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

ENFORCEMENT OF IDENTITY THEFT LAWS

July, 2007

CIPPIC Working Paper No. 5 (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 Researchers: Wendy Parkes, Mark Erik Hecht
Research Assistants: Thomas Legault, Janet Lo
Project Director: Philippa Lawson

Suggested Citation:

CIPPIC (2007), "Enforcement of Identity Theft Laws", CIPPIC Working Paper No.5 (ID Theft Series), July 2007, Ottawa: Canadian Internet Policy and Public Interest Clinic.

Working Paper Series:

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

CIPPIC

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

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

TABLE OF CONTENTS

Page

EXECUTIVE SUMMARY

This paper identifies and discusses issues regarding the investigation and prosecution of identity theft crimes. It reviews the challenges facing law enforcement agencies, many of which stem from the inter-jurisdictional nature of such crimes as well as the lag time between the acts of theft or fraud and their discovery. The cross-jurisdictional nature of identity theft calls for the collaboration between different agencies, while the increasingly sophisticated techniques used by identity thieves results in thieves often being one step ahead of law enforcement agencies.

Despite these challenges, there have been many successes on the law enforcement front. Improved awareness and training on the part of law enforcement agencies, closer attention to victim concerns, and inter-jurisdictional cooperation between law enforcement agencies appear to be helping police in their efforts to catch and prosecute identity thieves.

NOTE RE TERMINOLOGY

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

1. INTRODUCTION

Law enforcement agencies play a central role in combating identity theft and in assisting victims. Yet, investigating and prosecuting cases of identity theft present several significant challenges to law enforcement agencies. According to one of Canada's leading police forces, identity theft is *the* most difficult crime to investigate.[1]

Various actors within government and law enforcement agencies are involved in the investigation and prosecution of identity theft. While federal and provincial departments play a role, the central responsibility often falls on the shoulders of local police forces. Identity theft laws cannot be effective if local law enforcement agencies lack the resources to investigate identity theft and collect evidence required for successful prosecutions.[2]

While identity theft raises enforcement issues common to other types of crime, it also poses its own set of unique challenges. This paper examines those challenges and reviews how they are being addressed by law enforcement agencies in Canada and the United States (U.S.). As will be seen, many reports have been published documenting the American experience. Thus far, no equivalent studies have been conducted in Canada and, as such, interviews with law enforcement officials coupled with police commentary in mainstream media are solely relied upon to inform the Canadian perspective.

2. CANADIAN INITIATIVES

2.1 Reporting and Recording of Identity Theft

2.1.1 Reporting Economic Crime On-line (RECOL)

In Canada, the Royal Canadian Mounted Police (RCMP) has created a Web-based initiative known as "Reporting Economic Crime On-line" (RECOL). RECOL is an integrated partnership between international, federal and provincial law enforcement agencies.I It includes regulators and private commercial organizations that have investigative interest in receiving a copy of economic crime complaints.[3] RECOL recommends which law enforcement, regulatory agency or private organization should take the lead in conducting the initial investigation. It also provides real time data on current trends and support for prevention and awareness.

---

[1] Ottawa Police Service, Media Release, "Canadian and American Strategy to Combat Identity Theft" (6 September 2005), online: <http://www.ottawapolice.ca/en/serving_ottawa/media_room/news.cfm?nr_id=2708>.

[2] Philippa Lawson and John Lawford, *Identity Theft: the Need for Better Consumer Protection* (Ottawa: Public Interest Advocacy Centre, November 2003), online: < http://www.piac.ca/financial/full_report> at 35 [PIAC Report].

[3] Reporting Economic Crime On-line (RECOL), online: <http://www.recol.ca/>.

2.1.2 PhoneBusters

Another popular reporting organization in the context of identity theft is PhoneBusters, which was launched in 1993 by the Ontario Provincial Police (OPP) to counter telemarketing fraud. The RCMP and the federal Competition Bureau have since joined as secondary partners in the initiative. PhoneBusters is the central agency in Canada that collects information on telemarketing, advanced fee fraud letters and identity theft complaints.[4] PhoneBusters also plays an educational role for victims of mass marketing scams but does not appear to take part in the investigative or law enforcement process itself.

PhoneBusters' mandate is to facilitate the prosecution of fraud. Its original focus was purely fraudulent telemarketing but has since expanded; however, it remains mainly focused on financial fraud. Not all data compiled by PhoneBusters pertains to identity theft, as many are mass marketing or telemarketing scams. In the realm of identity theft, PhoneBusters tracks complaints of financial victimization as the result of "scams". Thus, the identity theft data that PhoneBusters collects tends to focus on financial identity theft as opposed to identity theft used by criminals to establish aliases. Although PhoneBusters does not publish a definition for identity theft, the organization's Website explains:

> When an impostor co-opts your name, your Social Insurance Number (SIN), your credit card number, or some other piece of your personal information for their use – in short when someone appropriates your personal information without your knowledge – it's a crime, pure and simple.[5]

As such, their definition of identity theft mirrors the one used for the purposes of this paper.

2.2 Investigating Identity Theft

2.2.1 National and Provincial Initiatives

2.2.1.1 Royal Canadian Mounted Police (RCMP)

Although the RCMP does not have an identity theft unit *per se*, its Commercial Crime Branch and its various sub-agencies are involved in investigations related to bankruptcy, counterfeit currency, frauds against the federal government and other types of white-

[4] PhoneBusters, online: <http://www.phonebusters.com/english/aboutus.html>.
[5] PhoneBusters online: <ttp://www.phonebusters.com/english/recognizeit_identitythe.html>.

collar crime at the local, regional, provincial, national and international levels.[6] Located in Ottawa, the Bureau for Counterfeit and Document Examinations provides expertise on counterfeits and documents.[7] The Counterfeit Analysis Program examines suspect travel documents to determine if they are genuine. In addition to examining passports and visas, the program focuses on suppressing the manufacture and distribution of counterfeit payment cards within Canada. The Documents Section examines questionable documents to identify the author, method of protection to see if they have been altered. The RCMP maintains liaison with the U.S. Secret Service and with Interpol for international counterfeit investigations.

