IDENTITY THEFT:
THE NEED FOR BETTER CONSUMER PROTECTION

Written by Philippa Lawson & John Lawford
Public Interest Advocacy Centre
1204 – ONE Nicholas St.
Ottawa, Ontario
K1N 7B7

November 2003

With Funding from Industry Canada

The Public Interest Advocacy Centre
(PIAC)
Suite 1204
ONE Nicholas Street
Ottawa, ON
K1N 7B7

Tel: (613) 562-4002 Fax: (613) 562-0007

e-mail: piac@piac.ca website: www.piac.ca

Acknowledgements

This paper was written by Philippa Lawson & John Lawford. Research was performed by Kristen Kizoff, Kathleen Priestman, and Naila Parsons.

Canadian Cataloguing and Publication Data

Lawson, Philippa
Lawford, John

IDENTITY THEFT:
THE NEED FOR BETTER CONSUMER PROTECTION

ISBN 1-895060-59-1

IDENTITY THEFT:
THE NEED FOR BETTER CONSUMER PROTECTION

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Identity theft is a rapidly growing problem in Canada. It represents a grave threat to consumer security and confidence in the modern marketplace. It also represents a serious challenge to business in general and to the financial marketplace in particular.

Identity theft is the unauthorized collection and fraudulent use of someone else's personal information. Victims of ID theft suffer financial loss, damage to their reputation, and emotional distress, and are left with the complicated and sometimes arduous task of clearing their names.

ID theft is a truly modern crime, being carried on out of the sight of, and often beyond the effective reach of, the victim. It is carried out through compromising electronic data systems, obtaining false primary documents, directing mail to new addresses, obtaining new credit accounts and improperly charging existing ones. It can be carried out by a next-door neighbour or by criminals hunting from thousands of miles away. It relies on the commercial culture of ubiquitous personal information holdings, easy consumer credit and the facility of modern technology. It also relies on lax consumer security. However, ID thieves also exploit business and government information leaks, credit industry excesses and unsafe practices, inadequate consumer control over trade in credit information, and the use of personal information for collateral uses. Government identification weaknesses, government ID "function creep", a lack of specific ID theft offences, uncoordinated law enforcement and unfocussed privacy laws round out the list. Given these weaknesses, in many cases, there is no action consumers can reasonably take to prevent ID theft.

Biometrics and a national ID card have recently been touted as the answer to ID theft.[1] Neither of these 'magic bullets" will have a serious effect on ID theft. ID theft results from the combination of human and systemic factors listed above and can only be dealt with by addressing the causes individually and collectively.

This report attempts to define the scope of ID theft in Canada and to provide an explanation for its existence. It then provides recommendations for improvement of the present regime in a manner that both respects consumers and has the greatest likelihood of sparing them from the nightmare of ID theft. PIAC calls upon consumers, but especially upon business, government and law enforcement, to meet the ID theft challenge head on.

[1] See the remarks of Minister Denis Coderre, Minister of Citizenship and Immigration, at the forum: "Biometrics: Implications and Applications", Ottawa, October 8, 2003, (http://www.cic.gc.ca/english/press/speech/bio-forum.html) and similar remarks entitled: "Document Integrity And Biometrics: Exploring The Options For Our Future" at the Kiwanis Club, Ottawa, Ontario, September 19, 2003 (http://www.cic.gc.ca/english/press/speech/biometrics.html).

INTRODUCTION

This study was undertaken in order to gain a better understanding of the identity theft problem, to assess its severity from the consumer perspective, and to make policy recommendations to government and other stakeholders.

Research was conducted from June 2002 to October 2003, and included Internet searches, monitoring of news reports, a review of US legislation, and interviews with individual experts and others working on the issue. Many people in government, the private sector, and consumer groups are currently examining the problem of identity theft. Over the period of our research, there has been an enormous increase in attention to the issue as illustrated by the numerous news articles, reports, and legislative initiatives cited. It is hoped that this concentrated attention will result in effective measures to reduce the incidence of, and damage caused by, identity theft.

This report examines identity theft as a consumer issue. It therefore focuses primarily on theft of consumer information for financial gain, rather than on theft or counterfeiting of government-issued identity documents for use by international terrorists and others in non-financial criminal activities. It does not examine the growing problem of "business identity theft", nor does it look at trademark violations as a form of ID theft.

WHAT IS IDENTITY THEFT?

Identity theft ("ID theft") is the unauthorized collection and fraudulent use of someone else's personal information. Victims of ID theft suffer financial loss, damage to their reputation, and emotional distress, and are left with the complicated and sometimes arduous task of clearing their names.

WHY DO THIEVES STEAL IDENTITIES?

The most common purpose of ID theft is financial gain: identity thieves typically use personally-identifying information of others, such as Social Insurance Numbers, credit cards, debit cards and PINs, to open bank accounts, obtain loans, run up utility, cell phone or other bills, and spend money that is not theirs.

Other reasons for stealing personal information include ruining the reputation of another person,[2] starting a new life under a new identity, and avoiding criminal prosecution. Criminals, from local deadbeats to international terrorists, use false identification to escape detection by law enforcement officials, both before and after committing crimes. In the US, innocent ID theft victims have been arrested and jailed for crimes that an imposter committed. Non-criminal imposters also steal and use other identities in order to hide from abusive situations or to leave behind a poor work and financial history.

[2] Mari Frank, "Identity Theft: Who's Helping the Innocent Victims?", *White-Collar Crime Fighter* (May 1999); see also http://www.identitytheft.org

The most common uses of stolen identities, according to the US Federal Trade Commission,[3] are:

- using or opening a credit card account fraudulently;
- opening telecommunications or utility accounts fraudulently;
- passing bad cheques or opening a new bank account in the other person's name;
- getting loans in the other person's name; and
- working in another person's name.

This report focuses on consumer ID theft, as opposed to identity cloning,[4] or business ID theft.[5] In particular, it focuses on ID theft as the basis for financial fraud – the most common way in which ID thieves abuse their victims.

WHAT PERSONAL INFORMATION IS USED BY ID THIEVES?

While virtually all personally-identifying information can be useful to identity thieves, commonly stolen information includes:

- name, address, telephone number
- date of birth
- mother's maiden name (commonly used as a password)
- Social Insurance Number (SIN)
- credit card number and expiry date
- bank account number and Personal Identification Number (PIN)
- driver's licence number
- health card number
- passport
- birth certificate

THE NATURE AND EXTENT OF IDENTITY THEFT

How it occurs

Identity thieves obtain personal information in a variety of ways, including:

- outright theft, such as:
  - stealing wallets and purses;
  - stealing PDAs and laptop computers;
  - stealing mail with banking or credit card statements, pre-approved credit offers, telephone calling cards or tax information;

---

[3] See: http://www.consumer.gov/idtheft/info.htm. See also: http://www.idtheftcenter.org/facts.html.

[4] Identity cloning: "In this crime the imposter uses the victim's information to establish a new life. They work and live as you." (ID Theft Resource Center: http://www.idtheftcenter.org/cresources.shtml). Although perpetrators usually establish themselves at another address in an attempt to avoid contact with the law under their true identity, extreme examples including copying the victim's physical appearance, habits and even occupying the victim's home.

[5] Business ID theft is similar to personal identity theft. "Typically the perpetrator gets credit cards or checking accounts in the name of the business. The business finds out when unhappy suppliers send collection notices or their business rating score is affected." (ID Theft Resource Center: http://www.idtheftcenter.org/cresources.shtml).

    - stealing computer hard drives from businesses or government;[6] or
    - stealing personal information from workplace records or computer databases;
- finding of lost wallets, purses, PDAs or laptops (often graciously "returned" after the information is copied);
- rummaging through the garbage for personal data ("dumpster diving");
- digging up information from publicly available sources, such as the Internet, funeral notices, or public directories;
- hiring online data brokers to search electronically for personal information about someone;
- bribing employees of a business to hand over personal information about customers;
- purchase of used computing equipment, usually from financial institutions, hoping for inadvertently undeleted personal information files;[7]
- hacking into computer databases via the Internet;
- creating "phisher" websites, often posing as billing sites for legitimate online commerce sites, designed to solicit personal information from web surfers[8];
- watching people type in their PINs in bank machines and debit card terminals, or using a phony terminal to obtain PINs; and
- "pretexting"[9] – for example:
    - posing as an Internet service provider, potential employer, or market researcher and requesting personal information directly from the individual for a seemingly legitimate purpose; or even
    - posing as an "identity theft prevention" service and obtaining personal information such as drivers licence no., SIN, mother's maiden name, and bank account numbers.

ID thieves may act alone or in concert, as part of an organized criminal activity. ID theft is often linked to other fraudulent activities, and larger organized crime activities. For example, Canadian law enforcement officials estimate that that there are hundreds of financial lending scams operating out of this country, which not only bilk customers of money directly,[10] but also obtain personal information such as credit card numbers from the scam victims and fraudulently use that information to further the scam.[11] There has even been the suggestion that ID theft is widely used to finance and facilitate other crimes, such as terrorism.[12] ID theft may therefore become a national security issue.[13]

---

[6] Recent events have shown government is not immune from break-ins. See "Theft threatens privacy of 120,000 – Revenue minister orders probe after computers stolen from tax office", September 30, 2003, Citizen special (Canada.com). Online at: http://canada.com/national/story.asp?id=B80CF8C4-3F7E-4836-9A4A-0355D87F537B.

[7] See "'Error' sends bank files to eBay" *Toronto Star*, September 15, 2003, and ""Bank tells 350 clients it messed up", *Toronto Star*, September 19, 2003 (http://www.thestar.com/).

8 See "Web site spoofer pleads guilty, faces prison" *IDG News Service*, September 16, 2003 (http://www.arnnet.com.au/).

[9] See the FTC's fact sheet on pretexting at http://www.ftc.gov/bcp/conline/pubs/credit/pretext.htm

[10] e.g., by offering loan or debt consolidation services for a fee, but never providing the services.

[11] Mark Anderson, "Scammers posing as lenders to snatch info", *Sacramento Business Journal*, February 28, 2003.

[12] Jennette Gayer, "Policing Privacy: Law Enforcement's Response to Identity Theft", CALPIRG (May 2003) ("Policing Privacy") at p. 8 (http://www.calpirg.org/reports/policingprivacy2003.pdf).

[13] See "Identity Crisis", Washington Post Magazine, August 10, 2003, p. W14.

How the damage is done

Once they have enough information (e.g., name, address, credit card, SIN, mother's maiden name), identity thieves pretend to be that person, and may do any of the following in the guise of the other person:

- open a new credit card account (e.g., using name, date of birth, and SIN), and not pay the bills (the delinquent report is then reported on the victim's credit report);
- ask the post office to redirect mail to another location – this way, they not only hide bills from the victim for some time, but also obtain more personal information about the individual;
- ask the credit card issuer to change the mailing address for credit card statements, so that the victim doesn't realize that charges are being run up;
- ask the bank to increase the credit limit on the credit card;
- open a bank account and write bad cheques on the account;
- obtain wireless or other phone service and run up large bills;
- withdraw monies from the victim's bank account;
- purchase cars or other expensive items, by getting a loan in the victim's name;
- buy misleading domain names on the Internet (e.g., "change-ebay.com") that are then used to defraud consumers out of money and/or more personal information;[14]
- pose as another person selling goods in an online auction, but don't deliver the goods;[15]
- sign up for Internet accounts which are then used to send spam, and use another person's email address as the return address on spam messages;[16]
- file for bankruptcy to avoid paying debts or being evicted, in the victim's name

[14] Paul Fiesta, "Identity Thieves strike eBay", CNET News.com (Nov.22, 2002).
[15] Leslie Walker, "Bidding for Trouble?", *Washington Post* (May 11, 2003) p.F01.
[16] Saul Hansell, "Man charged with fraud in spam case", *The New York Times: nytimes.com* (May 15, 2003).

How ID Theft Victims' Information is Misused[17] 2002 161,819 Victims			
Theft Type	**% of all Victims**	**Theft Type**	**% of all Victims**
Credit card fraud	**42**	**Phone or utilities fraud**	**22**
- New accounts	24.4	- Wireless new	10.5
- Existing accounts	12.1	- Telephone new	5.2
- Unspecified	5.4	- Utilities new	3.0
		- Unauthorized charges to existing accounts	0.7
		- Unspecified	2.2
Bank fraud	**17**	**Employment related fraud**	**9**
- Existing accounts	8.1		
- New accounts	3.7		
- Electronic funds transfer	3.1		
- Unspecified	2.0		
Government documents or benefits fraud	**8**	**Loan fraud**	**6**
- Driver's licence issued/forged	3.0	- Personal/business loan	2.6
- Fraudulent tax return	1.9	- Auto loan/lease	2.1
- Social security card issued/forged	1.7	- Real estate loan	0.9
- Government benefits applied/received	0.8	- Unspecified	0.5
- Other government documents issued/forged	0.3		
- Unspecified	0.1		
Other identity theft fraud	**16**	**Attempted identity theft**	**8**
- Other	9.1		
- Illegal/criminal	2.0		
- Medical	1.7		
- Internet/email	1.4		
- Apartment/house rented	1.0		
- Bankruptcy	0.4		
- Securities/other investments	0.2		

A significant and growing problem

There are no comprehensive statistics on identity theft in Canada. Victims complain to a variety of diverse bodies, including credit bureaus, banks, credit card companies, the

[17] Federal Trade Commission, *National and State Trends in Fraud and Identity Theft*, January 22, 2003, p. 9. The data in the report is from Consumer Sentinel and the Identity Theft Data Clearinghouse. Seven per cent of the 2002 Consumer Sentinel complaints were contributed by PhoneBusters, a national telemarketing fraud centre operated by the Ontario Provincial Police. The percentages add to more than 100 because 22 per cent of victims reported more than one type of identity theft.

government, and police, making it difficult to pin down and monitor statistics on this phenomenon. Law enforcement agencies started collecting and reporting statistics only recently, and are now attempting to track them via a national anti-fraud service called "PhoneBusters".[18] PhoneBusters reports the following identity theft complaint statistics for 2002 and 2003 as of September 3, 2003:[19]

	2002	
PROVINCES	**VICTIMS**	**$ LOSSES**
ON	4028	$ 5,643,102.19
BC	1042	$ 912,680.40
AB	635	$ 593,599.25
MB	196	$ 165,953.92
SK	106	$ 54,747.82
UNKNOWN	144	$ 1,235.00
NB	131	$ 130,455.19
NS	185	$ 138,932.62
NF	46	$ 24,855.20
PE	16	$ 2,183.42
NT	2	$ 0
QC	1644	$ 1,160,533.44
YT	2	$ 0
NU	1	$ 1,100.00
TOTALS	**8178**	**$ 8,829,378.45**
AT RISK	1978	N/A

	To 3/09/03	
PROVINCES	**VICTIMS**	**$ LOSSES**
ON	3874	$ 9,085,468.61
BC	1206	$ 925,418.84
AB	724	$ 806,745.84
MB	133	$ 165,565.52
SK	125	$ 289,478.41
UNKNOWN	50	$ 13,842.66
NB	119	$ 219,119.47
NS	139	$ 84,569.68
NF	61	$ 84,015.56
PE	10	$ 2,150.00
NT	1	$ 0
QC	2372	$ 2,428,490.31
YT	1	$ 0
NU	2	$ 3000.00
TOTALS	**8817**	**$14,107,864.90**
AT RISK	436	N/A

[18] PhoneBusters is described as the "national deceptive telemarketing call centre, operated by the Ontario Provincial Police." It collects victim evidence, documentation and statistics. It was created in 1993 to fight telemarketing scams, but now works on identity theft and other online frauds as well. See www.phonebusters.com .

[19] See http://www.phonebusters.com/Eng/Statistics/idtheft_stats_index.html. All figures are as of September 3, 2003, stated in Canadian funds. "$ Losses" represent any losses that are incurred because an identity theft has taken place. It could be anything from charges to a credit card, withdrawal from banks, merchandise purchased or cash stolen from a wallet.

In 2002, PhoneBusters thus reported 8178 ID theft victims, with losses amounting over $1,000 per victim. In the first three quarters of 2003, it reported 8817 victims, with losses of $1600 per victim. These numbers only include cases reported to PhoneBusters, and so do not give a complete picture of the extent of the problem. Detective Staff Sergeant Barry Elliot of PhoneBusters notes that many thefts go unreported, and that the actual number of victims and losses is therefore likely much higher.[20] In spring 2002, he estimated that there are approximately 1,000 victims of identity theft per month in Canada, or 12,000 a year.[21] The third quarter 2003 PhoneBusters statistics bear this estimate out. However, others peg the number of victims as much higher: for example, John Sliter of the Royal Canadian Mounted Police Economic Crimes Branch estimated that "20,000 Canadians will fall victim to the theft of their vital information in 2002."[22]

Credit reporting agencies – also known as credit bureaus – deal with ID theft because they maintain consumers' credit reports. ID theft victims must contact the credit bureaus to have their credit reports corrected and to place fraud alerts on their reports to prevent the granting of credit to ID thieves. Credit bureaus have an interest in the accuracy, reliability and integrity of their databases, and therefore in the battle against ID theft. As such, they are uniquely placed to understand the extent of the problem of identity theft.

