has never used it to call overseas, but it is suddenly being used to make several overseas calls in a short period of time, the account might be suspended until the rightful cardholder contacts the company to verify that he or she is the one making the calls.

Credit card companies also monitor their accounts.[55] For example, if the magnetic strip on the back of a card stops functioning, the owner can still make purchases using the card. The teller will manually enter the card number. If this happens a few times in a short period, it will likely be picked up by the account monitoring. The credit card issuer will then usually contact the cardholder to ensure the transactions are his or hers. Other types of suspicious activities are also monitored.

Monitoring is also used in information systems security. A common security mechanism used to protect networks is intrusion-detection systems (IDS).

4.1.5. Credit Bureau Reports: Prevention and Victim Assistance

Credit bureaus monitor accounts and will place fraud alerts if requested to do so by identity theft victims or law enforcement agencies. Fraud alerts are also known as "security alerts". According to TransUnion,[56] an individual has the right to place a fraud alert on his or her credit report. This informs potential creditors that they may be a victim of identity theft.

The alert may be placed on a file by calling one of the three nationwide consumer reporting agencies. As soon as that agency processes the fraud alert, it will notify the other two credit bureaus, which then must also place fraud alerts on their corresponding file. A fraud alert tells creditors to contact the person before they extend credit, open a

[55] CIBC, *CIBC Dividend Platinum Card*, online: <http://www.cibc.com/ca/visa/dividend-platinum/dividend-plat-ftrs.html>.
[56] TransUnion, *Fraud Alerts*, online: <http://www.transunion.com/content/page.jsp?id=/personalsolutions/general/data/fraudAlert.xml>.

new account, or change existing accounts. While most creditors will call the person concerned, they are not obliged to do so by law, thus it is not fail-proof protection.[57]

A fraud alert differs from a security freeze, a common procedure in other jurisdictions including the U.S. A security freeze requires the credit bureau to contact the individual for whom a credit report is requested and obtain express authorization before releasing the credit report to the requester.[58] A fraud alert only requires the credit bureau to notify the credit grantor that the individual might have been a victim of identity theft. Security freezes are not currently offered to Canadian customers or to identity theft victims.

4.1.6. Notification of Phishing Attempts

Canadian banks generally warn customers about phishing attempts. They usually post information on specific phishing scams and provide general safety tips to their clients.

The following financial institutions have such notices:

- CIBC;[59]
- National Bank of Canada;[60]
- TD Bank Financial Group;[61]
- BMO Bank of Montreal;[62]
- RBC Financial Group;[63]
- Citizens Bank of Canada;[64] and
- VISA.[65]

These alerts help educate clients who use online banking. The general security information provided is also useful in contexts other than online banking: it reduces the risk of identity theft and increases Canadian awareness of these potential risks.

---

[57] Consumer Measures Committee, *Tools: What and How to Tell Customers about a Breach*, online: <http://cmcweb.ca/epic/internet/incmc-cmc.nsf/en/fe00094e.html>.

[58] Consumer Measures Committee, *Working Together to Prevent Identity Theft*, 6 July 2005, online: <http://cmcweb.ca/epic/internet/incmc-cmc.nsf/vwapj/Consultation%20Workbook_IDTheft.pdf/$FILE/Consultation%20Workbook_IDTheft.pdf> at p. 15.

[59] CIBC, *E-mail Fraud Examples*, online: <http://www.cibc.com/ca/legal/fraud-examples.html>.

[60] National Bank of Canada, *E-mail scams*, online: <http://www.bnc.ca/bnc/cda/productfamily/0,1010,divId-2_langId-1_navCode-848,00.html>.

[61] TD Bank Financial Group, *Security Information – Email Safety*, online: <http://www.td.com/security/email.jsp>.

[62] BMO Bank of Montreal, *Phishing*, online: <http://www4.bmo.com/popup/0,4442,35649_2379123,00.html>.

[63] RBC Financial Group, *Security*, online: <http://www.rbc.com/security/bulletinPhishing.html>.