2.2.1.2 Ontario Provincial Police (OPP)

The Ontario Provincial Police has an Identity Theft Team located in Orillia, Ontario. The OPP also houses an Electronic Crime Section which provides specialized investigative services to OPP regions and Ontario municipal police services when facing investigations in which electronic equipment or the internet are identified as the key elements of the investigation.[8] The growth of the electronic market and access to high-speed internet has had a significant impact on the number and diversity of requests for assistance received by the Electronic Crime Section. The OPP is a member of the Canadian Bankers Association and Fraud Investigators of Canada who provide up-to-date information to the OPP as identity theft and fraud techniques evolve.[9]

2.2.2 Examples of Local Police Services

2.2.2.1 Ottawa Police Service

Identity theft has been identified as the leading Ottawa scam for 2006.[10] Ottawa's local police force has an Organized Fraud Section devoted to investigating fraud matters and

[6] Royal Canadian Mounted Police, Commercial Crime Branch, online: <http://www.rcmp-grc.gc.ca/fio/commercial_crime_e.htm>.

[7] Royal Canadian Mounted Police, Bureau for Counterfeit and Document Examinations, online: <http://www.rcmp-grc.gc.ca/factsheets/fact_bcde_e.htm>.

[8] Ontario Provincial Police, Investigation Support Bureau, online: <http://opp.ca/Organization/InvestigationsOrganizedCrime/opp_000457.html>.

[9] Interview of Sergeant Detective Debbie Bell of PhoneBusters by Janet Lo (31 May 2007) [Interview with OPP Sgt. Det. Bell].

[10] Jon Willing, "In fraud we trust: Identity theft tops chart in Ottawa scams", *The Ottawa Sun* (10 July 2007), online: <http://www.ottawasun.com/News/OttawaAndRegion/2007/07/10/4327210-sun.html> ["In fraud we trust"]. It is important to note that the article itself does not specify a definition of identity theft. That said, the language is likely consistent with the term used Ottawa Police Services since the list of "scams" cited was compiled by the fraud detective squad. In our interview with Sgt. Harper of the Ottawa Police Organized Fraud Section, he did not specify a definition of "identity theft" as used by their department; however he did use examples of credit card and debit card fraud and title and mortgage fraud as cases of identity theft in which his team would investigate.

trends that can be linked, tracked and documented.[11] Police officers in the Organized Fraud Section investigate all types of fraud including credit card and debit card fraud, counterfeit documents and identity theft. The Organized Fraud Section also investigates phishing and other cyber crimes. That being said, the Organized Fraud Section only investigates fraud that has an "organized" component. The section is comprised of a general investigative team, a debit card fraud team, a credit card fraud team and a corporate fraud team.[12]

The Ottawa Police collaborates with other law enforcement agencies to share their corporate knowledge. Police officials meet on a monthly basis to share information with other local police services, especially those in Montreal and Toronto, as scams tend to target larger urban centres and then migrate to Ottawa. Partnerships with the OPP and RCMP are maintained. As well, the Ottawa Police Organized Fraud Section meets with the Federal Bureau of Investigation (FBI), the U.S. Secret Service, Interpol and banking institutions on a monthly basis.[13]

2.2.2.2 Vancouver Police

The Identity Theft Task Force (ITTF) was initiated by the Vancouver Police Department in early 2005.[14] Its mission is to target suspects involved in identity theft, mail theft and crimes committed for the purposes of gathering personal and financial information. These crimes range from break and enter at medical offices to theft from cars and mail boxes. A liaison has been set up with financial institutions, insurance companies, retail investigators and other businesses to facilitate the pooling of resources to combat identity theft. Establishing an intelligence databank is a priority for the ITTF. It has also created initiatives such as the "bait mail" program and "postal key warning".[15] The Task Force works closely with a Special Crown Prosecutor and a Canada Post Inspector. As well as conducting investigations, the ITTF provides training materials and briefings to law enforcement officers.

---

[11] Ottawa Police, Organized Fraud Section, online: <http://www.ottawapolice.ca/en/serving_ottawa/support_units/fraud_main.cfm>.

[12] Interview of Sergeant Jamie Harper of the Ottawa Police by Janet Lo (6 June 2007) [Interview with Ottawa Police Sgt. Harper].

[13] *Ibid*.

[14] Vancouver Police Department, Patrol Support Section, online: <http://www.city.vancouver.bc.ca/police/operations/patrolsupport>.

[15] The bait mail program involves police officers drafting carefully crafted e-mails to use as "bait" to "catch" Internet scammers. (See also "Scamming the scammers: Web vigilantes work hard to bait email thieves" on ZDNet, online: <http://government.zdnet.com/?p=3283>.) The postal key warning is an initiative where local law enforcement educates their communities on the dangers of easily accessible mailboxes.

3. THE AMERICAN EXPERIENCE

3.1 OVERVIEW

Law enforcement agencies in the U.S. have made strides in combating identity theft in recent years. As noted by one academic, "[I]t is in the area of law enforcement where perhaps the greatest progress has been made so far in the fight against ID theft."[16] In particular, there appears to be an increased willingness of police to write, and make available to victims, identity theft reports and form task forces combining the expertise of law enforcement officers from different jurisdictions and between levels of government.

In the U.S., no single federal agency has jurisdiction over identity theft crimes. Task forces, both formal and informal, enable the pooling of resources, information, and expertise.[17] As well as participating in federal initiatives, many states have created their own task forces to assist in cross-jurisdictional high technology crimes such as identity theft and driver's licence fraud. These task forces also educate law enforcement agencies and assist victims.

Since 2002, a group of U.S. federal law enforcement and regulatory agencies (including the Department of Justice, the Postal Inspection Service, the Secret Service and the Federal Trade Commission (FTC)) have jointly sponsored a series of regional training seminars for state and local law enforcement authorities throughout the country. The participating agencies and the American Association of Motor Vehicle Administrators have conducted many one-day seminars. These seminars include practical guidance and information resources for state and local police, sheriffs and prosecutors on how to respond to and investigate identity theft.[18]

Other initiatives include the National White Collar Crime Center[19] which provides support for agencies investigating high tech crimes and the International Association of Financial Crimes Investigators[20] which works to prevent financial fraud worldwide. Despite the plethora of resources available, a survey performed in 2003 suggests that law enforcement personnel are not always aware of these initiatives and the services they provide.[21]

---

[16] Bob Sullivan, *Your Evil Twin: Behind the Identity Theft Epidemic* (Hoboken, New Jersey: John Wiley & Sons; 2004) at 159 [Sullivan].