Equifax Canada Inc. (Equifax), a major credit bureau, has seen an alarming increase in ID Theft reports. In 2000 Equifax handled 8,000 ID theft cases, up from 6,000 cases in 1999. In 2001 Equifax handled just over 12,000 cases. In 2002, that number had grown to over "17,000 incidents, nearly a 50% increase [from 2001]".[23] According to Equifax, "The most common instances of identity fraud occur with credit cards, cell phone memberships, furniture and electronic merchandise financing attempts, car leases, lines of credit and mortgage applications."[24] Equifax now encourages consumers with ID theft problems to contact PhoneBusters; with the permission of ID theft victims, Equifax will transmit its fraud information to PhoneBusters so that the data may be analyzed by PhoneBusters "to identify if any trends exist and . . . which institutions, regions or other sources are being targeted."[25]

Trans Union of Canada Inc. (TransUnion), the second major credit reporting agency in Canada, provides the following statistics showing trends in financial fraud in Canada since February 1997.[26] While not all of these frauds necessarily involve ID theft, the increase in cases each year is particularly notable, as are the high number of cases deemed by TransUnion to have "fraud potential":

---

[20] K. Marron, "Identity thieves plunder the Net" *The Globe and Mail* (28 June 2002) E1-2.
[21] L. Koziey, "Watchdog warns of savvy crooks: Commercial crime costly" *Calgary Herald* (19 April 2002) City B12, online: Canada.com < http://www.canada.com/calgary/calgaryherald/>.
[22] R. Soparlo, "Be careful about personal information" *The Leader Post (Regina)* (19 June 2002) Business & Agriculture B4/Front, online: Canada.com < http://www.canada.com/regina/leaderpost/>.
[23] Equifax Canada Inc., "Equifax and Phonebusters Assist Victims of Identity Fraud". Information Source, Winter 2003, www.equifax.ca.
[24] Equifax Canada Inc., "Protecting Your Identity", *Information Source*, Winter 2001, www.equifax.ca.
[25] "Equifax and Phonebusters Assist Victims of Identity Fraud", *supra*, at p. 2.
[26] Letter from Chantal Banfield, General Counsel, Trans Union of Canada, Inc., dated September 11, 2003.

Date	Total incoming	Total Processed: Fraud Confirmed	Total Processed: Fraud Potential
1997 (Feb. to Dec.)	982	**293**	689
1998	1937	**655**	1282
1999	4125	**1228**	2897
2000	8848	**2249**	6399
2001	16313	**5958**	9756
2002	24630	**5737**	20484
2003 (Jan. 3 – Jul. 3)	26683	**6764**	20631

Identity theft is a significant and an apparently growing problem in other countries as well. A British government report said last year that "identity theft is rife" in that country.[27] In the United States, identity theft has become a major national issue. Three national surveys of US adults, two in May 2003 and one released September 2003,[28] concluded that between 3.4% and 4.6% of US consumers (app. 7-10 million people) were victims of ID theft of some form in the previous year, an 81% rise over the number of victims in 2001.[29] In the Gartner study, identity theft was defined as a financial crime in which thieves steal personal information such as social security numbers, driver's license numbers, addresses, credit card number or bank account numbers and use that information to pose as the victim.[30] In the Harris Interactive survey, ID theft was defined as "a situation where someone assumes the identity of another and makes telephone calls or obtains merchandise, credit, or other valuable things in their name."[31]

The Harris survey further concluded that 33.4 million Americans have been victims of ID theft or fraud since 1990, that the incidence of ID theft is increasing, and that victims' out-of-pocket expenses have totaled $1.5 billion annually since January 2001.[32] The Synovate Report numbers were higher; it concluded that 12.7% of Americans had been victims of some form of ID theft in the last 5 years,[33] with the total annual cost to victims estimated at about $5 billion.[34]

The Federal Trade Commission (FTC) reported earlier this year that ID theft was the top fraud complaint reported by consumers in 2000, 2001, and 2002.[35] Forty-three percent of

[27] Cabinet Office, *Identity Fraud: A Study*, July 2002, p. 4.
[28] Federal Trade Commission – Identity Theft Survey Report, September 2003, http://www.ftc.gov/os/2003/09/synovatereport.pdf (Synovate Report).
[29] Gartner press release (July 21, 2003): see http://www4.gartner.com/5_about/press_releases/pr21july2003a.jsp . Reported in Robert Lemos, "Analyst: Crime pays for identity thieves" *CNET News.com* (July 21, 2003).
[30] Gartner distinguished between credit card fraud with and without ID theft, finding that 5.5% of US adults surveyed were victims of plain credit card fraud.
[31] Privacy & American Business, Press Release (July 30, 2003); see http://www.pandab.org/ .
[32] *Ibid.*
[33] Synovate Report, p. 11.
[34] Synovate Report, p. 6.
[35] Federal Trade Commission, news release, *FTC Releases Top 10 Consumer Complaint Categories in 2002*, January 22, 2003.

consumer fraud complaints to the FTC in 2002 involved identity theft.[36] In 2002, the FTC received reports from 162,000 ID theft victims, who reported 24 types of ID theft fraud to the Consumer Sentinel Network[37], an international network that collects information from over 100 organizations. Twenty-two per cent of the victims reported experiencing more than one type of ID theft. PhoneBusters Canada contributed seven per cent of the 2002 ID theft complaints to Consumer Sentinel.

The FTC now maintains a webpage devoted to the issue, and, together with other government and law enforcement agencies, consumer groups, and legislators, is attacking it on numerous fronts.[38]

ID theft is thus more than a significant problem – it's a *growing* problem. According to Tim Hudak, Ontario Minister of Consumer and Business Services, "In the past five years, identity theft has emerged as the fastest growing and most serious consumer crime in North America."[39] ID theft in the Consumer Sentinel database grew from 31,000 in 2000 to 86,000 in 2002 and then to 162,000 in 2002.[40] It is projected to jump to 210,000 for 2003.[41] In the UK, identity fraud increased by 462 per cent in 2000 compared with 1999, followed by another increase of 122 per cent in 2001.[42]

A costly problem

While the extent of ID theft incidence in Canada is not as clear, there is even more uncertainty over the cost of ID theft to victims, and to the economy as a whole. Referring to statistics for October 2001 to June 2002, indicating total losses of just under $6 million, spread over 5,352 victims, Detective Staff Sergeant Elliot of PhoneBusterss stated that the "figure probably reflects total losses of more than $20-million, as the full extent of losses from identity theft are not usually known when the crime is first discovered."[43]

As noted above, PhoneBusters' data suggests average monetary losses to Canadian ID theft victims of $1000 in 2002 and $1600 more recently. Other estimates run as high as $30,000 per victim.[44] According to a survey of ID theft complainants conducted in 2000

---

[36] Federal Trade Commission, National and State Trends in Identity Theft, January – December 2002 (http://www.consumer.gov/sentinel/pubs/Top10Fraud_2002.pdf).
[37] Consumer Sentinel members include more than 600 law enforcement agencies in Australia, Canada and the United States. It helps them build cases and detect trends in consumer fraud and identity theft. Consumer Sentinel gives law enforcers access to over 900,000 complaints. Source: www.consumer.gov/sentinel.
[38] See http://www.consumer.gov/idtheft/
[39] Ministry of Consumer and Business Services, news release, *Ontario government cracks down on identity theft*, June 24, 2002.
[40] Federal Trade Commission, *National and State Trends in Fraud and Identity Theft January – December 2002*, January 22, 2003, p. 3.
[41] Federal Trade Commission, Report – FTC Overview of the Identity Theft Program, October 1998 – September 2003, September 2003, fig. 1 (http://www.ftc.gov/os/2003/09/timelinereport.pdf.)
[42] Cabinet Office, *Identity Fraud: A Study*, July 2002, p. 14.
[43] K. Marron, "Identity thieves plunder the Net" *The Globe and Mail* (28 June 2002) E1-2.
[44] Inex Dyer, "Beating the Identity Thieves", *Ottawa Citizen* (July 13, 2003) p.D1.

by the US-based Privacy Rights Clearinghouse and the California Public Interest Research Group, it costs the average US victim more than US$800 in out-of-pocket expenses to cope with the damage to their accounts and reputations.[45] An FBI report issued in December 2002 cited an average victim loss of US$2,000.[46] The Synovate Report estimated that victims spent "[US]$500 on average to deal with their ID Theft experience" but that victims of "new accounts" frauds had to spend an average of US$1200.

The costs of identity theft go further than out-of-pocket victim losses. They include lost productivity due to time spent by victims at work, costs to businesses (e.g., losses due to credit and debit card fraud, time spent dealing with consumer complaints and providing victim redress), and time spent by victims outside working hours clearing their names.[47] The U.S. FTC Synovate Report, cited above, found that ID theft victims on average spent 30 hours to resolve their problem but that "new accounts" victims spent 60 hours.[48] The PRC/CALPIRG report cited above found that "victims spent an average of 175 hours actively trying to resolve the problems caused by their identity theft. Seven respondents estimated that they spent between 500 and 1500 hours on the problem."[49] According to the *Toronto Star*, a US consulting firm, Financial Insights, estimated it takes about 14 months before a consumer becomes aware of an ID thief's fraudulent activities.[50] However, the Synovate Report gives a more conservative estimate, stating that 1/3 of victims discover misuse of personal information within one week, while 12% of victims took more than 6 months to discover the misuse.[51]

One recent US report estimated that ID theft costs businesses in that country US$3.5 billion per year.[52] However, the Synovate Report cites a shocking figure of $47.6 billion lost to U.S. businesses last year.[53] The Canadian Council of Better Business Bureaus estimates that identity theft costs at least $2.5 billion a year to Canadian consumers, banks, credit card firms, stores and other businesses (aggregate).[54] ID theft is therefore

---

[45] http://www.privacyrights.org/ar/idtheft2000.htm .
[46] Manny Frishberg, "Concern grows about ID theft", *Wired News* (April 17, 2003)
[47] CALPIRG, Nowhere to Turn: Victims Speak Out on Identity Theft, May 1, 2000 (http://www.calpirg.org/consumer/privacy/idtheft2000/idtheft2000.pdf).
[48] Synovate Report, p. 6.
[49] *Op cit*., PRC/CALPIRG study.
[50] "Exxon Valdez of data leaks may have happened", *Toronto Star*, February 17, 2003, www.thestar.com.
[51] Synovate Report, p. 20.
[52] Manny Frishberg, "Concern grows about ID theft", *Wired News* (April 17, 2003), referencing a report by Senator Diane Feinstein (D-Calif.).
[53] Synovate Report, p. 7. The methodology used by the Report authors in achieving this figure is questionable. The Report extrapolates business losses from responses by victims. "Victims were asked to estimate the value of what the thief obtained from businesses, including financial institutions, using the victim's personal information." Report, p. 41. No attempt is made to define or break down the type of costs incurred by businesses. A more logical approach would be to survey the businesses directly affected, and particularly the financial and insurance firms who must often bear the final cost of fraud.
[54] Telephone conversation with Bob Whitelaw, President (June 25, 2003), and quoted by Minister Denis Coderre in an address to the Standing Committee on Citizenship and Immigration (Feb.6, 2003). This figure includes business losses to "brands" such as copyright infringement.

an important business issue,[55] although not as personal or devastating as it is a consumer issue.

More than financial loss

Apart from the direct financial loss to consumers, ID theft causes other harm. As the United States General Accounting Office (GAO) said last year:

> "Identity theft can cause substantial harm to the lives of individual citizens – potentially severe emotional or other non-monetary harm, as well as economic harm. Even though financial institutions may not hold victims liable for fraudulent debts, victims nonetheless often feel "personally violated" and have reported spending significant amounts of time trying to resolve the problems caused by identity theft – problems such as bounced checks, loan denials, credit card application rejections, and debt collection harassment."[56]

The GAO noted that some ID theft victims are subjected to criminal investigation, arrest, or conviction as a result of the thieves' activities.[57] For example, a victim was the subject of an arrest warrant based on speeding tickets issued to the perpetrator.[58] Some victims have also been denied employment or lost their jobs.[59]

A borderless crime

ID theft is increasingly a continental and global crime, a development reflected in Consumer Sentinel's international membership. The transborder flow of personal information for data processing and electronic commerce means that Canadians' information can be processed and stored almost anywhere in the world.[60] In February of this year a hacker accessed an American firm's computer system that held information on eight million accounts, including 100,000 Canadian credit card holders.[61] The Internet also allows a potential identity thief anywhere in the world to attempt the theft of personal information processed and stored in Canada or information on Canadians stored elsewhere in the world.

---

[55] The Canadian Bankers Association, however, notes a year over year decrease in dollar losses associated with credit card fraud (2000-1). See: http://www.cba.ca/en/content/stats/fastfacts/credit_card_fraud.pdf.
[56] United States General Accounting Office, *Identity Theft, Prevalence and Cost Appear to be Growing*, March 2002, p. 8.
[57] *Ibid.*
[58] *Ibid.*, p. 58.
[59] *Ibid.*, p. 56.
[60] However, note that the Organization for Economic Co-operation and Development (OECD) has issued "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (http://www1.oecd.org/publications/e-book/9302011E.PDF) which may mature into some form of protection. However, note a recent "health information ransom-taking" by a Pakistani data processor: D. Lazarus, San Francisco Chronicle, "A tough lesson on medical privacy: Pakistani transcriber threatens UCSF over back pay", October 23, 2003, http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2003/10/22/MNGCO2FN8G1.DTL
[61] "8 million credit card numbers accessed", *The Ottawa Citizen*, February 19, 2003.

FACTORS CONTRIBUTING TO IDENTITY THEFT

Many factors have contributed to the rise in incidence of identity theft over the past several years. Consumer behaviour is just one aspect of the problem; in many cases, there is nothing that the consumer could reasonably have done to prevent the theft.[62]

The US Public Interest Research Group contends that ID theft in the USA happens for two primary reasons: easy availability of Social Security Numbers, and sloppy practices of creditors and credit bureaus.[63] It is not clear what factors are most to blame for ID theft in Canada. What is clear, however, is that ID thieves are able to obtain credit under false pretenses too easily, and that even if consumers took all appropriate security measures, ID theft would remain a serious issue in Canada.

Cards, cards everywhere

The growth of credit, debit and banking cards is a major catalyst for the growth of ID theft. More credit cards and banking cards mean more potential opportunities for an ID thief, particularly when credit is easy to get, when merchants fail to authenticate credit card users' identity, and when some consumers and businesses are careless with information such as PINs.

ATM and debit cards

More than 34 million banking cards are in circulation among an adult population of 21.8 million Canadians; the cards were used more than 2.4 billion times in 2002.[64] According to the Canadian Bankers Association, 40 per cent of Canadians use an Automated Banking Machine (ABM) as the primary means of conducting financial transactions.[65]

Canadians are the highest users of debit cards in the world, making 63.5 debit card transactions per person in 2000.[66] Indeed, Interac Association consumer tracking research in 2001 indicated that *Interac* Direct Payment has surpassed cash as Canadian's preferred way to pay.[67]

Perhaps not surprisingly, debit card fraud is growing. In December 2002, Montreal police reported $37 million in losses due to debit card fraud during 2002, a 25% increase over the previous year. (This was compared to app. $4.5 million in credit card fraud.)[68]

Debit card and ATM fraud can take a number of forms, all of which involve obtaining the consumer's card (or a clone thereof), discovering the applicable PIN, then using the card

---

[62] For example, where personal information is stolen directly from corporate, or government, databases.
[63] US PIRG Fact Sheet 11 April 2003; http://www.pirg.org/consumer/credit/fcrafacts2003new.htm
[64] www.interac.ca
[65] www.cba.ca. Data is July 2002.
[66] *Ibid.*
[67] www.interac.org. Note, however, that debit card use in pure dollar amounts is significantly lower than Canadians' use of credit cards.
[68] "Debit-card fraud ring broken up in Montreal", *The Globe and Mail*, Dec.4, 2002, p.A10.

to access the consumer's bank account.[69] Thieves withdraw money from ATMs using stolen cards, cards accidentally left in an ATM, or fraudulently manufactured cards. PINs are typically discovered by "shoulder-surfing" (observing the user inputting the number), via a hidden camera, or by thieves fraudulently posing as bank employees, and asking consumers to validate or change their PIN over the phone.

In one recent example, criminals used fake terminals to swipe debit cards (swiping them twice – once in the hidden fake terminal and then again in the real terminal) at gasoline stations and corner stores, while accomplices observed and memorized victims' PINs.[70] In another, thieves inserted a device into the card reader that unlocks the doors to ATM premises, and thereby recorded card information, while a pinhole camera hidden on top of the bank machine captured the user's PIN.[71] Cloned debit cards were then created using this information and used to drain money from victims' bank accounts via ATMs. In other cases, hidden video cameras were installed above the debit terminal, so as to film the customer punching in their PIN. Store employees are also known to have stolen debit card information from customers (often via small "card skimmer" devices). [72]

One technique, once the PIN is known, is for the thief to distract the consumer at the ATM by dropping a twenty-dollar bill on the floor and asking if it belongs to the consumer. As the consumer bends over to retrieve the bill, the thief switches her ATM card with somebody else's, then drains her bank account after she leaves. Another scam targets seniors: the thief jams the ATM machine, then offers the senior assistance in punching in their PIN number. Thieves usually tell a story of how this just happened to them and how they are willing to show the senior how to slowly punch in the PIN numbers to overcome this malfunctioning machine.[73]

In addition, thieves also create "bogus machines" where the PINs are recorded at a fake terminal, often in a business, and the financial transaction is not sent to the financial institution. The thieves then issue a fake transaction record, and later add cash to the store register to balance the business books. Later a fake card is reproduced from the recording of the magnetic strip and PIN from the bogus machine.[74]

Banking and debit card fraud is of more concern to consumers than credit card fraud, not only because it appears to be superseding the latter in quantity. Consumers also may be unaware that a thief may use a debit card to a daily maximum for withdrawals from ATMs and also for additional amounts at a point of sale. Depending upon the account

---

[69] See Industry Canada's excellent pages on debit card fraud at: http://strategis.ic.gc.ca/epic/internet/inoca-bc.nsf/vwGeneratedInterE/ca01832e.html.