[64] Citizens Bank of Canada, *Phishing Alert*, online: <https://www.citizensbank.ca/Personal/AboutUs/PrivacySecurityStuff/Security/Fraud/PhishingAlert/>.

[65] VISA Canada, *Cut the line on Phishing Scams*, online: <http://www.visa.ca/en/personal/shop_protect_email.cfm>.

4.1.7. Minimum Requirements for Devices

The Interac Association is responsible for establishing and enforcing minimum requirements for ABMs and POS devices, transaction encryption, and due diligence on business partners involved in delivering INTERAC services to Canadians.[66] Their policies and guidelines encourage members to improve their security systems.

4.1.8. Electronic Statements

The use of electronic statements instead of statements delivered by regular mail reduces the incidents of mail theft and "dumpster diving" which are precursors to identity theft. Electronic statements can be delivered more securely than physical mail and are increasingly being used.

4.1.9. Public Awareness and Education

Government is not the only sector that serves to educate the public on identity theft: the corporate sector has also taken steps to educate and inform consumers so that they can reduce their risk of being victimized by identity theft.

Banks and many other financial institutions make a concerted effort to educate their clients about identity theft through monthly newsletters (such as Scotiabank's "*The Vault"*), through pamphlets sent with account statements, and through advice on their websites. Mastercard has its "PYID" program – Protect Your ID – for its clients, which includes tips on preventing identity theft. The Interac Association places newspaper notices pointing out the importance of covering one's PIN when it is being used, and has additional tips on its website.[67]

The Better Business Bureau partnered with the Ottawa police and the Competition Bureau in March 2006 to hold a "document destruction event", at which free shredding was offered.[68]

Industry associations also have programs to educate their members. The Canadian Marketing Association, for example, has issued a fact sheet for its members on steps for combating identity theft. The fact sheet notes that identity theft is "bad for business".[69]

4.1.10. Research

As well as having its own in-house policy research activities relating to identity theft, the corporate sector is involved in organizing and sponsoring the research of others. In November 2006, for example, the universities of Toronto and Waterloo, in partnership

---

[66] Interac Association, *Comments for the 2006 Review of Financial Sector Legislation*, June 2005, online: <http://www.fin.gc.ca/consultresp/06Rev_16e.html>.
[67] Interac Association, Security, online: <http://www.interac.org/en_nl_40_security.html>.
[68] Ottawa Citizen, "Residents come out to shred it and forge it", 26 March 2006.
[69] Canadian Marketing Association, Combatting Identity Theft: Next Steps, online: <http://www.the-cma.org/membership/memberbenefits.cfm>.

with Bell Security Solutions Inc.'s Privacy Centre of Excellence, held their 7th Annual Privacy and Security Workshop, the theme of which was identity theft and identity management.[70]

4.2. Codes

A number of businesses have adopted codes of practice, some of which are relevant to combating identity theft. Business sectors tend to prefer voluntary codes over legislation since they claim that these codes are flexible and efficient.[71]

The codes are often precursors to legislation, as when the federal government adopted the *Personal Information Protection and Electronic Documents Act* in 2000. The thrust of the law was to make adherence to the Model Code for the Protection of Personal Information mandatory for all organizations. This Code sets out ten principles which organizations should follow when dealing with their clients' personally identifiable information. The Code was published in March 2000 and was reaffirmed in 2001.

4.2.1. Canadian Code of Practice for Consumer Debit Card Services

The Canadian Code of Practice for Consumer Debit Card Services is a voluntary code of practice used by a variety of organizations that issue debit cards, accept them in transactions, and process transactions. The Code establishes who is liable for losses and the procedure to be used when unauthorized transactions occur.