[17] Graeme R. Newman and Megan M. McNally, *Identity Theft Literature Review: Report to the U.S. Department of Justice* (July 2005), online: <http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf> at 51[Newman and McNally].

[18] Bi-national Working Group on Cross-Border Mass Marketing Fraud, *A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States: Identity Theft* (October 2004), online: <http://www.ps-sp.gc.ca/prg/le/bs/report-en.asp> at 47 [Bi-national Working Group Report].

[19] National White Collar Crime Center, online: <http://www.nw3c.org/>.

[20] International Association of Financial Crimes Investigators, online: <http://www.iafci.org/>.

[21] Jennette Gayer, "Policing Privacy: Law Enforcement's Response to Identity Theft" (California: CALPIRG Education Fund, 2003), online: <http://www.calpirg.org/reports/policingprivacy2003.pdf> at 10 [Gayer].

The FBI also participates in identity theft investigations by partnering with task forces across the country and agencies such as the Federal Trade Commission (FTC). The FBI sponsors initiatives such as the National Identity Theft Working Group. This working group enables law enforcement, federal regulatory officials and members of the financial services industry to meet regularly to discuss identity theft with the aim of identifying and initiating long-term solutions.[22]

On May 10, 2006 President George W. Bush signed an executive order establishing a new Identity Theft Task Force.[23] The Task Force's mandate is to review the activities of executive branch departments; further improve the effectiveness and efficiency of the federal government's activities in the areas of identity theft awareness, prevention, detection, and prosecution; and promote and enhanced cooperation by federal departments and agencies with state and local authorities.

3.2 Reporting and Recording of Identity Theft

Since 1998, the FTC has been the U.S. federal government's lead agency for combating identity theft. Among other things, it is responsible for gathering data on identity theft crimes. The FTC's Identity Theft Data Clearinghouse is the federal government's database for tracking identity theft complaints, which it defines as "…someone [using] your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes".[24] Victims of identity theft and consumer fraud can call a hotline to report their problems and receive information. Complaints are entered into the Data Clearinghouse. The Clearinghouse assists policy makers in their understanding of the techniques and scope of identity theft in the U.S. The Data Clearinghouse is shared electronically with other law enforcement agencies nationwide via the Consumer Sentinel project

Consumer Sentinel is a "one-stop, secure investigative cyber tool and complaint database" that provides hundreds of law enforcement agencies immediate access to internet cons, telemarketing scams and other consumer fraud-related complaints.[25] Access to Consumer Sentinel is restricted to law enforcement agencies. Although it is a domestic tool, Canada's PhoneBusters is a leading partner of this initiative and some other Canadian law enforcement agencies do have access to Consumer Sentinel.

There are, however, limitations to their databases as not all federal agencies report to them.[26] A 2002 report by the U.S. Government Accountability Office (GAO) concluded

[22] Renny Craats, *Identity Theft* (Canmore: Altitude Publishing, 2006) at 127 [Craats].
[23] The White House, Office of the Press Secretary, "Executive Order: Strengthening Federal Efforts to Protect against Identity Theft" (10 May 2006), online: <http://www.whitehouse.gov/news/releases/2006/05/20060510-3.html>.
[24] Consumer Sentinel, ID Theft Clearinghouse, online: <http://www.consumer.gov/sentinel/idtchart.htm>. See also: <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html>.
[25] Consumer Sentinel, online: <http://www.consumer.gov/sentinel/about.htm>.
[26] Gayer, *supra* note 21 at 15.

that the single most effective step the federal government could take to combat identity theft would be to increase participation by U.S. police agencies in the Consumer Sentinel initiative which enables them to access the Data Clearinghouse.[27] At the time the report was made, few of these agencies were linked to the Data Clearinghouse.

The FTC also makes resources available to assist residents who are identity theft victims and, working with other agencies, conducts training sessions nationally for law enforcement officers.

Other initiatives include the Internet Fraud Complaint Center (now known as the Internet Crime Complaint Center), a joint project of the FBI and the National White Collar Crime Center. It was established in 2000 in response to growing incidents of internet fraud.[28] The Center provides victims of identity theft with a reporting mechanism and refers complaints to law enforcement and regulatory agencies. In its first five years, the Center had received over 100,000 complaints.[29]

In 2000, the FBI reported 922 identity theft arrests. The same year, U.S. federal prosecutors filed 2,172 cases.[30] In the U.S. it has been estimated that only one out of every 700 identity theft crimes is ever prosecuted.[31] One U.S. report found that on average, only 11% of identity theft cases are ever solved.[32]

4. CANADIAN FIGURES ON IDENTITY THEFT

In contrast to the U.S, few statistics are kept on identity theft investigations and prosecutions in Canada. Statistics Canada and the Canadian Centre for Justice Statistics track statistics on "fraud" as a general category of property crime. Fraud, however, is not subdivided to parse out identity theft complaints.[33] Police units track their statistics in a similar way. For example, the Ottawa Police sort their data by section, so the count of cases investigated by the Organized Fraud Section encompasses a broad set of fraud cases some of which are identity theft cases but many which are not.