[70] "BC is stung as debit-card criminals hit", *The Globe and Mail*, Dec.5, 2002, p.A7.

[71] "Thieves develop new debit scam", *The Ottawa Citizen*, Jan.12, 2003.

[72] "Card skimming involves copying of data off legitimate credit cards and debit cards onto counterfeit cards which can be used to buy goods": "ID theft targeted by top crime body" Australian IT News, September 30, 2003. (http://australianit.news.com.au/common/print/0,7208,7409481%5E15319%5E%5Enbv%5E15306,00.htm)

[73] See http://www.police.regina.sk.ca/FraudScam.htm .

[74] See description of bogus machine fraud at Industry Canada's website: http://strategis.ic.gc.ca/epic/internet/inoca-bc.nsf/vwGeneratedInterE/ca01834e.html.

being accessed, a thief may also be permitted to "deposit" a blank envelope to increase a balance and then withdraw additional funds.[75]

Recent research indicates that, unlike credit card users, debit card users are only slightly more likely to be reimbursed than to be found responsible for allegedly unauthorized debit card transactions.[76] Despite the adoption of a Code of Practice under which consumer liability for unauthorized debit card transactions is to be limited,[77] some financial institutions continue to hold consumers liable for losses resulting from circumstances beyond their control.[78]

Finally, it is worth noting that internal malfeasance at financial institutions is also a possibility with debit cards and bank accounts and one about which consumers can do little (besides be vigilant in regularly checking banking records). Recently, the Federal Privacy Commissioner dealt with such a complaint, namely that a financial institution had allowed an employee identity thief to gain access to a client's identity to make fraudulent transactions.[79] The Commissioner found the theft was a contravention the federal privacy legislation (PIPEDA).[80] However, the Commissioner concluded the bank could not be faulted for its employee's actions at a systemic level, as it had had adequate screening procedures for employees and had quickly identified the fraud and taken remedial action. However, the bank customer had actually uncovered the fraud himself.

Credit cards

At the end of 2001, 68.6 million credit cards were in circulation in Canada – almost three cards for every adult Canadian over the age of 18.[81] The number of VISA and MasterCard credit cards increased by 10 per cent in 2001 over 2000.[82] Not surprisingly, credit card fraud is the most common form of reported ID theft, making up 42 per cent of ID theft incidents. Interestingly, however, only a small proportion of credit cards are fraudulently used. In 2001 there were 44.1 million VISA and MasterCard credit cards in Canada, with a net retail volume of $121.8 billion. Only 118,138 cards (0.27%) were fraudulently used, while the amount of fraudulent accounts written-off was $142.3 million (0.17%).[83]

---

[75] See Industry Canada, "How much could you lose?" at http://strategis.ic.gc.ca/epic/internet/inoca-bc.nsf/vwGeneratedInterE/ca01837e.html.
[76] EKOS Research Associates Inc., "Evaluation of Operations related to the Canadian Code of Practice for Consumer Debit Card Services", submitted to the Electronic Funds Transfer Working Group (October 31, 2002); Highlights prepared by Office of Consumer Affairs, Industry Canada. ("Ekos Debit Card Study").
[77] See Canadian Code of Practice for Consumer Debit Card Services, at http://strategis.ic.gc.ca/epic/internet/inoca-bc.nsf/vwapj/Debit_Card_Code2.pdf/$FILE/Debit_Card_Code2.pdf.
[78] Ekos Debit Card Study, *supra.* Industry Canada's views on the interpretation and application of the Code to common debit card fraud events are found at: http://strategis.ic.gc.ca/epic/internet/inoca-bc.nsf/vwGeneratedInterE/ca01834e.html.
[79] Decision #121, available online at: http://www.canlii.org/ca/cas/pcc/2003/2003pcc10055.html.
[80] This case is discussed further, below.
[81] Financial Consumer Agency of Canada, *Credit Cards and You*, spring 2002.
[82] *Ibid.*
[83] Information provided to PIAC by Industry Canada.

VISA and MasterCard cardholders are currently protected from the financial risk associated with such ID theft through "zero liability" policies in the event of unauthorized use.[84] However, protection from liability for unauthorized credit card transactions does not resolve the problem for consumers. First, amounts written-off to fraud are indirectly recovered from consumers through high interest rates and other charges. Second, given that 22 per cent of victims reported more than one type of identity theft, fraudulently obtained credit cards may well play a role in other types of ID theft as well.

Easy credit

Easy credit is another factor contributing to ID theft. Unsolicited credit card offers – many of them pre-approved – flood Canadians' mailboxes every day. Financial institutions issue credit cards to students, send unsolicited credit card cheques to customers, and increase credit card limits without consumers' prior consent. Not only are pre-screened credit offers and unsolicited credit card cheques vulnerable to physical theft, imposters are able to obtain credit in other peoples' names far too easily. The virtual tidal wave of unsolicited credit card offers, particularly pre-screened or pre-approved offers has fed the ID theft problem. And unsolicited increases in credit card limits, without the consumer's consent, merely exacerbate the problem by raising the potential magnitude of fraud.

According to a recent survey of law enforcement officials in California by the California chapter of US PIRG (CALPIRG), "credit grantors" are singled out as too willing to extend credit without sufficient safeguards against fraud and identity theft.[85] The CALPIRG law enforcement survey lays primary responsibility for the creation of ID theft opportunities upon *credit issuers*. Credit agencies, banks, and other issuers of credit such as department stores and cell phone providers facilitate ID theft, and fail to cooperate with law enforcement officials in the investigation of alleged ID theft.[86]

Other studies cite the role of credit grantors in the growing problem of ID theft: a recent study conducted by Gartner Inc. noted that "financial services providers and others that extend credit to consumers, such as cell phone service operators or retail stores, often misclassify identity-theft crimes as credit losses". In a news release accompanying the Gartner survey results, it is emphasized that "banks and financial service providers must implement solutions that effectively screen for application fraud, so they don't wrongfully extend credit to identity thieves".[87]

---

[84] These policies are voluntary on the part of MasterCard and VISA, and therefore could change at any time. MasterCard will not hold cardholders liable for unauthorized purchases where their account is in good standing, where they exercised reasonable care in safeguarding their card, and where they have not reported two or more unauthorized events in the past 12 months. VISA's zero liability policy does not have any clear prerequisites, however liability may be imposed if the financial institution determines that the unauthorized transaction was caused by the gross negligence or fraudulent action of the cardholder.
[85] "Policing Privacy", *supra*. The first recommendation in this report is "Require credit issuers to adopt more fraud-proof practices". The second is "Make credit lenders pay for some of the trouble they cause."
[86] "Policing Privacy", *supra*.
[87] *Ibid.*

A more recent ID Analytics study of 200 million new U.S. credit card, chequing and cell phone accounts opened in 2001 "shows that 7 of 8 identity thefts are mis-categorized as simple credit losses."[88] The ID Analytics Report suggests that businesses were simply unaware of the extent of the problem. However, the Gartner report concluded that "the[se] industries …. do not have great incentive to fix the problem"[89] since the stock market would react negatively to large reported fraud losses. ID Analytics noted in their study that instant credit-granting institutions faced significantly higher rates of fraud than other lenders. "Any firm that offers fast credit approval is an easy mark for ID thieves . . . [w]e can't move away from instant credit but it is the enemy of good authenticity", stated the ID Analytics Report author when interviewed about the report.[90]

Online opportunities for theft and fraud

In the electronic marketplace, consumers are particularly exposed to identity theft and related fraud. Thieves now have much easier access to far more personal information about others than ever before. Moreover, they have access to far more ways in which to use that information fraudulently, to their advantage. According to the Federal Trade Commission:

> The Internet has dramatically altered the potential occurrence and impact of identity theft. First, the Internet provides access to identifying information through both illicit and legal means. The global publication of identifying details that previously were available only to a select few increases the potential for misuse of that information. Second, the ability of the identity thief to purchase goods and services from innumerable e-merchants expands the potential harm to the victim through numerous purchases. The explosion of financial services offered on-line, such as mortgages, credit cards, bank accounts and loans, provides a sense of anonymity to those potential identity thieves who would not risk committing identity theft in a face-to-face transaction.[91]

The growth of online banking and electronic commerce exemplifies the Internet's dramatic impact. Online banking in Canada doubled, from 8 per cent of financial transactions in 2000 to 16 per cent in 2002.[92] In the spring of 2002, 56 per cent of Canadians said they were very likely or somewhat likely to bank online in the next two to three years.[93] Yet, most of these consumers likely do not appreciate their exposure to risk of loss, or their liability, in the event of unauthorized online transactions.

---

[88] "Report: Lenders miss most ID theft" MSNBC News, September 22, 2003 (http://www.msnbc.com/news/970182.asp?0cv=BB10&cp1=1).
[89] "Identity Theft Fraud Prevention Solutions Start to Proliferate", Gartner Research Note: Markets, M-20-4466 (7 July 2003).
[90] "Report: Lenders miss most ID theft", *supra*.
[91] Quoted in United States General Accounting Office, *Identity Theft, Prevalence and Cost Appear to be Growing*, March 2002, p. 51.
[92] *The Canadian Marketing Pocket Book 2003*, World Advertising Research Centre, p. 42.
[93] *Ibid*.

Electronic commerce has been booming, despite consumer concerns about online fraud. According to Statistics Canada, companies received $10.4 billion in customer orders over the Internet in 2001, up 43 per cent from 2000.[94] VISA reported earlier this year that Canadians spent $772 million in 6.4 million online transactions during the 2002 Christmas season, up from $381 million a year earlier.[95] The US Census Bureau reported that retail electronic commerce sales for third quarter 2002 were $11.1 billion, up 34 per cent from third quarter 2001.[96] As opportunities for online ID theft and fraud increase, so does the likelihood of its incidence.

Easier access

Internet users may not appreciate the data trail that they leave on the Internet, through personal and professional websites, postings, registrations and use of Internet services. Personal information posted on unsecured websites is freely available to identity thieves as well as friends and colleagues. Indeed, a whole industry of online "data brokers" has emerged, offering to troll and mine the Internet for personal data on specified individuals. Depending on how exposed an individual has left herself online, a great deal of personal information can be gathered, without much effort.

With a little more effort, hackers are able to break into computer databases and obtain highly sensitive personal information such as credit card details. Without strong security measures, business and government databases are highly vulnerable to invasion by ID thieves. One fraudster recently admitted to purchasing credit card numbers from hackers on the Internet, and using them to purchase over $300,000 worth of computer equipment.[97] Gartner Group estimates that "through 2005, 20 percent of enterprises will experience a serious (beyond virus) Internet security incident", targeting either information or intellectual property.[98]

> With more than 600 million individuals worldwide now on the Internet, cybercriminals are taking advantage of users, enterprises and unsecured systems to usher in a new era of high-profit, low-overhead crimes, according to Gartner, Inc. [99]

More sophisticated hackers scour Internet cafes, libraries and other publicly available computer terminals to steal personal information unwittingly left by previous users, who do not clear the terminal's memory before leaving. In a reported case from Japan, hackers determined the passwords some people used to access their bank accounts online, apparently by using special software to identify the keystrokes inputted by previous users

---

[94] Statistics Canada, *The Daily*, April 2, 2002, www.statcan.ca
[95] "Canadians warm to online shopping", *The Ottawa Citizen*, January 14, 2003, p. D1.
[96] www.census.gov
[97] Jon Swartz, "Hackers evolve from pranksters into profiteers", *USA TODAY,* (March 16, 2003).
[98] *Gartner says that through 2005, 20 percent of enterprises will experience a serious Internet security incident"*, News Release (August 7, 2003).
[99] *Ibid.*, see: http://www4.gartner.com/5_about/press_releases/pr7aug2003b.jsp

of public computer terminals. They then withdrew large amounts of money from the accounts.[100]

More information

At the same time, identity thieves have more information about individuals available to them via the Internet than they ever had before electronic commerce. Personal information such as names, email addresses, physical addresses, phone numbers, and birth dates is readily available online. Other, more sensitive, data such as credit card and bank account numbers are stored in large computer databases that are vulnerable to hackers.

Online scams

Identity thieves are using the Internet in ever-more ingenious ways to obtain personal information from consumers. Spoofers posing as Internet auction or service providers, potential employers, credit card issuers, or other real commercial entities send e-mail to consumers with links to fake "phisher" websites, luring them to provide banking and credit card details for confirmation or other seemingly legitimate purposes.

In February 2003, the popular internet job site Monster.com acknowledged in an e-mail message to job seekers that "regrettably, from time to time, false job postings are listed online and used to illegally collect personal information from unsuspecting job seekers".[101] Resumes, of course, provide a gold mine of information for identity thieves.

In the same month, Sympatico, Canada's largest Internet service provider, warned its customers about a fake email requesting personal and financial information, including banking card and PIN numbers. The email asked people to complete an online form on a Web site that looked like Sympatico's Web site in order to correct an error in billing information.[102] Customers of Internet auction provider eBay and payment service provider PayPal have been subjected to similar e-mail scams in recent months. Bogus email messages that look like legitimate messages from the service provider are sent to customers, instructing them to enter their credit card and/or bank account numbers in an online form embedded in the email message, in order to avoid having their account terminated.

Another particularly ironic online scam involves phony "fraud alert" or "identity theft prevention" services. In the guise of offering such services, thieves obtain personal information such as SINs, credit and bank account numbers, driver's license numbers, and mother's maiden name.[103] In June 2003, customers of an online company called "Best Buy" received a fraudulent e-mail message entitled "Fraud Alert" from imposters of Best Buy, warning them of possible credit card misuse and urging them to go to a

---

[100] Jon Swartz, "Hackers evolve from pranksters into profiteers", *USA TODAY,* (March 16, 2003).
[101] "Monster.com warns about ID theft", *Wired News* (Feb.27, 2003)
[102] CBC News, February 25, 2003, www.cbc.ca.
[103] www.newyork.bbb.org/identitytheft/newscams.html

special website and enter their Social Security and credit card numbers in order to correct the problem.[104]

Sloppy information security (The "better late than never" file)

Lax business and government security

One of the leading contributors to ID theft is inadequate corporate and government information security, a situation over which consumers have little or no control. Identity thieves have taken advantage of careless waste practices, unnecessary disclosure of sensitive personal information on documents sent by mail, inadequately secured physical files and electronic databases, and inadequate screening or supervision of employees. Reported incidents abound, while no one knows the extent of unreported incidents.

In March 2003, Edmonton police shut down what they believed to be an organized ID theft operation, which had apparently gathered confidential bank and business records from trash bins outside banks and businesses.[105]

Thieves also go after hard drives containing confidential customer information. BC's Ministry of Human Resources warned 568 clients of potential ID theft after a computer server was stolen from its offices in March 2003. Earlier that year, a hard drive containing the private information of nearly one million Canadians was stolen from the Regina offices of ISM Canada, a data-processing company that handles confidential data for governments and corporations. The information on the hard-disk drive included names, addresses, bank account details, beneficiaries, social insurance numbers, pension values, pre-authorized chequing information and mothers' maiden names.[106] According to the *Toronto Star*, the data on the drive apparently was not encrypted or partitioned in a way that would protect the data from being copied.[107]

In December 2002, computer equipment containing sensitive personal information about more than 500,000 Americans, including their names, addresses, and Social Security numbers, was stolen from TriWest Healthcare Alliance. According to the president and CEO of TriWest:

> "Since the discovery of the theft, we have taken measures to reconfigure our systems and enhance our security. In addition, we have been working with federal personnel and a top private sector information security company to review all aspects of our physical and data security in an attempt to make sure that we understand all of the actions we should take to minimize the chance that such an event is repeated. … I hope that my colleagues in the business community will

[104] FTC, "Fraudulent Email Seeks to Capture Consumer Information" (June 24, 2003)
[105] "Police break up Identity-theft ring", Edmonton.cbc.ca (March 20, 2003).
[106] "Insurer unsure if Ottawa data at risk", *The Ottawa Citizen*, January 31, 2003, p. E1.
[107] *Ibid.*

take the time to learn about the risks that have come with the information age and what proactive steps need to be taken to protect your customers."[108]

Although consumers may take comfort that TriWest Healthcare Alliance eventually shut the barn door, they may wonder why their horses were not behind a closed door when the rustlers struck. And to add a little spice to consumers' anxiety, the company required two weeks after the theft to identify and notify the customers whose information had been stolen. Presumably the thieves did not need two weeks to use the information.

Finally, four computers were stolen from a Canada Customs and Revenue Agency office in Laval, Québec on September 4, 2003, in what may be "the biggest data loss since identity theft became an issue."[109] One computer was a portable server containing unencrypted information on 120,000 construction contractors and subcontractors. Information included names, dates of birth, home addresses and social insurance numbers – everything required for identity theft. The Revenue Minister has undertaken to contact all 120,000 persons and promised new social insurance numbers. Apparently the portable server was required to be left in a high security room overnight, but that the employee in charge simply neglected to lock it up.

These examples are just some of those that were reported to authorities and that received media coverage. It is not known how many more such thefts go unreported or unnoticed.

Sloppy corporate or government information practices are not restricted to poor physical security against break-ins.