4.2.2. Canadian Code of Practice for Consumer Protection in Electronic Commerce

The Canadian Code of Practice for Consumer Protection in Electronic Commerce establishes benchmarks for good business practice for merchants who conduct commercial activities with consumers online. Developed by the federal/provincial/territorial Consumer Measures Committee, the Code leaves unchanged rights, remedies, and other obligations that may exist as a result of consumer protection, privacy, or other laws and regulations, or other general or sector-specific voluntary codes of conduct to which vendors may subscribe.[72]

4.2.3. Internet Sales Contract Harmonization Template

On May 25, 2001, federal, provincial and territorial Ministers responsible for consumer affairs approved a new approach to harmonizing consumer protection legislation in electronic commerce. The new approach helps ensure that consumers benefit from equal protection across the country. A common template endorsed by the Ministers covers

---

[70] Privacy Centre of Excellence (Bell Security Solutions Inc.), the Centre for Innovation Law and Policy (University of Toronto) and the Centre for Applied Cryptographic Research (University of Waterloo), *7th Annual Privacy and Security Workshop, Toronto, 2006* (unpublished agenda and background papers, 2006).

[71] Submission, *supra* note 42, p. 73.

[72] Consumer Measures Committee, *Canadian Code of Practice for Consumer Protection in Electronic Commerce*, online: <http://cmcweb.ca/epic/internet/incmc-cmc.nsf/en/fe00064e.html#contents>.

contract formation, cancellation rights, credit card charge-backs and information provision.[73]

4.2.4. Interac Online: Customer Service Rules

These rules set out the customer service requirements that must be put in place respecting INTERAC Online. The requirements focus on the interests of the customer. The Customer Service Rules outline the responsibilities of different parties involved in offering INTERAC Online services.

The service rules are based on general principles, which include: a) INTERAC Online must provide a level of protection to customers that promotes the use of the service as a preferred payment mechanism; b) the creation of appropriate incentives to manage risk, such that the risk of loss will be allocated to the party best able to control the outcome (i.e., the Issuer, Acquirer, Merchant or Customer); and c) customers must be fully informed of the risks associated with the use of INTERAC Online and of the process for dealing with any dispute that arises.[74]

The responsibility of card issuers includes ensuring that the customer accepts the terms of service. The Terms and Conditions stipulate that customers are not liable for losses resulting from circumstances beyond their control. These circumstances include:

i. losses resulting from system malfunctions, technical failures, or other processing errors at the issuer or at any person for whom the issuer is responsible;
ii. losses caused by fraud or negligence at the issuer or by any person for whom the issuer is responsible;
iii. losses where the customer has been the victim of fraud, force or intimidation, provided that the customer has not contributed to the loss, promptly notifies the issuer when (s)he becomes aware of the incident and cooperates fully in any subsequent investigation.

The Customer Service Rules recognize the risks posed by the use of the system, including the risk that customers might be victims of fraud. However, the protections that must be put in place are described using vague language. There is no indication, for example, as to how "a level of protection to customers that promotes the use of the Service" will be provided.

5. CONCLUSIONS

This paper has provided a selective overview of government and corporate sector policies that can help prevent, detect, or reduce the impact of identity theft. These sectors are

[73] Industry Canada, *Internet Sales Contract Harmonization Template*, online: <http://strategis.ic.gc.ca/epic/internet/inoca-bc.nsf/vwapj/Sales_Template.pdf/$FILE/Sales_Template.pdf>.
[74] ACSYS, *Interac Online: Customer Service Rules*, 1 March 2005, online: <http://www.interaconline.com/customer_service_rules.pdf> at p. 3.

becoming increasingly aware of the importance of having such policies, not only for the benefit of their clients but also for themselves. There is still considerable scope for new and improved policies, leading to better practices. Moreover, governments and businesses have policies that in fact leave individuals vulnerable to the threat of identity theft, even though this is not intended. However, progress has been made on many fronts.

Nongovernmental organizations, which come in many shapes and sizes, operate on the fringe of the policymaking process. Nevertheless, individually and collectively, they bring a different and generally useful perspective to the problem. They help to bring issues to the attention of governments and businesses and propose solutions. Although it is difficult to measure their impact on policymaking, it is reasonable to assume that they do carry some influence.

This Paper also illustrates the cross-jurisdictional nature of identity theft problems and solutions. Domestically, policy solutions require more than single-source initiatives. Federal/provincial/territorial initiatives such as the Consumer Measures Committee, joint government-industry cooperation, and participation in the activities of international bodies are all needed to provide a thorough, united, and effective solution to the problem of identity theft.