That said, the statistics that are available are still worthy of note. The Organized Fraud Section of the Ottawa Police, by way of example, receives an average of 3,300 calls per year, 2,200 of which are "legitimate" fraud calls.[34] It is estimated that in Ontario there

[27] Sullivan, *supra* note 16 at 156.
[28] Internet Crime Complaint Center, online: <http://www.ic3.gov/>.
[29] Craats, *supra* note 22 at 129.
[30] Bob Sullivan, "ID theft victims get little help: Law enforcement still struggling to keep up with crime" *MSNBC* (10 February 2003), online: <http://www.msnbc.msn.com/id/3078497>.
[31] Sullivan, *supra* note 16 at 159.
[32] Gayer, *supra* note 21 and Newman and McNally, *supra* note 17 at 58.
[33] Statistics Canada, *Crime Statistics in Canada, 2005* (Canadian Centre for Justice Statistics), online: <http://www.statcan.ca/bsolc/english/bsolc?catno=85-002-X20060049251>.
[34] Interview with Ottawa Police Sgt. Harper, *supra* note 12.

are 1,400 to 1,800 calls reporting identity theft to law enforcement agencies every month.[35]

5. CHALLENGES TO INVESTIGATION OF ID THEFT CRIMES

5.1. Ascertaining the Identity of the Offender

According to Canadian law enforcement agencies, the greatest challenge to enforcing identity theft laws is identifying the suspect- the prerequisite to beginning an investigation.[36] A secondary challenge is the difficulty in identifying when, where and how the victim's identity was compromised. An investigation needs to narrow down the possible circumstances that allowed the victim's identity to be compromised.[37]

Identity theft has become a lucrative business performed by professional criminals who are savvy, tech-smart, well-connected, organized and have the tools and resources to share information with each other.[38] A single offender may often use more than one identity or alias and thieves may use methods that make it difficult to trace their identity. This can complicate and confuse investigators.[39] Technology therefore poses another challenge in ascertaining the offender: it is virtually impossible to track the source of scammers who use pay-as-you-go cell phones and devious email accounts.[40] Law enforcement agents must rely heavily on tips in this regard.

To further complicate matters, it has been estimated that over 85% of fraud suspects provide a different name when they are arrested. Many suspects carry forged identification documents or legitimate identification documents obtained under the name of another person. Where the police are not satisfied with the identity provided by an arrested suspect, they can detain him or her until they are satisfied.[41] Sometimes, identity theft is not discovered until after an individual has been prosecuted for a number of other crimes.[42]

Investigations are never abandoned but they may "go cold". Where an identity thief uses the same address in more than one fraud, a case can often be re-opened. PhoneBusters and RECOL are investigative aids to the police allowing them to find commonalities between similar crimes that are likely to have been perpetrated by the same thief. On occasion, PhoneBusters will compile an information package when there are a number of complaints with a common tie. PhoneBusters will give this information to whichever of

[35] *Ibid.*
[36] Interview with Ottawa Police Staff Sergeant Leo Janveau and Sergeant Investigator Ron Cooper by Thomas Legault (25 September 2006) [Interview with Ottawa Police Staff Sgt. Janveau and Sgt. Investigator Cooper].
[37] Interview with OPP Det. Sgt. Bell, *supra* note 9.
[38] Interview with Ottawa Police Sgt. Harper, *supra* note 12.
[39] Interview with Ottawa Police Staff Sgt. Janveau and Sgt. Investigator Cooper, *supra* note 36.
[40] Sergeant Ron Cooper, Ottawa Police, in "In fraud we trust", *supra* note 10.
[41] Interview with Ottawa Police Staff Sgt. Janveau and Sgt. Investigator Cooper, *supra* note 36.
[42] Interview with OPP Det. Sgt. Bell, *supra* note 9.

their strategic partners is best able to investigate the scam, be it the local police service, institutional or corporate security or even law enforcement agencies outside of Canada.[43]

5.2. Lack of Physical Proximity

One of the first challenges faced by law enforcement agencies is the fact that there may be a large geographical separation between the victim and the identity thief. In an ordinary theft case, police can isolate the neighbourhood and go door to door to talk to witnesses. In an identity theft case, traditional methodology no longer applies.[44]

The standard model of law enforcement assumes that the commission of an offence involves physical proximity between the perpetrator and the victim.[45] This assumption has shaped how law enforcement agencies approach criminal investigations. However, identity theft does not respect local, provincial, regional or international borders. Tracking down those responsible for the crime and forwarding the case for prosecution can become especially difficult when thief and victim are far apart.[46]

5.3. Multiple Jurisdictions

The typical identity theft crime involves at least three parties: the thief, the victim(s) and the defrauded institution(s). A credit card may be stolen in one city and then used in another city or, as is more often the case, online. Fraudulently purchased items may then be shipped to an address in yet another city. The thief is usually in a different jurisdiction than the victim, especially when personal information belonging to the victim was acquired via the internet. The defrauded institution, such as a bank, might be headquartered in yet another jurisdiction.

In such a scenario, law enforcement agencies must deal with multiple jurisdictions which may have completely different laws or legal systems. Some businesses might refuse to provide information to law enforcement agencies from other jurisdictions unless they are served with search warrants or similar judicial instruments.

According to a recent U.S. survey, jurisdictional issues are the biggest hurdle faced by American law enforcement agencies in the investigation of identity theft crimes.[47] A variety of these jurisdictional difficulties exist and law enforcement officials see the lack of inter-agency information sharing and cooperation as a challenge.[48] Without such cooperation, determining which evidence laws apply is difficult. Such considerations may ultimately influence where the offenders are prosecuted.

---

[43] *Ibid.*
[44] Gayer, *supra* note 21 at 5.
[45] Mohamed Chawki and Mohamed S. Abdel Wahab, "Identity Theft in Cyberspace: Issues and Solutions", (Spring 2006) vol. 11 no. 1 Lex Electronica at 5, online: <http://www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf>.
[46] Gayer, *supra* note 21 at 159.
[47] Gayer, *supra* note 21.
[48] Detective Joe Pendleton, Edmonton Police Force (presentation to Privacy and Security Conference, February 13-14, 2003, Victoria, B.C.), in PIAC Report, *supra* note 2 at 35.

Although Canadian law enforcement agencies must contend with the jurisdictional issues that arise from instances of international identity theft, the state jurisdictional issues that exist in the U.S. do not arise. The *Canadian Criminal Code*[49] applies in all provinces and territories as does the *Canada Evidence Act*.[50] However, with the advancements in technology and expansion of organized crime entities, identity theft has truly become an international crime. When the first phase of identity theft is committed via electronic means, the resultant fraud can occur anywhere in the world. A possible solution to this dilemma is the use of extra-territorial law within Canada.