- Earlier this year, the US federal prosecutors announced that an H&R Block office manager used customers' names, Social Security numbers, and dates of birth to steal their refund cheques, withdraw cash from their bank accounts and spend thousands of dollars with fake credit cards.[110]
- A University of Texas student hacked into the school's database and stole 55,000 Social Security numbers.[111]
- Eight million VISA, MasterCard and Amex customers were at risk after an intruder managed to access the data of a company that processes online credit card orders.[112]
- A medical assistant in Virginia was charged with five counts of identity fraud and theft earlier this year, for allegedly stealing patient information and using it to apply for hundreds of credit cards.[113]
- Another recently publicized case involved a computer help-desk employee with access to passwords from banks and credit companies. The employee allegedly downloaded credit card and bank account data from credit bureaus on 30,000 people

[108] Press statement, David J McIntyre, Jr., President and CEO, TriWest Healthcare Alliance (December 31, 2002) www.triwest.com.
[109] See "Theft threatens privacy of 120,000", *supra*.
[110] "Identity theft targeted H&R Block customers", *USA Today*, (January 3, 2003), www.usatoday.com.
[111] Jonathan Krim, "States seen as lax on database security", W*ashington Post* (March 26, 2003) p.E05.
[112] *Ibid.*
[113] W*ashington Post* (Feb.6, 2003)

over three years, and then sold that data to scam artists for $60 per name. As of December 2002, authorities had identified $2.7m.in losses as a result of this theft.[114]

- In July 2003, a con artist pleaded guilty to installing monitoring software in 14 different Kinko's stores in New York City, recording more than 450 private user names and passwords over several months, and then using this information to open and access online bank accounts.[115]

According to a December 2002 news report, law enforcement experts in the USA now estimate that half of all mass ID theft cases come from thefts of business databanks that are not properly safeguarded.[116] The article quotes an FTC official stating:

> "There is a shift by identity thieves from going after single individuals to going after a mass amount of information. There's an awful lot of bribery of insiders going on."[117]

Despite a law requiring that personal information be properly safeguarded,[118] Canadians are not immune to sloppy corporate information security practices. In the ISM Canada case reported above, an ISM Canada employee was charged with the theft.[119] The federal government recently acknowledged that one of its employees electronically stole personal data from about 200 Canadians, and may have passed the data on to another party. The government sent a letter to those affected, informing them that the information (which did not include tax or financial data) may have been disclosed to a third party.[120]

In early 2002, a few hundred consumers had their credit reports stolen after ordering them by mail from Equifax, one of the three national credit bureaus in Canada.[121] These reports include the individuals' full SIN. In this case, it was not clear whether the theft occurred before or after the mailings entered the postal system. Following this incident, Equifax stopped disclosing full SINs and credit card numbers on reports sent by mail to consumers.

Mail theft is recognized as one of the most common methods by which identity thieves obtain personal information. Canada Post requires that in-person requests for mail redirection be supported by two pieces of ID: one with a photo, and one with the current address and a signature. Despite this policy, thieves have succeeded in fraudulently redirecting mail and using the subsequently obtained personal information to obtain

---

[114] "Identity theft more often an inside job", *Washington Post* (Dec.3, 2002), p.A01
[115] "Hilo Web risks low", *Hawaii Tribune Herald* (August 5, 2003).
[116] "Identity theft more often an inside job", *Washington Post* (Dec.3, 2002), p.A01
[117] *Ibid.*
[118] The *Personal Information Protection and Electronic Documents Act* ("PIPEDA") applies to all federally regulated companies, and will extend to the provincial sphere that is not already subject to similar laws on January 1, 2004.
[119] "Exxon Valdez of data leaks may have happened", *Toronto Star*, February 17, 2003, www.thestar.com.
[120] Simon Tuck, "Mob role suggested in theft of SINs, other data", *Globe and Mail* (May 27, 2003), p.A4
[121] Maryanna Lewyckyj, "Crooks want to steal your identity", *Toronto Sun* (Feb.10, 2002); Ellen Roseman, "Identity thieves prey on slack mail security", *Toronto Star* (April 20, 2002).

credit and run up large bills.[122] In the reported case, the postal clerks in question may not have followed company policy.

In the summer of 2003, Canada Post began offering an online change of address service. Instead of an in-person ID check, a far more secure requirement if properly performed, the online service requires only a valid credit card, in addition to name and both old and new addresses. A written confirmation is sent by mail to the old address, within 10 business days of the request. The service is not available if the person requesting states that they will not have access to their old address during the next 10 business days.[123]

Lax consumer security

It is also true that some consumers do not take sufficient precautions to protect their personal information and to guard against ID theft. For example, consumers may disclose their banking card PINs to friends and family, or write their PINs and passwords down rather than committing them to memory. Many people continue to dispose of financial and other records containing sensitive personal information without first shredding or otherwise eliminating the personal information that could be abused by ID thieves.[124] Other consumers provide sensitive personal information in response to telephone calls and emails, without first confirming the legitimacy of the request.

This is a two-part problem, involving lack of consumer awareness as well as consumer carelessness. A recent study focused on debit cards, for example, indicates that 16% of Canadians are unaware of their liability for losses if they reveal their PIN to someone else. Only 21% understood that they could be liable for losses if their PIN was based on a number found in another document.[125]

In today's marketplace, consumers pay for goods and services with more than money. They also pay with valuable personal information – names, credit card numbers, SINs, and so on. The information is not only valuable to ID thieves – it is also valuable to merchants for marketing purposes. Consumers have an obligation in today's marketplace to inform themselves about personal information management just as they inform themselves about product quality, price, and safety.

However, improving consumer awareness of risks and responsibilities regarding ID theft involves an onus not just on consumers to inform themselves, but also on other parties bring this information to the attention of consumers. Clearly, better consumer education efforts by financial institutions, credit bureaus, governments and consumer groups would lead to better informed consumers about personal information practices. Businesses

---

[122] CBC Marketplace report (Feb.8, 2000). See www.cbc.ca/consumers/market/files/scams/idtheft/index2.html .

[123] See http://www.canadapost.ca/tools/mmm/bin/gettingstarted.asp?lang=en.

[124] CBC Marketplace reports finding a Canada Customs tax information package with names and social insurance numbers printed on the front, in the seventh blue box that they checked in a Mississauga neighbourhood. See above, FN 81.

[125] EKOS Research Associates Inc., *Evaluation of Operations related to the Canadian Code of Practice for Consumer Debit Card services*: *Highlights* (Office of Consumer Affairs, Industry Canada; Oct.31, 2002).

engaging in commercial practices that expose consumers to ID theft - and especially those who promote services that put consumers at risk (e.g., debit cards, unsolicited credit, online sharing of personal information) - have a particular responsibility in this regard.

Function creep gets creepy

Allowing personal identity documents and numbers to be used by multiple parties for multiple purposes also increases the risk of identity theft.

Social Insurance Number use and abuse

One of the most valuable identifiers for ID thieves is the government-issued Social Insurance Number (SIN). Each SIN provides a unique identifier for that individual – which is what makes it so valuable for both legitimate businesses and ID thieves. As the Privacy Commissioner of Canada states, "Your SIN can be used to steal your identity."[126]

The Social Insurance Number was created in 1964 to serve as a client account number for the administration of the Canada Pension Plan and employment insurance programs. In 1967 Canada Customs and Revenue Agency started using the SIN for tax reporting purposes. Canadians must provide their SIN to Government of Canada departments or agencies, their employers, and anyone who prepares income tax information on their behalf – for example, interest income.

However, SINs are commonly requested in order to authenticate consumer identity or to check a consumer's credit rating. Because it is a unique identifier, the SIN is perceived as offering more accuracy than other identifiers, and is thus favoured as a file identifier by many organizations that manage personal information, including credit bureaus. As more businesses collect and use SINs for data management purposes, the more likely it is that SINs could be used to find and match information from one database to another.

While provision of SINs to companies and agencies not specifically entitled to collect them is optional on the part of the consumer, credit bureaus and other companies still routinely request this information from consumers. This practice feeds into the ID theft problem by exposing SINs to potential ID theft. At worst, SINs may be openly disclosed on consumer credit reports or other documentation and thus vulnerable to mail and other forms of theft.[127] At best, SINs are truncated or omitted from documents sent outside the company, in which case they are still subject to theft by insiders.[128]

This problem is compounded when the same companies rely upon SINs to authenticate consumer identity: the more vulnerable SINs are to theft, the more likely it is that an

[126] Fact Sheet, Social Insurance Number, Privacy Commissioner of Canada, www.privcom.gc.ca
[127] Equifax ceased this practice in 2002, after suffering an ID theft incident involving mailed consumer reports with full SINs disclosed. Consumer SINs are disclosed only to businesses who provided those SINs to the credit bureau. (Conversation with Equifax representative, July 16, 2003).
[128] Equifax notes that SINs can in fact be an effective tool in the fight against fraud. See discussion with Northern Credit Bureaus, below.

imposter will have a consumer's SIN, and will therefore be more able to defeat the authentication process.

Credit bureaus take the opposite position, namely, that providing SINs to credit bureaus could greatly reduce identity theft. SINs are presently the sole unique identifier available to credit bureaus, states Richard Huot of Northern Credit Bureaus Inc., the third national Canadian credit reporting service.[129] In fact, he states, consumers who choose to decline giving a credit bureau access to their SINs may be compounding the likelihood of fraud, since consumers are impeding verification of other crucial information against SINs, and vice versa. Given the frequency of address changes in the Canadian population, and the frequency of identical names, credit bureaus need the SIN number to cross-reference the other information for accuracy, claims Huot. He also notes frequent transposition by banks and other credit grantors of personal information (such as birth dates or SINs) when individuals and their spouses make joint applications for credit (such as for a "spouse card" on a credit card account).[130] Ultimately, the cost of identity theft, as well as finding simple mistakes in, and fixing the credit records of individuals, is borne by consumers. At present, credit bureaus pass on their authentication expenses in the form of higher credit check costs. Finally, Huot notes, the credit bureaus would be content with a different unique identifier than a SIN – one more secure and less open to abuse – but only one that was widely accepted by credit grantors and other clients.

It is difficult to gauge this claim, however, it appears quite plausible that without a unique identifier of come sort, ID thieves are more likely to be able to direct credit information to a bogus address – at least for the time necessary to undertake serious fraud. The difficulty with using SINs for such unique identifiers is that they presently provide access to so many government services.

In 1998, the Auditor General of Canada stated that the SIN had become a "de facto national identifier for income-related transactions, contrary to the government's intent", noting that:

> "Existing SIN application procedures are insufficient to guard against fraud and abuse. … Minimal effort is dedicated to investigations of SIN fraud and abuse, and penalties are minimal, with no real impact on deterrence."[131]

[129] Telephone conversation with Richard Huot, Northern Credit Bureaus Inc., September 25, 2003.
[130] Huot also suggests credit bureaus be provided lists of SINs of recently deceased persons on a regular basis by governments, so that credit bureaus may freeze these reports. (Thieves often troll obituaries in local newspapers for potential identities).
[131] 1998 Report of the Auditor General of Canada, chapter 16, www.oag-bvg.gc.ca.

Types of SIN Abuse

Federal, Provincial and Municipal Social Programs

- Obtaining benefits from Canada Pension Plan, Quebec Pension Plan, Employment Insurance and social assistance using different names or while working under another identity.
- Using many identities to collect Old Age Security cheques.
- Fabricating a new identity and obtaining a student loan.
- Obtaining credit for grants or sales tax credits using different names.
- Obtaining many health cards.

Federal and Provincial Income Tax

- Splitting income or obtaining various tax credits by using several names.
- Using many identities to hide investment income.

Work Permits and Licenses

- Obtaining work permits using different names.
- Obtaining a replacement driver's license under a different identity.

Commercial Activities

- Obtaining many credit cards or many lines of credit using different names, and disappearing once the maximum credit limit on all of them has been reached.
- Securing loans in banks using faked identification and subsequently disappearing.
- Making term deposits using different names.
- Renting luxury cars with the intent of selling them in foreign countries and subsequently disappearing under a new identity.

Source: 1998 Report of the Auditor General of Canada, Chapter 16.

According to the Auditor General's 1998 report, there were about 3.8 million more active SINs than the size of the population aged 20 or over.[132] The 2000 Auditor General's report noted that this gap had been reduced to 800,000 SINs and that the government had increased the number of investigations of SIN fraud and abuse.[133] However, not everyone is impressed. Ken Rubin, a researcher and expert on access to government information, had this to say in June 2002:

> "….despite millions of dollars being spent on these investigations over the last three years, there have been fewer that 45 prosecutions for SIN card misuse. SIN administrators acknowledge they lack the resources to weed out all the problems associated with the misuse of the SIN card. They also know that people wanting to steal and use cards fraudulently are usually one step ahead of the authorities."[134]

While no law prevents businesses from asking for consumers' SINs, the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) offers some solace. Until December 31, 2003, the Act applies only to the personal information of clients and

[132] *Ibid.*
[133] 2000 Report of the Auditor General of Canada, chapter 33, www.oag-bvg.gc.ca.
[134] "SIN numbers threaten Canadians' rights", Windsor Star, June 18,2002, p. A8.

employees in the federally regulated private sector. On January 1, 2004, the law will extend to every organization that collects, uses or discloses personal information in the course of a commercial activity within a province, whether or not the organization is a federally regulated business. The federal government may exempt organizations and/or activities in provinces that have adopted privacy legislation that is similar to the federal law.

According to the Privacy Commissioner of Canada:

> "Under the new law, organizations like banks, telecommunications companies and airlines cannot require you to consent to the collection, use or disclosure of your personal information unless it is required for a specific and legitimate purpose.
>
> "This means that unless an organization can demonstrate that your SIN is required by law, or that no alternative identifier would suffice to complete the transaction, you cannot be denied a product or service on the grounds of your refusal to provide your SIN.
>
> "If you disagree with a commercial organization's request for your SIN, you can complain to the Privacy Commissioner of Canada, who will investigate the complaint."[135]

Even so, consumers may find that they get faster or better service when they provide their SIN to companies who have no statutory right to collect it. For example, CIBC VISA cardholders seeking online access to their account, who cannot remember their password, are asked to provide a variety of personal information for authentication purposes, including – on an optional basis – SIN and Drivers' Licence numbers. Attempts by a PIAC researcher to use this service without giving her SIN or Driver's Licence number failed, and bank personnel confirmed that this problem was widespread.

Other government-issued identifiers

While SINs are the most valuable personal identifier, other personal identifiers are also subject to "function creep" by governments and the private sector. As noted above, drivers' licence numbers are being used by at least one financial institution for authentication purposes.

In the USA, driver's licenses have been partially protected from abuse by federal legislation: the *Driver Privacy Protection Act* makes it unlawful (subject to some exceptions) to disclose or obtain personal information from a motor vehicle record unless the subject expressly consents to such disclosure. However, the state of Florida authorizes the sale of this information to private sector businesses. During the 2001-2002 fiscal year, the state collected about US$27m. from the sale of these records to a number of corporations, including providers of "identification and credential verification services". Two class action lawsuits have been filed in Florida, alleging that two of the largest

[135] *Ibid.*

information brokers in the USA have invaded the privacy of millions of Florida motorists by obtaining and reselling personal data from motor vehicle records in that state.[136]

Moreover, this legislation does not prohibit merchants from requiring that customers provide driver's license information on cheques, a common practice in the marketplace. Hence, the data remains vulnerable to abuse.[137]

Use of consumer data for unsolicited marketing purposes

In the private sector, consumer information is widely used and shared for the purposes of unsolicited marketing, sometimes with the consumer's knowledge and consent, but often without meaningful consent. Companies routinely use data collected from their existing customers to market additional products or services to those customers – for example, unsolicited pre-approved credit or "convenience cheques" sent by credit card companies to their cardholders (and past cardholders). Companies also share such data with their affiliates so that the affiliates can engage in direct target marketing. Customer data is also shared with third parties for marketing purposes. For example, credit bureaus permit companies to monitor and update client information "prior to making a promotional offering".[138]

There is, indeed, a whole industry now of consumer profiling, data sharing, and direct marketing. These practices feed into the ID theft problem in a number of ways, including by exposing sensitive personal information to more people and thus making it more vulnerable to theft, as well as by sending mailings that contain sensitive personal information.

Legislative limits on function creep

As noted above, Canada has broadly applicable data protection legislation that restricts the right of private sector companies to collect, use and disclose personal information. The PIPEDA addresses the problem of "function creep" by requiring that organizations in the private sector obtain the individual's knowledge and consent before using or disclosing personal information for a purpose not originally consented to.

However, the Act's provisions regarding notification are not particularly strong; they state only that "Organizations shall make *a reasonable effort* to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed."[139] (emphasis added). Individuals may therefore be unaware of new purposes for which their personal information is being used, and may thus have no opportunity to refuse consent to such new uses.

---

[136] Dan Christensen, "Major Information Brokers face class action for invasion of privacy" *Miami Daily Business Review* (June 24,2003)
[137] Comment from Beth Givens, Privacy Rights Clearinghouse (August 2003).
[138] Angie Barrados, *Consumer Reporting and Privacy: The Need for Better Protection* (PIAC, Nov.2000), p. 49.
[139] s.4.3.2, Schedule 1.

The PIPEDA is also unfortunately weak in respect of demands by companies for personal information that is not necessary for the requested service or transaction. It states:

> "An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use or disclosure of information beyond that required to fulfil the *explicitly specified, and legitimate* purposes."[140] (emphasis added)

In other words, the purposes in question need not be *necessary* for the requested service or transaction; they need only be "explicitly specified and legitimate". Hence, consumers may be denied access to a product or service if they refuse to provide personal information that is not actually <u>needed</u> for the transaction.[141]

In practice, organizations typically obtain consent through clauses in detailed contracts or terms of service, which consumers are not required to read and which are rarely brought to the consumer's attention in an effective manner. Moreover, businesses often require consumers to consent to non-essential uses as a condition of supply. Where consumers are given a choice, it is almost always via negative option, such that their consent to the information collection, use or disclosure is assumed, even where the consumer is unaware.