Historically, there has been a legislative presumption against the extra-territorial application of public law statutes as a matter of statutory interpretation in both Canada and the U.S.. This is based on a historical reluctance to infringe on the sovereignty of other States by purporting to regulate conduct that occurs wholly within another jurisdiction.[51] The modern approach differs, as it is based on the recognition that governmental authorities have a legitimate interest in activities that take place abroad but have an unlawful consequence within their jurisdiction. Similarly, authorities also have an interest in activities that take place within their jurisdiction but have unlawful consequences elsewhere.[52] In *Libman*, the Supreme Court of Canada summarized the modern approach to territoriality:

> ...all that is necessary to make an offence subject to the jurisdiction of our courts is that a significant portion of the activities constituting that offence took place in Canada. As it is put by modern academics, it is sufficient that there be a "real and substantial link" between an offence and this country, a test that is well-known in public and private international law.[53]

Following this reasoning, Canadian law enforcement agencies appear to have jurisdiction to investigate identity theft crimes outside Canada as long there is a “real and substantial” link to Canada via the victim or otherwise. As identity theft investigations span multiple jurisdictions it becomes increasingly important for local police services to collaborate with international law enforcement agencies.

5.4. New Technologies

According to police, criminals are increasingly using the internet to engage in various elements of their crimes and to hide from law enforcement agencies.[54] Identity thieves use the internet for many of their activities such as trafficking in personal information and

---

[49] *Criminal Code*, R.S.C. 1985, c. C-46, online: <http://laws.justice.gc.ca/en/C-46/>.
[50] *Canada Evidence Act*, R.S.C. 1985, c. C-5, online: <http://laws.justice.gc.ca/en/C-5/>.
[51] Uniform Law Conference of Canada, *Consumer Protection: Study on Regulatory Jurisdiction in Canada* (July 2001) online: <http://www.ulcc.ca/en/cls/index.cfm?sec=4&sub=4n>.
[52] *Ibid.*
[53] *R. v. Libman*, [1985] 2 S.C.R. 178, online: < http://canlii.org/en/ca/scc/doc/1985/1985canlii51/1985canlii51.html>, at para. 74.
[54] Interview with Ottawa Police Staff Sgt. Janveau and Sgt. Investigator Cooper, *supra* note 36.

credit card data. The internet affords identity thieves a great deal of anonymity, especially for the more technologically inclined thieves who use botnets (i.e., software robots) to hide their tracks. When identity thieves use new technologies, it is difficult for law enforcement agencies to discern a pattern of activity by an individual or group of individuals engaged in large-scale identity theft.[55] Many identity theft cases will therefore go un-investigated because the chances of catching identity thieves on the internet are minimal in an unregulated borderless cyber space.[56]

In North America, investigating identity theft in the age of new technologies is further hampered by the fact that not all agencies have trained staff to detect such criminal activity. Current police academy training does not appear to equip officers to deal with this level of sophistication.[57] Even where police officers do receive the necessary training, technologically complex crimes will add to the time and cost of the investigation.

Collecting evidence is yet another problem associated with online identity theft. The evidence will generally consist of IP addresses used in certain time frames, server logs and emails. Simply understanding the evidence requires a certain amount of technological knowledge. The evidence also needs to be collected quickly because some of it, such as server logs, are only available for a limited period of time after which they are overwritten or automatically deleted.

5.5. Information Breeding and Related Crimes

A single piece of personal information may be used to create forgeries or to obtain additional pieces of information. For example, a driver's licence may be used to obtain credit cards and other pieces of "legitimate" identification. This phenomena – known as identity breeding – increases the difficulty of and time needed for identity theft investigations.

Identity theft can complicate the investigations of other crimes as well. For example, many offenders rely on forged and fraudulently obtained documents in order to conceal their real identity.[58] Fraudsters use lost or stolen cards by trying to assume the appearance of the person on the card.

---

[55] Michael J. Elston and Scott A. Stein, "International Cooperation in On-Line Identity Theft Investigations: A Hopeful Future but a Frustrating Present," 16th Conference of the International Society for the Reform of Criminal Law, Charleston, South Carolina, 6-10 December 2002, online: <http://www.isrcl.org/>.

[56] Detective Bob Gauthier, Edmonton Police Service, in Janice Tibbetts, "Anti-fraud service swamped by victims of identity theft" *Ottawa Citizen* (5 July 2007), online: <http://www.canada.com/victoriatimescolonist/news/story.html?id=58818fc0-15a0-4e82-8ab9-d50db3fbf46f>.

[57] Sameer Hinduja, "Perceptions of local and state law enforcement concerning the role of computer crime investigative teams" (2004) vol. 27, no. 3, *Policing: An International Journal of Police Strategies & Management* at 342.

[58] Interview with Ottawa Police Staff Sgt. Janveau and Sgt. Investigator Cooper, *supra* note 36.

Identity theft typically feeds into other frauds, as fraud is a "go-to ploy" for organized crime syndicates in Ontario.[59] Many organized criminals are turning to the lucrative opportunities generated by identity theft and fraud to fund drug and other habits.[60] These crime networks use the profits generated from identity theft and fraud to go to drugs, weapons, prostitution, loan sharking and lifestyle.[61]

5.6. Failure by Victims and Organizations to Report Theft and Fraud

In the U.S., the FTC reports that only 26% of victims report the incident of theft to the police.[62] According to one investigator:

> [I]t is difficult to determine the actual number of identity thefts because many victims do not report these crimes. Also, there is no single organization that handles identity theft complaints. Reports are made to multiple institutions such as government and police offices, credit bureaus and credit card companies.[63]

In Canada, RECOL and PhoneBusters databases are valuable domestic investigative tools and can provide statistics on the different types of fraud. PhoneBusters reports that its call centre received at least 7,778 phone calls from identity theft victims last year, with estimated losses around $16.3 million.[64] The information in these databases, however, represents the incidents that are simply *reported* to these police initiatives and do not include the incidents of unreported theft. As such, they are not representative of fraud or identity theft rates in Canada. Various surveys estimate that the number of Canadians who have been victimized by identity thieves is between two million and four million. Experts, however, agree that there are no truly reliable statistics to measure the problem.[65]

---

[59] "Fraud a growing rip-off" *Ottawa Sun* (9 July 2007), online: <http://ottsun.canoe.ca/News/BreakingNews/2007/07/09/4326882.html>.