Research indicates that most consumers are in fact not aware of the data collection, use and disclosure to which they are agreeing when they purchase products and services.[142] Hence, the effectiveness of this legislation in reducing function creep, and other practices that facilitate ID theft, is unclear.

Another relatively weak aspect of the PIPEDA involves proper destruction of records. Principle 5 of the PIPEDA requires that personal information "be retained only as long as necessary for the fulfilment of [the specified] purposes". However, s.4.5.3 states only that "personal information that is no longer required to fulfil the identified purposes *should* be destroyed, erased or made anonymous" (emphasis added).

---

[140] s.4.3.3, Schedule 1.

[141] The Office of the Privacy Commissioner of Canada disputes this interpretation and contends that PIPEDA's "reasonable person" test effectively limits the types of information a business may collect in order to provide goods or services. In effect, the OPCC argues that the combination of the "explicit and legitimate purposes" requirement, when viewed through the lens of the reasonable person test, effectively requires businesses only to collect information strictly necessary to the transaction. This assumes, of course, that reasonableness will always be viewed by the OPCC as equating bare necessity, and assumes there will be effective monitoring of these practices by complaints brought before the OPCC.

[142] EKOS Research Associates Inc., *Business Usage of Consumer Information for Direct Marketing: What the Public Thinks* (August 2001), accessible via http://www.piac.ca/privacy.htm . This survey showed that over half (54%) of those participating in loyalty programs were unaware of the fact that many of these programs collect, use and disclose information about their purchasing habits in order that companies can target them with new products and services.

In contrast, California has enacted a "shredding law", which requires that businesses shred, erase, or otherwise destroy records containing personal information upon disposal.[143] It is not clear why the Canadian law is voluntary in this respect.

The federal government and most provinces also have legislation governing public sector treatment of personal information. These statutes impose obligations on government departments and agencies to respect the privacy rights of Canadians by placing limits on the collection, use and disclosure of personal information.[144]

Inadequate consumer control over trade in credit information

ID theft victims often discover that something is wrong when they are denied a financial or other service because of poor credit rating. At this point in time, damage has been already done. Once ID thieves have the information they need, they proceed to spend the victim's money, run up bills, and ruin their credit rating. Central to this problem are the agencies that traffic in consumer credit information: credit bureaus.

Credit bureaus in the USA are criticized by CALPIRG for allowing a poorly-screened audience of third parties to buy credit reports, and for permitting credit reports to be issued to ID thieves on minimal information (two or three easily ascertained "points of correspondence" such as name, address and employer name).[145] CALPIRG's report also suggests that a high level of inaccuracies in credit reports may make it easier for ID thieves to operate by permitting them to access reports on dated, incorrect, or partial information. The CALPIRG report also criticizes other practices surrounding credit bureaus such as improper handling of "fraud alerts" on their reports (for example, providing a credit "score" to a creditor who only asks for the raw "score" without an accompanying fraud alert notice, even if the fraud alert is on the actual credit report).

Both Equifax (Canada) and TransUnion (Canada) dispute these charges, noting that there are no Canadian studies establishing similar problems in Canada. TransUnion specifically cites its anti-fraud measures and notes that it offers a line of fraud products to its customers to curtail fraud, including identity theft (Equifax has similar fraud measures and anti-fraud products). TransUnion also notes that creditors seeking a credit report "have to meet extensive membership procedures" in order to be authorized to receive reports.[146] Equifax (Canada) argues that "as much as 40% of ID theft in the US is done by

---

[143] California Civil Code, 1798.80-82

[144] See the federal *Privacy Act*, and provincial legislation such as Ontario's *Freedom of Information and Protection of Privacy Act* (a list of the relevant provincial statutes is accessible at http://www.privcom.gc.ca/information/comms_e.asp). A review of the effectiveness of these legislative instruments is beyond the scope of this paper, but could be considered in connection with an audit of government identification information practices.

[145] CALPIRG, Nowhere to Turn: Victims Speak Out on Identity Theft, May 1, 2000 (http://www.calpirg.org/consumer/privacy/idtheft2000/idtheft2000.pdf) at pp. 12-14.

[146] Letter from Trans Union of Canada, Inc., op. cit., p. 2. Most provincial credit reporting acts also limit the classes of persons to whom credit reports may be issued (although the lists may be quite generous – for example, the Ontario *Consumer Reporting Act*, s. 8 includes a category of persons with "direct business need for the information").

family members or close associates" and "[t]here is no evidence to show that credit-reporting agencies are the source of any significant incidents of ID theft."[147]

PhoneBusters receives virtually no complaints regarding ID theft *originating* with credit bureaus. However, Detective Staff Sergeant Elliot acknowledges that credit bureaus' reluctance to implement more aggressive fraud alerting procedures on Canadian credit reports may contribute to the problem.[148]

In Canada, credit bureaus are regulated provincially. Every province but New Brunswick has legislation governing the provision of what are known as "consumer reporting services".[149] While not harmonized, these statutes offer roughly similar protections against unauthorized access to credit information. In Ontario, such protections include:

- a requirement for "reasonable efforts to corroborate" unfavourable personal information before reporting it,[150]
- a prohibition against requesting or obtaining a credit report without first giving written notice to the consumer;[151]
- a prohibition against divulging personal information to a credit bureau or other credit grantors without consumer consent, unless written notice is given to the consumer at the time of the application for credit;[152]
- limits on the right of parties to obtain individual names from a credit bureau based on criteria submitted, and obligations on credit bureaus to notify individual consumers prior to providing such information to third parties;[153]
- the right of consumers to obtain a copy of their credit report in plain language at no charge;[154] and
- obligations of credit reporting agencies to investigate consumer claims of inaccuracies, correct erroneous information, and report such corrections to anyone who was provided with the consumer's credit report during a specified period. [155]

Despite all these rules, consumers are still largely unaware of the extent to which their credit information is being shared, with whom it is being shared, and for what purposes. As noted in a 2000 PIAC report,

---

[147] Equifax Canada representative; August 2003. Citing FTC data, Gartner Inc. reports that over half of all ID theft in the USA is committed by criminals who have established relationships with their victims – such as family members, roommates, neighbours, or co-workers: Gartner news release (July 21, 2003).
[148] Telephone interview with Detective Staff Sergeant Barry Elliott (September 23, 2003). One of the credit bureaus' stated concerns is placing fraud alerts on credit reports after being informed of fraud potential by authorities but before the credit bureau has been able to contact the consumer for consent. This can be viewed as a violation of the PIPEDA.
[149] E.g., Ontario's *Consumer Reporting Act*, R.S.O.1190 c.C.33.
[150] subs.9(3)(b).
[151] subs.10(2).
[152] subs.10(5).
[153] s. 11.
[154] s. 12;
[155] s. 13. In Ontario, PEI, Nova Scotia and Manitoba, the period is the last 2 months; in Alberta, the last 6 months; in B.C., Saskatchewan and Newfoundland, the last 12 months.

> "The consent clauses currently in use in credit contracts rarely provide enough information to constitute meaningful consent by consumers to having their information shared through the credit reporting system. They do not explain how information will be used and by whom, nor do they give consumers any control over how their information is used, even after the consumer is no longer a customer of the creditor."[156]

This does not appear to have changed significantly since 2000; consent clauses used in credit contracts remain, in large part, broad and unspecific.

Moreover, consumers are typically not informed at the time that unfavourable credit information is placed on their file. It is unclear what efforts, if any, credit bureaus make to corroborate such information, even where required by law.[157] And there is no requirement for credit bureaus to obtain proof of customer consent before releasing personal information to third parties. Nor are credit bureaus required to notify consumers of possible fraudulent activity when, for example, numerous credit applications are submitted within a short time period. The onus is instead on consumers to review their credit reports periodically in order to check for fraudulent activity.[158]

Creditors typically notify consumers of their intention to review credit reports, or to divulge information to credit bureaus, in credit application forms. Hence, consumers are not notified at the time that credit is granted in their name to ID thieves. Creditors are not even required to take note of fraud alerts placed on consumer reports. Nor are they required to ensure that all personal information in a credit application matches that in the credit file, before proceeding to grant credit.

Clearly, much can be done to improve practices in this area with a view to reducing the extent of ID theft and the magnitude of financial harm caused by it.

Weak law enforcement

A further factor underlying the current ID theft problem is ineffective deterrence. The Canadian *Criminal Code* includes several provisions relating to identity theft, including:

- fraud (s. 380)
- obtaining credit by a false pretence or by fraud, and knowingly making a false statement with intent that it be relied upon, for the purpose of procuring the delivery of property, the payment of money, the making of a loan, the grant or extension of credit, etc. (s. 362)

---

[156] Angie Barrados, PIAC, *op cit,* p.50.

[157] Investigations are apparently conducted upon request by consumers, but not otherwise – unless, of course, the receipt of unfavourable credit information coincides with other evidence of fraud.

[158] As a matter of practice, credit bureaus do notify all potentially affected consumers when they become aware of a possible fraud. Equifax, TransUnion and Northern have special units devoted to combating fraud. However, the credit bureaus are presently discussing preventative notification, due to concerns about the impact of the possible impact of the PIPEDA (source: Telephone interview with Det. Sgt. Barry Elliott (September 23, 2003).

- forgery (ss. 366-378)
- theft, forgery, etc., of credit card (s. 342)
- if done with intent to defraud, the making, executing, drawing, signing, accepting or endorsing of a document in the name or on the account of another person (s.374)
- forgery of or uttering forged passport (s. 57)
- personation with intent (s. 403)
- unauthorized use of computer (s. 342.1)

However, most of these *Criminal Code* offences require proof of the accused's intent to gain advantage by means of the fraud. In other words, mere possession of multiple identity documents is not a crime in and of itself. The fraud must also involve intent to gain some advantage or cause some disadvantage to others. (Exceptions include forgery of a passport (subs. 57(1)) and theft of a credit card (subs. 342(1)) – in these cases, the mere forgery or theft is a crime.) Yet, it can be difficult to prove intent; police may catch an ID thief in possession of multiple identification documents or information belonging to others, yet be unable to prove that the accused used or intended to use this information to his advantage.

Most of the ID theft-related offences are "hybrid offences", meaning that they can be treated by the Crown as indictable or summary depending on the gravity of the case, but some are indictable offences only.[159] If treated as indictable, most carry a maximum prison term of ten years.[160] However, anecdotal evidence suggests that actual sentences for ID theft convictions are much lower – so low as to deter police from spending the time and effort necessary to secure convictions.[161]

In addition to the *Criminal Code* are numerous other federal statutes creating offences for improper use or disclosure of specific types of information. These offences carry a range of penalties: fines, imprisonment or both. For example,

The *Employment Insurance Act* makes it an offence to:
- knowingly apply for more than one SIN;
- use someone else's number to deceive and defraud;
- loan or sell a SIN or a SIN card to deceive or defraud;
- or, manufacture a SIN card.

The penalty for any of these offenses is a fine of up to $1,000, imprisonment for up to one year, or both.[162]

---

[159] Indictable offences are considered more serious than offences punishable on summary conviction, carrying heavier sentences and involving more elaborate processes. Where the offence can be classified as either indictable or summary, it is up to the Crown to elect which way to proceed. The following offences are indictable offences only: ss. 57; 58; 362(b),(c),(d); 374; 375. The remaining offences identified above can be treated as indictable or summary, depending on the severity of the case in question.

[160] Sections 57 and 374 carry maximum prison terms of 14 years.

[161] Email communication with Brent Grover, Corporate Information and Privacy Advisor, Ministry of Management Services, Government of British Columbia.

[162] Source: www.hrdc-drhc.gc.ca. However, there are few prosecutions under these sections.

The issue is also addressed by a patchwork of provincial offences:

- under the Ontario *Consumer Reporting Act*, every person who (a) knowingly, furnishes false information in any application under this Act or in any statement or return required to be furnished under this Act or the regulations; (b) fails to comply with any order, direction or other requirement made under this Act; or (c) contravenes any provision of this Act or the regulations, is guilty of an offence;[163]
- under the Ontario *Mortgage Brokers Act*, every person who, knowingly furnishes false information in any application, statement or return required under the Act is guilty of an offence;[164]
- under the Ontario *Vital Statistics Act*, it is an offence to wilfully make or cause to be made a false statement in any documentation required under the Act;[165]
- under the Nova Scotia *Vital Statistics Act*, it is an offence to obtain or attempt to obtain a birth certificate or a copy of the registration of a birth for fraudulent or other improper purpose;[166]
- under the Ontario *Health Cards and Numbers Control Act*, it is an offence to collect or use another person's health card number;[167]
- under the Ontario *Freedom of Information and Protection of Privacy Act,*[168] it is an offence for government officials to wilfully disclose personal information in contravention of the Act, or to willfully maintain a personal information bank in contravention of the Act.

Despite these legislative tools, the incidence of ID theft in Canada appears, as elsewhere, to be growing. Clearly the legal regime is designed to address individual facets of ID theft but not respond to the activity in a specific manner. Law enforcement officials cite a number of challenges, including lack of an offence for simple possession of false or multiple identification, the expense of ID theft investigations, the inter-jurisdictional nature of many ID theft cases, and the need for inter-agency information sharing and co-operation.[169] Clearly, resources are another issue: according to one expert, identity thieves have $10 to spend for every $1 that law enforcement agencies and other fraud investigators have.[170]

Suggestions from law enforcement officials include:

- creation of a new offence for simple possession of multiple identification;[171]

[163] R.S.O. 1990, c. C.33, s. 23 (1).
[164] R.S.O. 1990, c. M.39, s. 31
[165] S.O. 2001, c. 21, s. 14, s.56.
[166] R.S., c.494, s. 1. s.49A.
[167] S.O. 1991, c. 1, s. 3 (1).
[168] R.S.O. 1990, c.F.31, s.61.
[169] Detective Joe Pendleton, Edmonton Police Force, presentation to Privacy and Security Conference, February 13-14, 2003, Victoria, BC Canada.
[170] Conversation between Kathleen Priestman and Sonja Schindeler, VP, Product Development, Trans Union of Canada, Inc. (July 10, 2002)
[171] Telephone conversation with Dave Jeggo, Supt., Economic Crimes Branch, RCMP (8 July 2003), Bernie Murphy, Ontario Provincial Police (9 July 2003).

- national coordination of ID theft investigations;
- increased dialogue among various law enforcement agencies, both nationally and internationally;
- more aggressive investigation and prosecution of ID theft cases; and
- sentencing that is designed to deter ID theft.[172]

MEASURES DESIGNED TO PREVENT ID THEFT

In addition to the legislation cited above, governments and businesses in Canada and the USA have implemented some notable measures with a view to preventing ID theft. Some of these are discussed below.

Criminalization of mere identity theft

One of the six most common recommendations made by Californian police officers recently surveyed by CALPIRG on the issue of ID theft was that mere trafficking in personal information, without intent to use it for any particular purpose, should be made an offence.[173] Indiana's recently passed ID theft legislation criminalizes the possession of false identification so as to provide, in part, that a person who: "knowingly or intentionally obtains, possesses, transfers, or uses the identifying information of another person . . .without the other person's consent; and . . . with intent to: **(A) harm or defraud another person; (B) assume another person's identity; or (C) profess to be another person;** commits identity deception, a Class D felony."[174] Interestingly, the law exempts attempts by minors to obtain alcohol and other "adult" products, no doubt to avoid prosecutions for all but the hard core ID fraudsters. The perpetrator may be charged even before any actual loss to victims.

Law enforcement and government officials in Canada are currently working on a proposal to revise the *Criminal Code* so as to make simple possession of multiple identity – without the need to prove intent – a crime.[175]

Inter-jurisdictional cooperation and training of law enforcement officials

Strong laws are of little use if law enforcement agencies do not have the tools and resources to use them. Not only do police need adequate staff to pursue what are often

---

[172] Detective Joe Pendleton, *Ibid.*

[173] Jennette Gayer, "Policing Privacy: Law Enforcement's Response to Identity Theft", CALPIRG (May 2003).

[174] Enrolled Senate Bill 0320, First Regular Session 113th General Assembly (2003) (http://www.in.gov/legislative/bills/2003/SE/SE0320.1.html)

175 Interview with Superintendent Dave Jeggo, Economic Crime Branch, RCMP (July 16, 2003). The Canadian Association of Chiefs of Police have endorsed creating this new offence and have suggested the following wording: ""Everyone commits an offence who, for an unlawful purpose and without colour of right, has in his possession, uses or deals in any way with personal identity information". (Res. 2002-02).

very time-consuming cases, they also need to be able to cooperate efficiently with their colleagues in other jurisdictions.[176]

In the US, the FTC assists in criminal law enforcement and alerts state Attorneys General to the FTC resources, emphasizing how they can be used to assist state residents who are ID theft victims. Together with other agencies, the FTC conducts ID theft training local law enforcement officers across the country. It maintains a centralized database of victim complaints that is made available to law enforcement agencies nationwide.

Requirements for obtaining government-issued ID documents

Recognizing the problem of ID theft, governments are taking measures to limit the issuance of identity documents based on fraudulent applications. As noted above, the federal government has recently tried to crack down on SIN abuse. For all SIN requests (first-time, replacement, amendment, corrections, etc.), applicants must now provide an original document proving their identity and status in Canada (e.g., birth certificate or permanent resident card). They must also provide an original supporting document (e.g., marriage certificate) if the name on the primary document is different from that on the application form.

The requirements for obtaining passports in Canada have been made more strict since 2001. As in the past, passport applications and accompanying photos must be certified by a guarantor. An original proof of Canadian citizenship must also be provided. At least one other document with the applicant's current name and signature, such as a driver's license, a provincial health care card, an old age security card, is also required. If not an original, then the copy must also be certified by the guarantor.

Birth certificates are issued by provinces; each province has its own requirements. In 2002, Ontario implemented new rules designed to protect the integrity of birth certificates. Under the *Vital Statistics Statute Law Amendment Act (Security of Documents), 2001*:

- Ontarians are required to report lost, stolen or destroyed birth certificates;
- Lost, stolen, found or destroyed birth certificates will be deactivated;
- Information on deactivated documents will be shared with other government programs, including the federal passport office;
- Fines for willfully providing false information when applying for vital statistics documents were significantly increased; and
- Only one birth certificate will be issued at a time for any individual.

[176] Promisingly, the OECD recently announced its approval of "OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders" which will promote enhanced cooperation of consumer protection agencies to combat fraudulent activities, such as ID theft, across borders. See Industry Canada news release at http://strategis.ic.gc.ca/epic/internet/incb-bc.nsf/vwGeneratedInterE/ct02581e.html and OECD Guidelines at: http://www1.oecd.org/publications/e-book/9303063E.PDF.

Coincident with these legislative changes, the Ontario government launched a public campaign in 2002 to educate consumers about identity theft and to encourage preventative practices.[177]

Prompt disclosure of security breaches

Corporate and government databases are increasingly becoming the target of ID theft, whether by employees, outside thieves, or hackers. In order that affected consumers can take measures to limit the ability of ID thieves to misuse their personal information, it is essential that they be notified of the breach immediately. Yet, companies are reluctant to report such breaches because of the bad publicity it will entail.

California therefore now requires companies (both for-profit and non-profit) that store data electronically and conduct business in that state, as well as state government agencies to warn customers of security breaches in their computer networks.[178] Such companies and agencies must alert customers whenever "unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person". "Personal information" is defined as first name or initial and last name, with one of the following: Social Security number, driver's license number, state identification number, or credit or debit card number and security code. Companies must notify customers "in the most expedient time possible" by email or regular mail. Where 500,000 or more customers are affected, or notification would cost more than US$250,000, notification is permitted via a conspicuous website posting and media advisory.

A federal bill modeled on the California law was introduced in June 2003 by Senator Dianne Feinstein.[179] The "Notification of Risk to Personal Data Act" would require organizations to notify individuals promptly of any computer security breach that involves unauthorized access to sensitive personal information such as social security numbers or credit cards. Notification would be accomplished by letter or electronic mail. Where that is either impossible or too costly, media notification and website postings would be required. Failure to notify could result in fines of up to $25,000 per day.[180]

Finally, another federal bill, the "Identity Theft Notification and Credit Reporting Act of 2003" (Senate Bill 1633 IS) (Corzine), was introduced September 17, 2003 and takes a more focussed approach. The bill requires all financial institutions to notify all customers of personal information breaches. It also requires all financial institutions to automatically notify credit bureaus and law enforcement agencies, in accordance with FTC rules to be drafted. Each credit bureau must place a fraud alert on each file affected.

---

[177] http://www.cbs.gov.on.ca/mcbs/english/576LWL.htm

[178] California Senate Bill 1386; (now codified as California Civil Code §§1798.25-1798.29 and §§1798.80-1798.84). Effective July 1, 2003. See also "New California law forces companies to disclose hacking", SiliconValley.com (June 23, 2003). Note that consumers may bring a civil action for any breach of the law (in addition to other penalties that may be applied to the company). California Civil Code, §1798.84.

[179] Senate Bill 1350.

[180] Ryan Singel, "Bill to Force Data Theft Notices", *WIRED News* (June 27, 2003)

(Consumers are notified of the disclosure to credit bureaus and law enforcement agencies in their notification.) Fraud alerts are defined by this Bill, which requires that the fraud alert be provided to all credit grantors, notwithstanding the form of the credit report (including summary reports or bare credit scores). Credit is not permitted to be granted by the credit issuer until it has received express authorization of the consumer, effectively creating a credit freeze. The Bill would finally extend the right of consumers to free access to their credit report once yearly, and would allow free access once every three months to those with a fraud alert on their credit report. The tying of identity information breach notification to credit reporting is particularly welcome and a proactive measure likely to protect consumers.

Address verification by credit issuers

Californian law requires that credit issuers verify the address of the consumer if:

(a) an application for credit shows an address different from that on the pre-approved offer; or
(b) a request for a duplicate credit card is received within 10 days of a request for a change of address.[181]

Such verification helps to detect ID theft and can prevent ID thieves from benefiting from their theft.

Authentication of consumer identity

Fraudulent use of another person's identity to make purchases, obtain credit, obtain access to that person's credit report, or engage in other transactions can be prevented through the use of effective authentication measures. Such measures range from simple physical identity checks (e.g., requirement to attend in person, hand signature on credit card) to requirements for original identity documentation (e.g., for government-issued documents). Careful merchants, for example, always check the consumer's signature on receipts with the signature on the credit card, and may demand to see additional information (e.g., photo ID) where suspicious.

Such verification of individual identity should not involve the *collection* of additional personal information; rather, simple checking of the information should be sufficient.[182] The more personal information recorded, the more susceptible it is to abuse.

---

[181] California Civil Code, 1747.06

[182] Note the U.S. *Patriot Act*, under regulations made pursuant to s. 326, requires banks and other financial intermediaries to set up a "Customer Identification Program". They must ask to see personal identification and ask for date of birth, address and "taxpayer ID number" (usually a SSN). There is no requirement, however, that banks or others keep copies of such documentation. However, banks are permitted to keep copies of identification, and although the American Bankers Association recommends against it, "the man who wrote the rule said that it would be "prudent" to do so": *Privacy Journal*, "ID Requirements in Banks", June 2003, Vol. 29, No. 8, p. 5.

Passwords and PINs are now widely used to prevent unauthorized access to personal banking and other services. However, the proliferation of this form of authentication ignores the inherent limits on an individual's ability to remember several different passwords and PINs associated with different services, without recording them in a manner that would be helpful to ID thieves. Realistically, most individuals will have to use the same password for multiple purposes, or record the different passwords with their associated uses, in order to remember them. Reliance on these methods of authentication, while helpful, is therefore of limited assistance in the effort to reduce ID theft.

New authentication services, such as digital signatures in the online context, are now emerging, but are not yet widely used.

Biometrics, which authenticate identity based on the unique physical features of the individual (e.g., fingerprint, retina scan), are also being considered for many applications in which user identity needs to be authenticated. There are, however, serious privacy concerns with such technologies.[183] As some have pointed out, there is nothing secure about biometric ID cards unless the papers required to get them are equally secure. Reliance on biometrics requires absolute certainty that the right biometric data is associated with the identification document or database. A UK expert noted the possibility of "more reliable fake IDs, because once someone is able to get a card with false information, there will probably be no means by which that false information can be queried".[184] While Canadians may tolerate biometrics as an eventual part of passport issuance due to foreign requirements,[185] everyday reliance on such systems in Canada is rightly judged as far too invasive a technology.

It has been suggested that a national identity card would help to reduce the incidence of ID theft in Canada.[186] However, it is not clear that such a card would have this benefit – in fact, it could even exacerbate the problem of ID theft,[187] since fraudulently obtained cards would be even more difficult to identify and retract, and victims would likely have even more difficulty obtaining getting redress. Such a "universal identifier" would invariably face immense pressure towards function creep – it could become a "super-SIN".[188] Moreover, the concept of a mandatory identity card is repugnant to many

---

[183] See Statement of George Radwanski, Privacy Commissioner of Canada, to the Standing Committee on Citizenship and Immigration (March 18, 2003) (http://www.privcom.gc.ca/speech/2003/02_05_a_030318_e.asp).
[184] Mike Davis, quoted in Sarah Arnott, "Doubts surround national ID cards", vnunet.com (July 10, 2003)
[185] See comments of former Privacy Commissioner of Canada Bruce Phillips, delivered to Conference "Frontiers of Privacy and Security", Victoria, B.C., February 14, 2003.
[186] Minister Denis Coderre, Appearance before the Standing Committee on Citizenship and Immigration (Feb.6, 2003) and see footnote 1.
[187] Simon Davies. "The Id Card Is The Fraudster's Friend," The Sunday Telegraph, July 7, 2002: http://www.telegraph.co.uk/opinion/main.jhtml?xml=%2Fopinion%2F2002%2F07%2F07%2Fdo0703.xml.
[188] "SUBMISSION ON A NATIONAL IDENTITY CARD", Office of the Information and Privacy Commissioner for British Columbia, February 17, 2003. (http://www.oipcbc.org/publications/speeches_presentations/NIDsubm021703final.pdf).

Canadians, as indicated by the strong negative reaction to Minister Coderre's proposal.[189] Certainly the privacy implications of a National ID Card have not yet been fully discussed.[190] The cost of any system is also uncertain and potentially enormous.[191] Nor has the case been persuasively made that the Card would necessarily limit identity theft in a manner that represents an acceptable trade-off between privacy and security.[192]

Limiting disclosure of personal information

The federal PIPEDA includes general requirements for the secure protection of personal information, as well as for limited disclosure of personal information.[193] However, none of these requirements specifically addresses the problem of routine disclosure that, while not necessary offensive itself, can expose sensitive personal information to ID theft. Until recently, for example, credit bureaus included full credit card account numbers and social insurance numbers on consumer credit reports sent to consumers. After such reports fell prey to ID thieves last year, Equifax Canada changed its policy such that credit records sent to consumers no longer show their full credit card or SIN numbers.[194]

Consumer education and outreach

Consumers themselves play an important role in fraud prevention. In order to do so effectively, however, they must understand how ID theft occurs, and what measures they can take to prevent it from happening to them.[195] Many government agencies, business entities and consumer groups are making efforts to educate consumers about ID theft and their role in preventing it. Excellent resources in the USA include the ID Theft Resource Centre,[196] Privacy Rights Clearinghouse,[197] the National Consumer League,[198] the

---

[189] Victor Malarek, "Is your passport worth the paper?", *Globe and Mail* (March 15, 2003) p.F5; Elizabeth Thompson, "Invasive ID plan could cost billions, MPs warned; Privacy threatened, watchdog argues", *Canwest News Service* (March 19, 2003).

[190] See "News Release: Interim Privacy Commissioner questions merit of a national ID card", September 18, 2003 (http://www.privcom.gc.ca/media/nr-c/2003/02_05_b_030918_e.asp).

[191] *Ibid.*

[192] *Ibid.* The Interim Privacy Commissioner's concerns include the following comment: "It is also said that an identification card would help combat identity theft. Again, how that would work is not at all clear. A comprehensive infrastructure of electronic card readers and trained personnel would be very complex technically, and very expensive to deploy. And the system would still rest at some point on foundation documents like birth certificates and drivers licences, so an identity thief who surreptitiously obtained foundation documents could still apply for a card in someone else's name."

[193] Principles 7 and 4, respectively, of Schedule 1 to the *PIPEDA*. The Federal Privacy Commissioner, in a recent decision (#121, discussed above), found that a financial institution that allowed an employee identity thief to gain access to a client's identity to make fraudulent transactions was in contravention of principles 4.3 and 4.5 of the PIPEDA. However, the Commissioner concluded the bank could not be faulted for its employee's actions at a systemic level, as it had had adequate screening procedures for employees and had quickly identified the fraud and taken remedial action. However, the customer, not the bank, discovered the fraud. It may therefore be asked if the bank had an adequately proactive fraud discovery system.

[194] Ellen Roseman, "Identity thieves prey on slack mail security", *Toronto Star* (April 20, 2002), p.D03.

[195] We provide this information below, in the chapter entitled "What Consumers can do to prevent ID theft".

[196] http://www.idtheftcenter.org/

[197] http://www.privacyrights.org/identity.htm#sheets

[198] http://nclnet.org/privacy/

Federal Trade Commission,[199] and the US Department of Justice.[200] Sources of consumer information and advice in Canada include PhoneBusters,[201] Privacy Commissioners,[202] TransUnion (a credit bureau),[203] Industry Canada's "Consumer Connection",[204] and the Ontario Ministry of Consumer and Business Services.[205] While these and other resources are helpful, they are only seen by consumers who have Internet access and who either are referred to the site, or come across it in their online research. Consumer education requires more proactive measures, offline as well as online.

Moreover, as pointed out above, even the most successful consumer education will be limited in effectiveness. This is because ID theft so often occurs in a context over which the consumer has no control. Even perfect fraud prevention practices by consumers will not solve the ID theft problem. Efforts to stem the tide of ID theft should therefore focus mainly on industry practices.

MEASURES THAT MAY ASSIST IN DETECTING IDENTITY THEFT

Given that ID theft is usually not detected until long after it occurred, measures to enable early detection are critical.

Access to one's personal information held by organizations

Numerous laws provide consumers with the right to access their personal information held by organizations. Through such access, consumers may be able to identify fraudulent activity that would not otherwise have been noticed. Public sector privacy legislation provides citizens with the right to access their personal information held by government.[206] Similarly, private sector data protection legislation, both general and sector-specific, gives individuals the right to access their personal data held by business organizations.[207] Perhaps most relevant is the consumer's right to access her credit report, at minimal cost and effort, a right which is granted by every provincial statute governing credit reporting.[208]

Monitoring and detection by credit service providers

Credit card theft detection

In an effort to manage their own financial risk, credit card providers monitor account activity with a view to identifying abnormal transactional patterns. Credit card companies

---

[199] http://www.consumer.gov/idtheft/
[200] http://www.usdoj.gov/criminal/fraud/idtheft.html/
[201] http://www.phonebusters.com/Eng/SpotaScam/scams_identity_theft.html
[202] See, for example, http://www.privcom.gc.ca/ and http://www.ipc.on.ca/
[203] http://www.tuscores.ca
[204] http://strategis.ic.gc.ca/SSG/ca01831e.html
[205] http://www.cbs.gov.on.ca/mcbs/english/5JQN9M.htm
[206] See the federal *Privacy Act*, as well as provincial *Freedom of Information and Protection of Privacy Acts*, op cit.
[207] e.g., PIPEDA, s.8.
[208] see, for example, s.12 of Ontario's *Consumer Reporting Act*.

typically track customer transactions in order to identify unusual spending patterns that suggest fraud. Cardholders are contacted in order to confirm transactions or to identify the fraud at an early stage.[209]

Cardcops.com is a website service that allows users to check a their card numbers against a database of stolen credit card numbers. The service, set up by an anti-fraud education group in the USA, collects the information from Internet chat rooms where thieves have been checking whether stolen card numbers are still good to use or have been deactivated. Cardcops provides free access to the database but does charge for an automatic notification service.

Debit card theft detection

Although debit card misuse tracking may present more challenges than credit card tracking, it would seem to be possible to transfer similar techniques to identifying abnormal transactional patterns in debit card use. However, to date there appear to be no such initiatives by debit card processors or issuers.

Credit bureaus

With the rise of ID theft, the market for fraud detection services is growing. Credit bureaus, for example, offer a number of fraud detection tools to businesses, including access to a database of potentially fraudulent information, use of which can alert businesses to possible fraud before they issue credit or open an account. Business input is compared against the database, and if there is a match, a warning message is generated to prompt further investigation. Another service automatically alerts credit grantors to heavy inquiry activity, as well as mismatches between input information and information on file. A further fraud detection service allows merchants or their processors to verify the billing name and address of consumers' presenting credit cards for payment on the internet or for mail order / telephone order purchases.[210] However, all of these products target the credit supplier, and are not offered to the subject of credit, the consumer.

A similar early-warning system to that employed with credit cards may be emerging using software tracking unusual activity on an individual's credit report, such as creditor inquiries and opening of new accounts. (As noted, Equifax and TransUnion both offer fraud alert services to their creditor clients, but not to individual subjects of credit reports.) In the U.S., ID Analytics executives who worked to develop the "Falcon" credit card fraud alert programs are reportedly working on a similar program for credit applications. The system would assign an "ID score" to each credit application, "similar to a credit score, which indicates the likelihood that a given application is fraudulent." It appears this system would operate outside the credit bureaus and would require creditors

[209] A leading such service is known as Falcon™ Fraud Manager from Fair Isaac.

[210] See http://www.tuc.ca/TUCorp/subscriber/managementproducts.htm#1 and http://www.equifax.com/EFX_Canada/services_and_solutions/fraud_services/index.html

to join the system and pay for it[211] – which these credit companies may be reluctant to do without legislation requiring such a system.

ID theft insurance and credit-monitoring

In the USA, credit-monitoring services are now offered to individual consumers for a price, ranging from US$40 to $80 per year.[212] While an obvious value proposition for consumers concerned about their vulnerability to ID theft, reliance on market solutions such as this inappropriately shifts the cost of the problem onto innocent consumers, many of whom cannot afford the service in any case. Such services are beginning to appear in Canada.

In a similar vein, identity theft insurance is now offered by a number of companies in the USA, usually for a fee.[213] Other services offered only to US residents include American Express's "CreditSecure" service, which, for a fee of US$9.95/mo. or $99.95/year, offers credit monitoring services and ID theft insurance coverage, as well as sample dispute letters and toll-free assistance.[214]

Once again, these are market responses to a growing problem, responses that are not satisfactory insofar as they unfairly shift the burden onto consumers and are available only to those who can afford them. To a large extent, as well, they may be providing unnecessary insurance, in that much of the loss insured against may be covered by credit card company zero-loss policies and debit card loss policies.[215] All consumers, rich and poor, knowledgeable and unknowledgeable, need protection against ID theft, and should have resources such as these available to them at no, or minimal, cost.