[60] Inspector Barry Baxter, Royal Canadian Mounted Police Commercial Crime Branch, in Carly Weeks, "Weak penalties and crime's ease encourage drugs and arms dealers" *Vancouver Sun* (5 July 2007), online: <http://www.canada.com/vancouversun/news/story.html?id=c0e6ff40-b33d-4a8a-9e85-e16ebe21ca3f>.

[61] Carly Weeks, "Lose your identity with a simple swipe of a card" *The Halifax Daily News* (4 July 2007), online: <http://www.hfxnews.ca/index.cfm?sid=42071&sc=96>.

[62] Newman and McNally, *supra* note 17 at 47.

[63] David Canton, "Today's Business Law: Identity theft targeted" *The London Free Press* (29 October 2005), online: <http://www.lfpress.ca/cgi-bin/publish.cgi?p=110581&x=articles&s=shopping>.

[64] Nestor E. Arellano, "ID Theft on the rise in Canada, reveals survey" *ITWorldCanada.com* (18 June 2007), online: <http://www.intergovworld.com/article/302021160a010408005313808552df54/pg1.htm>.

[65] Janice Tibbetts, "Identity-theft expert says seniors least-victimized age group" *Ottawa Citizen* (9 July 2007), online: <http://www.canada.com/topics/news/national/story.html?id=26903be6-86d0-48f8-b91e-3ad34bee7206&k=99851> For a sampling of Canadian surveys on Identity Theft see: <http://www.insurance-canada.ca/consinfohome/Ipsos--Concern-Identity-Theft-612.php>; <http://www.ipsos na.com/news/pressrelease.cfm?id=2871>; <http://www.competitionbureau.gc.ca/internet/index.cfm?itemID=2281&lg=e>.

It is estimated that debit and credit card fraud costs the Canadian economy about $1 million a day.[66] The Interact Association reported debit card fraud losses totalling 94.6 million in Canada in 2006 and Canadians reported $291 million in Visa, MasterCard, and American Express fraud losses in 2006.[67] RECOL and PhoneBusters are only scratching the surface of identity theft victim reports. So while PhoneBusters was created to counter the problem of telemarketing fraud, today it has come to operate as Canada's national response to identity theft by default because no other agency appears to be taking charge.[68]

Retail stores and merchants, along with individual cardholders, also rarely report theft or misuse of a credit card or bank cards to the police.[69] As well, other businesses often do not report suspect activities. Under-reporting of suspect activities, which could be linked to identity theft, "gives an incomplete image of the situation and may hamper efforts to protect the greater public good."[70] While U.S. law aims to reduce this problem by requiring that organizations report suspicious activity, similar requirements do not exist in Canada. For example, businesses are not required by law to report when thieves hack into their data systems. It is clear that under-reporting represents a large barrier to the accurate collection of national and international statistics on identity theft.[71]

5.7. Lack of Cooperation by Financial Institutions

Several participants in a recent U.S. survey lamented lack of cooperation of their financial institutions in the investigation of identity theft.[72] According to American law enforcement officers, it is a constant struggle to get information from these institutions during the course of investigations. It seems that financial institutions become more cooperative only when they suffer a major loss due to the theft.

---

[66] Inspector Barry Baxtor, Royal Canadian Mounted Police Commercial Crime Branch, in Janice Tibbetts and Carly Weeks, "Your name, wallet prey to ID thieves" *Vancouver Sun* (3 July 2007), online: <http://www.canada.com/vancouversun/story.html?id=3fcde748-2178-4bac-a41d-f0cd0e6b23a1&k=41876> [Your name, wallet prey to ID thieves"].

[67] *Ibid.*

[68] Detective Sergeant Debbie Bell, PhoneBusters, in Janice Tibbetts, "Anti-fraud service swamped by victims of identity theft" *Victoria Times Colonist* (5 July 2007), online: <http://www.canada.com/victoriatimescolonist/news/story.html?id=58818fc0-15a0-4e82-8ab9-d50db3fbf46f> ["Anti-fraud service swamped"]. In our interview with Detective Sergeant Debbie Bell on May 31, 2007, she also suggested that there is often miscommunication and a misunderstanding of the role of PhoneBusters. A common misnomer is the belief that PhoneBusters investigates complaints. PhoneBuster's mandate is to collect information on mass marketing scams. This misnomer is not one that is simply held by the general public. A victim often calls PhoneBusters because the local police have directed them to the hotline to file an investigative report.

[69] Newman and McNally, *supra* note 17 at 47.

[70] Bi-national Working Group Report, *supra* note 18 at 47.

[71] Criminal Intelligence Service Canada, *2005 Annual Report on Organized Crime in Canada: The Organized Crime Marketplace in Canada, Criminal Markets, Financial, Identity Theft*, online: <http://www.cisc.gc.ca/annual_reports/annual_report2005/identity_theft_2005_e.htm >.

[72] Gayer, *supra* note 21 at 10.

Despite the fact that Canadian banks may have the best picture of the true scope of credit card and debit card fraud in Canada, they are not under any legal obligation to share information unless a court order is issued.[73] Banks typically notify the victim when they discover extraordinary account activity that suggests identity theft. If the activity is confirmed by the customer as fraudulent and the bank accepts this assertion, the bank may then ask the customer to file a police report on behalf of the bank, as the bank usually reimburses the victim for the financial loss they have suffered. When a bank notifies the police, there are usually more investigative leads.[74] The Ottawa Police, for example, noted that banks tend to cooperate even when the amount of fraud is not significant.[75] By contrast, some victims have accused the banks of not doing enough to monitor their files for suspicious movements or to assist them in investigating the alleged forgery or fraud.[76] This seems to be supported by various local law enforcement agencies in Canada who have noted banks are often willing to "write off" identity theft as the cost of doing business.[77]

5.8. Limits on Sharing of Information for Investigatory Purposes

The Canadian Association of Chiefs of Police has called for greater access to federal and provincial government databanks for the purpose of validating identification documents.[78] Privacy laws however place limits on the sharing of information among agencies in order to protect Canadians from the abuse of their personally identifiable information. Further examination of this issue is required in order to determine whether or how privacy laws can be structured so as to achieve their goals without unduly impeding law enforcement investigations relating to identity theft.