Telecheque payments to be disallowed

The Canadian Payments Association, the national body tasked with supervising the Canadian clearing and settlement mechanisms has decided to refuse to process "telecheques" effective January 1, 2004.[216] These are cheque-like instruments that are created when a consumer contacts a business using a telecheque service:

> A tele-cheque is a paper item that has the physical attributes of a cheque, but unlike a typical cheque, it is prepared and signed by someone (usually a

---

[211] ID Analytics has "announced a partnership with Primary Payment System (PPS)" a financial risk management company to market to, and deploy the system in, financial institutions. See: "ID Analytics and Primary Payment Systems Bring the ID Score to Retail Banking to Fight Identity Fraud", PRNEWSWIRE, August 19, 2003, http://news.corporate.findlaw.com/prnewswire/20030819/19aug2003134149.html.

[212] E.g., PrivacyGuard.com, Privista.com, Consumerinfo.com and Equifax.com.

[213] E.g., PromiseMark.com, Identityfraud.com, TrueLink.com, Travelers Insurance, Chubb Insurance.

[214] http://www.americanexpress.mycreditsecure.com/home.asp?source=3

[215] See Canadian Code of Practice for Consumer Debit Card Services, at http://strategis.ic.gc.ca/epic/internet/inoca-bc.nsf/vwapj/Debit_Card_Code2.pdf/$FILE/Debit_Card_Code2.pdf, discussed above..

[216] Prohibition of Tele-cheques in the Clearing & Settlement System – Policy Statement, Canadian Payments Association, June 1, 2003 (http://www.cdnpay.ca/news/tele.asp).

> Payee) purporting to act on the authority of the account holder (i.e., the Payor) and as such does not include the signature of the Payor. To initiate a tele-cheque, the Payee generally obtains the necessary account information from the Payor over the telephone or via the Internet. Furthermore, the payment is not supported by an underlying written authorization [e.g., Payor's Pre-Authorized Debit (PAD) Agreement or power of attorney]. By reason of the manner in which the account information is obtained and the item is created, a tele-cheque is also commonly referred to as a "cheque-by-phone" or an "e-cheque".[217]

Since there is no way for the financial institution to verify the information provided by a telecheque has been authorized, the CPA has taken this "pro-active measure", even though the CPA is not presently aware of any fraudulent use of telecheques in Canada to date.[218] The removal of this payment option is therefore an example of ID risk management, and an example of the forward-looking policies of removing high ID-theft-risk products before they become a cost to consumers and a source of ID fraud.

Mandatory address change notification

As another ID theft risk management technique, Detective Staff Sergeant Barry Elliott of PhoneBusters would tighten up the use of false addresses by legally requiring individuals to register changes of address with government departments, financial institutions and other key services.[219] At present, such a legal requirement of change of address is generally found only in drivers' licensing statutes. Elliott claims such a requirement of forced prudence on individuals would significantly curtail ID thieves' ability to use outdated addresses or set up new ones, a key element of ID theft. However, enforcement of such a law may be impractical, and the potential effects upon consumer's privacy have not been considered.

MEASURES DESIGNED TO ASSIST VICTIMS

Credit bureaus – fraud alerts

According to Equifax, the company "will add a statement to your file to alert credit grantors that you may be a victim of fraudulent activity. This may mean that the next time you apply for credit you will be questioned more thoroughly as a precautionary measure. The credit grantor wants to make sure that you are, in fact, the person you say you are." Unfortunately it does not mean that a credit grantor will contact the consumer before opening new accounts, accounts that could be opened by an ID thief. And the potential safeguard assumes that credit grantors check with Equifax before granting credit.

---

[217] *Ibid.*
[218] News Release, "TELE-CHEQUES TO BE PROHIBITED IN CANADIAN CLEARING SYSTEM", Canadian Payments Association, June 23, 2003 (http://www.cdnpay.ca/publications/news_tele.asp).
[219] Telephone interview with Det. Sgt. Barry Elliott (September 23, 2003).

TransUnion will alert credit grantors to get in touch with the consumer before opening new accounts. The company "will review your credit file and identify potentially fraudulent accounts, inquiries to your account and recent fraudulent applications that may have been made in your name. A protective statement is added to your credit report, alerting future credit grantors. This statement, which includes your phone numbers (home and work), alerts them to contact you and verify your identification before opening new accounts." However, this is not a guarantee that credit grantors will contact the consumer – and the potential safeguard assumes credit grantors check your credit with Trans Union.

Northern Credit Bureaus Inc. likewise will place a fraud alert on an individual's credit report with contact information for that individual and has toll-free phone and fax numbers for consumers to report ID theft.[220] However, this information is not posted on Northern's website.

Credit bureaus have a vested interest in the reliability and accuracy of their databases and should be amenable to consumer initiatives to increase this reliability. The complication appears to arise in the method of undertaking such fixes, who should initiate them, and who should pay for them. As noted above, legislation may be needed which requires credit bureaus to place a fraud alert on files that a creditor has identified (and is required to identify) as possible identity theft targets due to a breach of information security.

Credit bureaus – security "freeze"

Most businesses will not open credit accounts without checking a consumer's credit history first. If a credit file is frozen, even someone who has an individual's name and SIN would probably not be able to get credit in that person's name.

Consumers in California have the right to put a security freeze on their credit files, free of charge, if they are the victim of identity theft and have a police report.[221] If a consumer wants to open a new credit account or get a new loan, he or she can lift the freeze on his or her credit file. The freeze can be lifted for a period of time. Or it can be lifted for specific creditors. After sending a letter asking for the freeze, each of the credit bureaus sends consumers a PIN. They can lift the freeze by telephone, using their PINs. The credit bureaus must lift the freeze within three days.

Such "credit freezing" services are neither required nor even available to individuals in Canada. They would entail costs to credit bureaus – costs of both implementing the freeze and of being unable to sell frozen reports. Credit bureaus are unlikely to embrace this extra cost without legislative coercion.[222] California law addresses this dilemma by requiring free freezes for victims of ID theft, while allowing credit bureaus to charge consumers for "preventative" freezes.[223] Such charges may need to be regulated in order to be reasonable and affordable to consumers.

---

[220] Telephone conversation with Richard Huot, Northern Credit Bureaus Inc., September 25, 2003.
[221] California Civil Code 1785.11.1 and .2 Non-victims are charged for this service.
[222] See Senate Bill 1633, discussed above, for an example of this type of legislation.
[223] See http://www.privacyprotection.ca.gov/security_freeze.pdf for a description of the California practice.

Standard ID theft affidavit

In the United States, a standard ID theft affidavit exists that is accepted or endorsed by many companies and organizations. The affidavit was developed in conjunction with banks, credit grantors and consumer advocates. This simplifies the affidavit process for consumers. A standard affidavit does not exist in Canada at this time, however a tool to achieve the same effect is presently being worked on by federal/provincial/territorial governments in conjunction with stakeholders.[224]

Protection from debt collectors

Under Californian law, no creditor can sell a consumer's debt to a collection agency once the consumer has reported the fraud to a credit bureau.[225] Also, ID theft victims have a statutory right to request an injunction against debt collectors who pursue collection after being notified of the fraud.[226]

In Ontario, debt collectors are prohibited from further collection activities once the alleged debtor has informed the agency or collector that they are not in fact the debtor, "unless the collection agency or the collector first takes all reasonable precautions to ensure that the person is in fact the debtor".[227] It is not clear to what extent this requirement to take reasonable precautions has helped ID theft victims stop misdirected collection activities. As long as the consumer has evidence of the fraud (e.g., via an affidavit as described above, or a police report), such evidence should be sufficient to invoke this prohibition.

Court-ordered restoration of victim credit reports

One of the most troubling aspects of ID theft is the time and trouble that victims must endure in order to clear their names, even long after the theft was discovered and agencies notified. The most common problem involves centralized credit reports, given their wide usage by all sorts of credit-granting businesses. Indiana recently passed a law that gives courts the authority to order credit reporting agencies to restore a victim's credit history.[228]

---

[224] Telephone conversation with Barry Elliott (September 23, 2003) and e-mail from Office of Consumer Affairs, Industry Canada (October 20, 2003).
[225] California Civil Code, 1785.16.2
[226] *Ibid.*, 1798.92-97
[227] *Collection Agencies Act Regulations,* R.R.O.1990 Reg.74, subs.20(h). This rule is part of a harmonized package of regulations affecting collection agencies that all provinces and territories are considering enacting.
[228] Enrolled Senate Bill 0320, First Regular Session 113th General Assembly (2003) (http://www.in.gov/legislative/bills/2003/SE/SE0320.1.html)

Toll-free hotline and online support

Victims need ready access to counselling and assistance. The FTC has operated a toll-free hotline for ID theft victims in the USA since 1999. The service is now widely known and used. In Canada, there is no similar service. PhoneBusters operates a hotline for telemarketing fraud, and is now dealing with ID theft as well, but not in the comprehensive and focussed way that the FTC is.

However, this dearth of easy-to-use options for ID theft victims in Canada may be changing. The Solicitor General and the RCMP announced the creation of the RECOL (Reporting Economic Crime Online) fraud reporting website October 3, 2003 (www.recol.ca).[229]

The website relies on individuals to provide personal profiles and consent to the law enforcement agency members to begin an investigation. Telephone support for those filing complaints will be provided by the PhoneBusters National Call Centre. The RECOL service is administered by the National White Collar Crime Centre of Canada. It represents a partnership of several law enforcement agencies and "other organizations concerned with white-collar crime". It is not clear if these other agencies will include credit bureaus and financial institutions or other credit grantors.

Nevertheless, the RECOL website provides a simple, user-friendly access point for consumers who need to begin the arduous process of investigating their ID theft problems.

Victim database

California operates a special ID theft registry for victims of criminal ID theft, to prevent false arrests. ID theft victims registered in the database are given a PIN code. If they are threatened with arrest by a police officer for a crime committed by the ID thief in their name, they can give the police officer a toll-free telephone number and the PIN code, which informs the officer that the individual is indeed an ID theft victim.[230] The Australian Crime Commission has recently created a National Identity Fraud Register, which it claims is the first national, functioning ID theft registry.[231]

---

[229] See "Federal Solicitor General Launches New Internet Site for Canadians to Report Economic Crimes", October 3, 2003, http://www.sgc.gc.ca/publications/news/20031003_e.asp.

[230] See http://www.ag.ca.gov/idtheft/general.htm. More information on criminal ID theft can be found at http://www.privacyrights.org/fs/fs17g-CrimIdTheft.htm. According to Beth Givens of the Privacy Rights Clearinghouse, only one or two people are currently registered in this database.

[231] Media Release, "ACC uses special powers to tackle identity crime", September 26, 2003 (http://www.crimecommission.gov.au/content/media_rel/2003/mr030926-ellison.pdf)

CONCLUSIONS AND POLICY RECOMMENDATIONS

Identity theft is a significant problem that is growing explosively in Canada, as elsewhere. It demands legislative and policy action, aimed at better protecting consumer information, deterring identity thieves, and assisting victims. While consumers must certainly take responsibility for protecting their own personal information, the role of businesses – especially those in the credit and data-management industries – in facilitating ID theft demands attention. As noted by a US expert:

> "Without industry prevention efforts, consumers whose identities have been stolen will continue to bear the brunt of social and economic costs."[232]

There are many "leak-points" in corporate data management systems, through which personal information is exposed to theft and abuse; these should be identified and addressed, starting with the credit-granting industry. In particular, credit grantors should be held to a higher standard of authentication in respect of applicants for credit, and should be held accountable for negligence (e.g., ignoring obvious clues such as missing information) that facilitates ID theft and related fraud.

Some of the factors contributing to ID theft can be addressed by providing consumers with better control over the collection, use, and disclosure of their personal information – for example, the ability to put a security freeze on credit files. In order to exercise such control, however, consumers also need knowledge – knowledge about risks and vulnerabilities of their personal data, as well as knowledge about their rights and responsibilities in respect of data management.

Other important causal factors require significant change in business practices – for example, less reliance on SINs for consumer identification and data management purposes, more stringent controls on the granting of credit, and verification of address change requests.

In addition, victims of this crime need to be able to regain their credit and reputations without undue effort. Business and governments should take more responsibility for assisting those who have fallen prey to ID theft, especially when it was through no fault of their own.

A note of caution is however in order: it is important that action to stem the tide of ID theft does not unduly infringe on individual privacy and civil liberties. National identity cards, biometric identifiers and integrated government databases[233] have all been suggested as methods by which to reduce the incidence of ID theft. However, these initiatives raise serious privacy issues, and should not therefore be undertaken without

---

[232] Gartner Inc., "Gartner says identity theft is up nearly 80 percent", News Release (July 21, 2003).
[233] James Pearce, "AU government's eyes are on you" *ZDNet Australia (*07 July 2003)

thorough public consultation, debate and careful consideration of their dangers in terms of civil liberties and freedom from state control. Other measures more focused on the ID theft problem should be instituted first. Only then should riskier innovations such as alternative unique identifiers be discussed.

The following are some specific recommendations:

Governments and Law Enforcement Agencies

Stronger enforcement of existing laws

Law enforcement agencies should be more aggressive, and should work more closely together to pursue and convict identity thieves under existing criminal laws. More resources should go into the investigation and prosecution of crimes involving identity theft, and sentences should reflect not only the impact on victims, but also the need to deter this apparently growing crime. Alternative approaches such as offering perpetrators reduced sentences for providing information on the method of performing ID theft could also be considered. Governments should work together with law enforcement experts to develop and implement effective training programs on ID theft detection and prosecution, for use by law enforcement agencies.

Possession of multiple persons' identity documents as a criminal offence

The federal government should complete its consideration of this proposal, engage in consultation with appropriate stakeholders, and, if it can be done without unduly infringing on civil liberties (e.g., by including appropriate exceptions), enact a new *Criminal Code* offence outlawing mere possession of multiple persons' identity documents.

Stronger data protection laws

Consumers need to be able to control the amount of personal information about them that is circulating in the marketplace and thus vulnerable to ID theft. The federal *Personal Information Protection and Electronic Documents Act* goes a long way towards providing consumers with such control. However, it needs strengthening in some respects. For example:

- consumers should always have the right to refuse to provide personal information that is not necessary for the requested service or transaction, without being denied the service or transaction, and without a reduction in the quality of service they receive;
- the Act should set clear limits on when opt-out consent can be used, and should provide clear criteria for validity of such consent;
- there should be time limits on the validity of consent to collection, use or disclosure of personal information in other than exceptional cases;

- organizations should be required to shred, erase, destroy or make anonymous all records containing personal information that are no longer required to fulfil the specified purposes for which they were collected or used.

Stronger protection against SIN abuse

While data protection laws limit the ability of private sector organizations to *require* that consumers provide their SIN in order to obtain products or services, they do not restrict any organization from *requesting* provision of SIN information. Hence, the onus is on the consumer to refuse such requests, and to be aware of their rights in this respect. Moreover, the law does not restrict organizations from providing significantly better service to those who provide SINs than to those who refuse.

Stronger legislation restricting the right of unauthorized SIN users to collect this highly sensitive information is therefore needed. Only those specifically authorized to do so should be permitted by law to collect this information.

Consideration should also be given to clearer and more specific limits on the use of SINs by those authorized to collect, use or provide this information. Interestingly, California has prohibited the public display of Social Security Numbers (SSNs), the printing of SSNs on mailed documents, and the unencrypted transmission of SSNs over the Internet.[234] Similar prohibitions should apply in Canada.

Finally, further to the Auditor General's 1998 report, more effort should be applied to prosecuting SIN abuse, and penalties actually imposed for this type of ID theft should be sufficient to have a strong deterrent effect.

Centralized clearinghouse for information on identity theft in Canada

The 1999 US *Identity Theft and Assumption Deterrence Act* (18 USC 1028) established an ID theft clearinghouse within the FTC. Through this initiative, the USA now has a national database of ID theft statistics that is shared with law enforcement agencies, and a website with useful information for the public on how to protect against ID theft. Canada appears to be heading in this direction, using the existing work being done by PhoneBusters, and now with RECOL, headed by the RCMP.

Government ID data audit

In Australia, "[a] whole-of-government study . . . is currently being undertaken to enhance the identification and verification processes for government agencies and to identify other measures to combat identity fraud." Consideration should be given to a similar study and audit of government identification information practices in Canada, at both the federal and provincial levels.[235] Such an audit would specifically address the

[234] California Civil Code, 1798.85 . California has also legislated a requirement for all health information providers to cease putting SSNs on health cards, by 2005.
[235] Media Release, "ACC uses special powers to tackle identity crime", *supra*.

particular issues noted above: SIN and other government-issued identifier use and abuse, criminal law reform and enforcement, and a privacy law review.

Governments and Businesses

Notification of security breaches

As in California, organizations (public and private) should be required by law to notify potentially affected individuals as soon as they become aware of unauthorized access to databases containing sensitive personal information such as SINs, credit card numbers, or bank account information. Failure to comply should be punishable by fines of a magnitude sufficient to ensure diligence in the security of such databases.

Standard ID theft affidavit

A standard ID theft affidavit that is endorsed and accepted by companies, credit bureaus, and other relevant organizations should be introduced in Canada, as in the USA.[236] This simplifies the process of disputing fraudulent debts for consumers and others. The affidavit should be developed in consultation with consumer groups, and should be standard across the country.

ID theft audit as part of privacy audit

The PIPEDA and other privacy laws should require an audit of all organizations' data security not only for obvious vulnerability to theft (e.g., "Safeguards", Principle 7, PIPEDA) but also specifically potential manipulation of data to the ends of ID theft.