5.9. Lack of Resources to Investigate Identity Theft

The increase in identity theft investigation and prosecution over the last decade suggests that more law enforcement resources are being directed toward this problem. That said, identity theft investigations can be very expensive as they consume a lot of police time and resources.[79] Law enforcement agencies may find it difficult not only to obtain needed resources but also to quantify in monetary and man power terms the resources devoted to identity crimes.[80]

---

[73] CanWest News Service (3 July 2007).
[74] Interview with Ottawa Police Sgt. Harper, *supra* note 12.
[75] Interview with Ottawa Police Sgt. Harper, *supra* note 12, and Ottawa Police Staff Sgt. Janveau and Sgt. Investigator Cooper, *supra* note 36.
[76] Interview with David Durand, a victim of identity theft, by CIPPIC staff (March 2007) and memo drafted by David Durand (4 May 2007).
[77] Detective Bob Gauthier, Edmonton Police Service, in "Your name, wallet prey to ID thieves," *supra* note 66. The article also recounted the story of Greg Ivany, a Canadian student who was a victim of debit card fraud. Ivany stated that the bank asked him not to contact the police because they did their own investigations. The bank told Ivany that if he contacted the police, it would hamper their investigation.
[78] Canadian Association of Chiefs of Police, Resolution #10/2004, online: <http://www.cacp.ca/> [CACP Resolution].
[79] CIFAS, "Is Identity Theft Serious?, online: < http://www.cifas.org.uk/default.asp?edit_id=556-56>.
[80] Gayer, *supra* note 21 at 13.

Expenses can mount when criminal activity crosses jurisdictional boundaries. A single case may involve investigating hundreds of bank accounts and tracing a similar number of victims. In order investigate identity theft committed via electronic means, investigators need the appropriate tools such as specialized tracking software. These tools can be costly. Further, travel may be required to conduct interviews in other jurisdictions.

According to the offices interviewed in a recent U.S. survey, most police departments classify cases as "workable or un-workable"[81]. A case is deemed un-workable when it has gone "cold". Given that most identity theft cases require roughly one month to investigate, cases become backlogged.[82] The delays in discovering the initial theft and delays in investigating caused by case backlogs often means that cases go "cold" before officers can investigate.

One Canadian officer reported that an "easy" case takes about 100 hours of investigation whereas a "complicated" case can take in excess of 500 hours.[83] The 2003 case of *R. v. Lukian* provides an example of the resource-intensiveness of such investigations. In this case, the main RCMP investigator spent 2,000 hours on the investigation.[84] As such, it is no surprise that an "extremely complicated" investigation can cost over $1 million.[85]

A lack of resources may lead police to refuse to investigate cases involving a loss if the amount is below a certain threshold.[86] In the U.S., thresholds for justifying a criminal investigation can go as high as $100,000.[87] No similar data is available for Canada. On a victim-by-victim basis, however, losses are often well below even the most minimal of police thresholds. Career criminals know about monetary thresholds and can generally avoid being investigated and prosecuted by keeping their fraudulent activity within these limits. Instead, they tend to target multiple victims.

Other considerations in deciding whether identity theft is investigated include the potential involvement of organized crime syndicates.[88] For example, the Ottawa Police Organized Fraud Section does not investigate unless the fraud is "organized." Identity theft is often not limited to lone criminals. Instead, it is an increasingly important tool of

[81] Gayer, *supra* note 21 at 15
[82] *Ibid*. Edmonton Police Detective Bob Gauthier admits that there are "piles and piles" of identity theft files in his office that will never be investigated in "Anti-fraud service swamped", *supra* note 56.
[83] *Gayer, supra* note 21.
[84] *R. v. Lukian*, 2003 ABQB 989.
[85] Interview with Ottawa Police Staff Sgt. Janveau and Sgt. Investigator Cooper, *supra* note 36.
[86] This happened to a woman in Florida, who was told by local police that they would not investigate because the loss did not involve more than $5,000. "Man sentenced to 14 years for ID theft" *Associated Press* (11 January 2005), online: <http://www.msnbc.msn.com/id/6813982/>.
[87] Sullivan, *supra* note 16 at 161.
[88] Newman and McNally, *supra* note 17 at ix.

criminal organizations.[89] The Interac Association has noted that debit card fraud is increasingly perpetrated by organized groups of individuals.[90]

5.10. Lack of Training

Police need special training in order to be able to investigate identity theft crimes effectively.[91] The exploitation of technology through phishing and the use of malware are expected to increase over time.[92] When identity theft is committed via electronic means, specialized training is essential for law enforcement agencies to have any chance of success.

In Ontario, Subsection 135(1) of the *Police Services Act*[93] gives the Lieutenant Governor in Council the power to make regulations prescribing standards for police services including standards for training and equipment provided to police officers. There is currently regulation mandating courses of training for members of the police force which require police officers to complete Basic Constable Training.[94] The Ottawa Police professes to be one of the best trained offices in North America. They are at the forefront of police training with cutting edge technology and equipment and a Professional Development Centre at Algonquin College that teaches specialized police training courses. The Ottawa Police has a high-tech crime unit which uses forensic techniques to investigate computer evidence.[95]

For officers directly assigned to computer forensics and technological crimes investigations, other local law enforcement agencies may require intensive and ongoing training in forensic principles especially focused on the practice and analysis of existing and emerging technologies in computer systems, networking and internet technologies. Training to develop and maintain the skill sets of technology crimes unit members takes an average of four to six weeks per year. Such an undertaking requires both commitment and flexibility from the officers assigned to such units.[96]

In response to these training issues, the Winnipeg Police Service is implementing an understudy program to ensure minimum training standards as well as an ongoing

---

[89] Public Policy Forum, *Public Policy Forum Roundtable on Identity Theft and Identity Fraud*, Ottawa (26 June 2003) at 12, online: <http://www.ppforum.ca/common/assets/publications/en/identity_theft_fraud.pdf>.
[90] Interac Association, "Comments for the 2006 Review of Financial Sector Legislation" (June 2005), online: <http://www.fin.gc.ca/consultresp/06Rev_16e.html>.
[91] Criminal Intelligence Service Canada, "2005 Annual Report on Organized Crime in Canada", online: <http://www.cisc.gc.ca/annual_reports/annual_report2005/table_of_contents_2005_e.htm >.
[92] *Ibid*.
[93] *Police Services Act*, R.S.O. 1990, c. P.15, online: < http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/90p15_e.htm>.
[94] *Courses of Training for Members of Police Forces*, O. Reg. 36/02, online: <http://www.canlii.org/on/laws/regu/2002r.36/20070614/whole.html>.
[95] Interview with Ottawa Police Sgt. Harper, *supra* note 12.
[96] Winnipeg Police Service, "How can police agencies keep up with new technology?", (2005) vol. 67, Issue 1, Gazette, online: <http://www.gazette.rcmp.gc.ca/article-en.html?&article_id=91>.

professional development program for members assigned to technology crimes. It is also implementing online information resources and has plans to extend training to all police officers. The goal is to provide officers with a basic understanding of the current technologies, the evidence that can be obtained and the proper procedures in handling such evidence.

The Ottawa and Winnipeg Police Services are specific examples of good police training in Canada in technology and internet crime but not all police services provide comparable training.

5.11. Perceived Deficiencies in the *Canadian Criminal Code*

Law enforcement agencies point to perceived deficiencies in the *Canadian Criminal Code* (Code) as a key challenge faced in prosecuting identity theft crimes.[97] Offences involving identity theft are typically prosecuted under *Code* sections outlawing various forms of fraudulent activity. The most commonly cited problem is the lack of an offence for possession of identification documentation or personal information with fraudulent intent. Police must instead prove that the documentation or information was a*ctually* used to commit an offence before they can arrest a suspect. The exception to this is the possession of stolen credit cards.[98] In 2004, the Canadian Association of Chiefs of Police called upon the federal government to "clearly define identity theft in the *Canadian Criminal Code* and enact a provision making it an offence to possess multiple pieces of identification."[99] The Department of Justice has been considering a number of possible amendments to the *Code* in order to address these perceived deficiencies.

6. SENTENCING AND DETERRENCE

According to anecdotal evidence from police forces and elsewhere, prison sentences for identity theft are so low that they deter enforcement agencies from spending the time and effort necessary to obtain convictions.[100] One recent article suggests that punishments in Canada are relatively light because the crime is not violent.[101] The article recounts examples of identity thieves who were prosecuted by the criminal justice system and received a "slap on the wrist". By way of example, in December 2005, an Edmonton woman was jailed for seven days for being caught with the credit card numbers of 3,300

[97] See CIPPIC Working Paper on *Legislative Approaches to Identity Theft* for more on this issue.
[98] See *Canadian Criminal Code*, s. 342(3), which states, "Every person who, fraudulently and without colour of right, possesses, uses, traffics in or permits another person to use credit card data, whether or not authentic, that would enable a person to use a credit card or to obtain the services that are provided by the issuer of a credit card to credit card holders is guilty of [….] an indictable offence and is liable to imprisonment for a term not exceeding ten years; or [….] an offence punishable on summary conviction.
[99] CACP Resolution, *supra* note 78.
[100] Interview with Ottawa Police Staff Sgt. Janveau and Sgt. Investigator Cooper, *supra* note 36. Email communication with Brent Grover, Corporate Information and Privacy Advisor, Ministry of Management Services, Government of British Columbia, in PIAC Report, *supra* note 2 at 34.
[101] "Anti-fraud service swamped", *supra* note 68.

online shoppers on her personal computer and numerous drivers' licenses containing her photo and stolen names.[102]

In Canada, sentences for debit card fraud range from a fine to a few months in jail. . These mild sentences do not, apparently, prevent repeat offences, as fraudsters treat them as a "cost of doing business".[103]

Various non-profit groups also support the idea of tougher penalties for identity thieves. In the U.S., penalties for drug-related crimes are so tough that criminals have apparently switched to identity theft as an income generator because rewards can be as lucrative.[104] According to law enforcement officers, penalties for identity theft are often low because prosecutors will only charge perpetrators with one count of the crime even when many individuals were victimized.[105] A recent U.S. survey found that 36% of the officers surveyed agree that stiffer sentences are required.[106] However, 85% of officers think that harsher penalties and consumer education alone will not solve the problem. In Canada, the Canadian Association for the Fifty Plus (CARP) has gone on record as stating that the mild sentences for identity theft is a challenge that puts its members at risk. CARP calls for stiff sentences especially if the victim is over 60.[107]

7. CONCLUSIONS

Law enforcement is an integral and essential step in bringing offenders to justice and thereby deterring other would-be offenders. In Canada and the U.S., law enforcement agencies are making considerable progress in addressing identity theft crimes both domestically and bilaterally. However, data on the extent and types of identity theft in Canada is lacking. Collection of information from victims and accurate reporting of rates of theft are necessary to further understand and combat this criminal enterprise. Moreover, sentences given to identity thieves have yet to reflect the economic gravity of the crime.

Law enforcement agencies are challenged by the increasing and often expert use of new technologies such as the internet by criminals. On one level, law enforcement agencies are simply outnumbered. On another level, agencies lack the technological knowledge and expertise of many criminals. The use of sophisticated technologies in committing identity theft requires highly technical equipment and training to properly investigate and collect useful information. Much of the future success of efforts to combat identity theft will therefore depend on law enforcement agencies' ability to receive sufficient financial and personnel support to combat this increasingly complex crime.

---

[102] *Ibid.*
[103] Interac Association, *supra* note 90.
[104] Sergeant Jim Hyde, Miami-Dade, Florida Police Department, in Gayner, *supra* note 21 at 26.
[105] *Ibid*.
[106] Gayner, *supra* note 21 at 14.
[107] CARP Canada's Association for the Fifty Plus, "CARP's Response to the Department of Justice Consultations" (9 December 2004), online: <http://en.50plus.com/PDF/brief_identitytheft_dec04.doc>.