Financial Services Industry

Identification and reporting of ID theft-related fraud

As noted above, many companies don't recognize identity theft fraud for what it is; instead, they simply write it off as credit losses, "causing a serious disconnect between the magnitude of identity theft that innocent consumers experience and the industry's proper recognition of the crime".[237] The financial services sector needs to be more proactive in identifying, as well as preventing, ID theft fraud.

Notification by credit card issuers of suspicious activity/Verification of address

If an application for credit shows a different address than that on the pre-approved offer, or if a cardholder requests an additional card within 30 days of a change of address, the card issuer should be required by law to notify the cardholder at both the new and former address, in order to verify the address.

---

[236] See www.consumer.gov/idtheft .
[237] Gartner Inc., "Gartner says identity theft is up nearly 80 percent", News Release (July 21, 2003).

More consumer control over the granting of credit

Consumers should not be subject to unsolicited pre-screened or pre-approved credit card offers without their prior explicit consent, obtained through an opt-in process.

Credit card limits are often increased without obtaining prior consent from cardholders, placing cardholders at greater risk if ID theft occurs. Prior informed consent should be obtained from consumers before increases to credit limits are implemented, and before any "convenience cheques" are mailed to them.

Checking for fraud alerts on credit files

Prospective creditors should be required to check the credit bureau files of applicants for fraud alerts,[238] and, where an alert exists, to refuse to grant credit without more formal proof of the borrower's identity. Credit issuers should be subject to substantial penalties if they ignore fraud alerts.

Truncation of credit card account numbers on electronic receipts

Electronic credit card receipts should show no more than five digits of the credit card account number, so that they cannot be used by ID thieves. Phased-in legislation may be necessary to ensure that this occurs throughout the marketplace.

Better disclosure by financial institutions to consumers of risks inherent in electronic banking, at and before the time of application for service

Electronic banking is being heavily promoted, no doubt because it lowers costs for financial institutions. While this option offers obvious benefits to consumers (e.g., 24 hour access), it also entails risks, such as a greater likelihood of unauthorized access to one's bank account due to reliance on cards and PINs. Yet such risks are not well communicated, and are therefore not fully appreciated by consumers.[239]

---

[238] Ideally, this check should include all the major credit bureaus, as each bureau holds different records. This may entail extra costs to borrowers in the form of loan application fees, however, it could be offset by the savings in credit costs by reducing identity theft.

[239] Most major Canadian banks now have electronic banking security webpages. Some have webpages that describe ID theft and provide information on preventing debit card fraud. However, the link between the two is de-emphasized, as is the risk of electronic banking in general. See, for example: http://www.rbc.com/security/identity.html , http://www.rbc.com/identity_tips.html and http://www.rbc.com/security/bulletinABM.html. In the latter webpage, Royal Bank of Canada claims:

> While alerting the public to scams is the responsibility of the police authorities, RBC reinforces procedures for the use and safeguarding of bank cards in many ways:
> - verbally,
> - prominently in materials that accompany a new card or replacement card,
> - in consumer awareness brochures such as "Straight Talk about Safeguarding Against Financial Fraud," available in branches or by calling 1-800-ROYAL-99.
> - on our web site

Financial institutions should be required to disclose such risks, clearly and prominently, both in their promotional documents and in all applications for electronic banking services. Financial institutions must set clear policies on consumer liability for debit card fraud – preferably zero liability policies as exist with major credit issuers.

Limited liability of consumers in case of banking fraud

Consumers need legislated protection from banking fraud, where such fraud is not the result of their own negligence or willful wrongdoing. Some financial institutions currently place unreasonably high levels of responsibility and liability on individual consumers of electronic banking services. If financial institutions are made liable for fraud that is not clearly due to consumer negligence or wrongdoing, there will be a much stronger incentive for such institutions to guard against such fraud in the first place.

Protection from debt collectors

All provinces should adopt the harmonized regulations on debt collection that have been proposed by the Consumer Measures Committee, a federal/provincial/territorial working group and adopted so far by Ontario and the NWT. These regulations include a clause prohibiting collection activities once the alleged debtor has informed the agency or collector that they are not in fact the debtor, unless the collection agency or the collector first takes all reasonable precautions to ensure that the person is in fact the debtor. Especially if combined with a standard ID theft affidavit, such that provision of the affidavit would trigger the prohibition, this rule could assist ID theft victims in stopping collection activities involving a debt that they did not incur.

Consumers should also have statutory rights to seek injunctions against collection agencies who fail to stop collection activities after being provided with an affidavit or other proof of the fact that they are not the debtor.

Finally, consumer protection statutes should prohibit creditors from transferring a consumer's debt to a collection agency once the consumer has reported the fraud to the credit bureau. Failure to respect this prohibition should be an offence, as well as a cause of action.

Credit Bureaus

Reducing leakage of sensitive consumer information

Credit bureaus should be required to keep SINs confidential and not to disclose them to consumers or others on credit reports. Credit bureaus should work with credit providers, governments and consumer groups in an attempt to define an alternative unique identifier for use in credit reporting.

More consumer control over flows of personal credit information

To the extent that credit bureaus disclose consumer credit information to third parties for the purpose of marketing financial services, the bureaus should be required to offer a simple means by which consumers can opt-out of such information sharing. As in the USA, Canadian credit bureaus should offer a single toll-free number through which consumers can stop the flow of such marketing offers.

Credit bureaus should also be required to obtain proof of consumer consent from organizations seeking to access the consumer's credit file.

Fraud alerts on credit files

The three national credit bureaus in Canada, Equifax, TransUnion and Northern, voluntarily offer to place fraud alerts on consumer credit files, where ID theft is suspected. However, as noted above, these voluntary practices are limited in effectiveness.

All credit reporting agencies should be required by law to place fraud alerts on consumer files upon request, at no cost, or upon notification by a creditor of a possible information leak. In addition, they should be required to communicate the entire text of the alert to all credit issuers who request any information (including bare credit scores) on that consumer. Credit issuers should be required to check for and observe fraud alerts on credit reports. Failure to comply should be a punishable offence and an actionable tort.

Security freezes on credit files

Consumers should be entitled to put a "security freeze" on their credit files. A security freeze means that one's credit file cannot be shared with potential creditors, insurance companies or employers doing background checks. Consumers should be able to lift the freeze for a period of time or for specific creditors by telephone, using a PIN.

Such freezes should be provided free of charge to victims of ID theft, and at low cost to other consumers.

Corroboration standards

Credit bureaus should be held to a meaningful standard of corroboration regarding negative information about a consumer submitted to them. Current legislative provisions in this respect should be clarified and made more specific.

Notifying consumers of possible fraud

As noted, credit bureaus should be required to inform credit *issuers* when new information on the consumer's file suggests possible fraud. Consumers also should be notified of possible fraud. However, care must be taken in communicating this

information to the consumer. It is tempting to suggest notifying consumers at all addresses on record for the past six months (or some other reasonable period), however, this may assist identity thieves by revealing suspicion of their activities, if the thieves have created a new false address. Thieves may attempt to justify the new credit pattern to potential credit issuers and the credit bureaus before the real consumer calls to inquire. However, whatever the shortcomings, this may be the only way to reach the real consumer.

Specific indicators of fraud should be identified by consumers and credit issuers in conjunction with credit bureaus and treated as triggers for such notification. Triggers could include situations where:

- an unusual number of credit applications are made within a short period of time;
- there are numerous inquiries within a short period of time;
- a new credit account is recorded on the credit report;
- there are discrepancies between the address on a credit application and that on the credit report; or
- certain negative information is placed on the credit report.[240]

Consumers

Practical self-defence and awareness

Often there is nothing the ID theft victim could have done to prevent the theft, however, there are basic steps that should become part of every consumer's ID theft "toolkit".[241] The Solicitor General of Canada and the U.S. Department of Justice have issued a joint Public Advisory for consumers on ID theft listing several steps.[242] The U.S. DOJ web site uses the acronym "SCAM" to describe the wary consumer mindset. It stands for:

- "Stingy" (one should give out only the minimal information necessary, and only when necessary);
- "Check" ("Check your financial information regularly, and look for what should be there and what shouldn't")
- "Ask" (regularly for a copy of your credit report – from all major bureaus)
- "Maintain" (careful records of your banking and financial accounts – for evidence)

---

[240] Richard Huot of Northern Credit Bureaus Inc., notes that many of these factors are potentially normal and neutral: for example, many consumers trigger multiple financing inquiries when car-shopping over a weekend. Care would have to be taken to set up a sensitive and smart system to reduce false positive (fraud) and false negative (no fraud) results. Huot also noted that negative credit information, if generated by the actual consumer, should not be accidentally excluded from the credit report due to the fraud alert system. (Telephone conversation with Richard Huot, Northern Credit Bureaus Inc., October 9, 2003).

[241] See Appendix B for a more detailed list of safeguards that individual consumers can implement in order to reduce the risk of ID theft. See Appendix C for advice on how to proceed if you are a victim of ID theft.

[242] http://www.usdoj.gov/opa/pr/2003/May/publicadvisory1.pdf. Note that many of the resource pages noted in Appendix A to this report list other steps for consumers.

APPENDIX A - USEFUL WEBSITES ON IDENTITY THEFT

CANADA:
www.PhoneBusters.com/Eng/SpotaScam/scams_identity_theft.html (police initiative)
www.recol.ca (RCMP-led single-window, online ID theft reporting website)
www.ipc.on.ca - search under "identity theft" (Ontario Privacy Commissioner)
www.privcom.gc.ca/fs-fi/02_05_d_10_e.asp (Federal Privacy Commissioner)
www.cbs.gov.on.ca/mcbs/english/55XMZ8.htm (Ontario government)
www.tuscores.ca – under "Personal Solutions" and "Fraud Victim Information" (TransUnion – a credit reporting agency)

USA:
www.consumer.gov/idtheft (Federal Trade Commission)
www.usdoj.gov/fraud.htm (U.S. Department of Justice)
www.idtheftcenter.org (Identity Theft Resource Center – a non-profit organization)
www.privacyrights.org (Privacy Rights Clearinghouse – a non-profit organization)
www.nclnet.org/privacy (National Consumers' League – a non-profit organization)

APPENDIX B - AVOIDING IDENTITY THEFT: RECOMMENDED PRACTICES FOR CONSUMERS

Social Insurance Numbers

- Keep your SIN card in a safe place – not in your wallet or purse. Only your employer needs to see your SIN card. All other *authorized* users (see below) need only be provided your number.
- Don't provide your SIN to unauthorized users such as businesses. By law, you must provide your SIN to authorized federal agencies, such as Human Resources Development Canada and Canada Customs and Revenue Agency, your employer, and anyone else who prepares income tax information on your behalf. This includes some provincial and municipal agencies that must report financial assistance payments for income tax purposes, and all institutions from which you earn interest or income, such as banks, credit unions and trust companies.
- Don't throw out documents such as tax forms without destroying your SIN.
- Keep your birth certificate in a safe place – not in your wallet or purse. It's a key document for obtaining a SIN and other important documents.
- If another person uses your Social Insurance Number for employment purposes or to receive other taxable income, you will receive a Notice of Reassessment from Canada Customs and Revenue Agency concerning undeclared earnings. This is an indication of fraudulent use of your Social Insurance Number, and should be reported to a Human Resources Development Canada (HRDC) office.
- You must report the loss or theft of your Social Insurance Number card to the police and obtain a copy of the police report that will indicate your card has been lost or stolen. Request a replacement card or a new Social Insurance Number from HRDC. Contact credit bureaus to request that an annotation be placed on your credit file. You may wish to request that creditors contact you before opening any new account.

Credit cards

Credit card fraud is the most common form of ID theft reported. Typically, ID thieves open new credit card accounts using a victim's identity or make fraudulent charges to existing accounts. While credit card issuers generally cover the cost of fraudulent transactions, failure by the consumer to take reasonable precautions or to report a stolen card can expose him or her to liability. Also, theft of credit card information can lead to other forms of ID theft. Even with "zero liability" protection against fraudulent credit card transactions, therefore, consumers need to take precautions:

- Do not have more cards than you need.
- Reduce your credit limit if you do not need the amount you have been granted. Pay attention to your credit limit. Credit card limits are often increased without the cardholder's prior consent.
- Review the charges on your credit card statement to ensure they are valid. If your credit card charges are available through online banking, keep a regular eye on the charges when you bank online.

- Try to ensure that businesses do not retain your credit card information in their records. Their records may not be secure. Remember that you have entrusted organizations to protect your credit card information if you let them make automatic recurring charges to your credit card.
- Do not respond to unsolicited telephone and email requests for your credit card information. Know whom you are dealing with. If you think the request may be legitimate, contact the organization before you provide information. Do not email or fax your credit card information.
- Protect your postal service mail from ID thieves. Use a secure mailbox that is not accessible to thieves looking for credit cards, credit card statements and unsolicited pre-screened credit card offers. Deposit outgoing mail in post office collection boxes or at your local post office.
- Watch for delays in the delivery of your mail. Pay attention to your billing cycles. Report anomalies in your mail service to Canada Post. An ID thief may have fraudulently changed your address at the post office, redirecting credit card information.
- Destroy credit card information on documents that you throw out. Remember that merchants often print your complete credit card number and name on credit card receipts.
- Don't print your credit card number on bank cheques.
- Do not carry your cards in your chequebook.
- Protect or destroy the credit card cheques that credit card companies often send cardholders.
- Never leave your credit cards unattended at work. The workplace is the number one place for thefts. Don't leave your credit cards in your car. A very high proportion of credit cards is stolen from motor vehicles.
- Protect your Personal Identification Number (PIN). Don't write it down, memorize it. If you have to record it, do so in a place and manner that ensure its confidentiality.
- Make a list of all your cards and their numbers in case you need to report a lost or stolen card – and keep the list in a safe place.
- If your credit card is lost or stolen, notify the credit card company immediately.
- If your credit cards or other identification have been stolen, immediately report the incident to the police. Obtain an incident or report number from the police.

Debit and banking cards

As noted earlier, more than 34 million debit or banking cards are in circulation among an adult population of 21.8 million Canadians; the cards were used more than 2.4 billion times in 2002. Unlike credit cards, however, debit cards do not generally offer "zero liability" protection in the event of fraud. Indeed, some debit card agreements state that the consumer is liable for fraudulent transactions, regardless of withdrawal or credit limits on the account.[243]

[243] E.g., CIBC.

The most effective way of protecting yourself from debit card fraud is not to use a debit card at all. Stick with cash, or use a credit card, under which your liability for unauthorized transactions is limited.

- Avoid using debit cards for purchases, especially where you are not familiar with the merchant.

It is much more difficult, however, to avoid using automatic tellers, which also require the use of cards and PINs. As long as you use any sort of automated banking service with a PIN, the following precautions should be taken:

- Do not have more cards than you need.
- Keep your banking card in a safe place.
- Review the terms of service (or service agreement) applicable to the particular banking/debit card that you have. Make sure that you understand your responsibilities and liabilities, and act accordingly.
- Protect your PIN. Don't write your PIN down – memorize it – and don't disclose it. No one from a financial institution, the police or a merchant should ask for your PIN. You are the only person who should know it.
- Use your hand or body to shield your PIN when you are conducting transactions at an ABM or at the point-of-sale.
  Change your PIN if you think it may have been disclosed.
- Review your monthly bank account statements or bankbooks on a regular basis. Keep all receipts, and look for extra or missing transactions. Report any discrepancies immediately.
- After completing an ABM or point-of-sale transaction, remember to take your card and, if provided, your transaction record.
- When you select a PIN, always avoid the obvious – your name, telephone number, date of birth, address. Instead, choose a number that others who know you would not guess. You could be liable for losses if you create your PIN by using your telephone number, date of birth, address or social insurance number.
- If your card is lost, stolen or is retained by an ABM, notify your financial institution immediately. Most institutions offer 1-800 telephone numbers and/or 24-hour service for lost or stolen cards.

Computers and the online world

As discussed earlier, email, online banking and electronic commerce are experiencing dramatic growth. In addition, consumers often keep track of their finances and prepare and store their income taxes on a computer. As a result, the personal computer has become a gateway to consumers' personal information for ID thieves. According to the *Globe and Mail*, ID theft "is a crime that involves systematically harvesting scraps of personal information that people leave scattered around the Internet and on poorly

protected computers."[244] The problem is compounded with the growth of always-on high-speed Internet access.

- Close the gate. Install firewall and anti-virus software on your computer – and keep the software up-to-date. A firewall stops uninvited guests from accessing your computer. Watch for "spyware" – software that is bundled with other software to track and transmit users' online behaviour.
- Install security repairs and patches for your computer's operating system. These are available on the Web site for your operating system.
- Make sure online credit card charges are handled through a secure site or in an encrypted mode. Merchants who use secure transaction systems will advertise the fact, give you information about their system and tell you who provides it. Internet browsers generally indicate when you are using a secure Internet link. Understand how your browser functions and alerts you about secure sites. Use the most up-to-date version of your browser. Look for the "lock" icon on the browser's status bar to be sure information is secure during transmission.
- Minimize the number of password-protected services that you subscribe to.
- Before subscribing to an online service that involves the transfer of funds (e.g., online banking, investment), read the terms of service and be aware of your liability in the event of fraud. Don't subscribe unless you are comfortable taking on that risk.
- Don't use obvious passwords – words that anyone could guess – when registering for Web sites. Include numbers as well as letters in your passwords. Don't use the same password for different sites. Don't store your passwords on your computer. If you can't remember your passwords, write them on a piece of paper and keep it hidden.
- Don't use your email address as your user ID on Web sites.
- Don't respond to email requests for private information.
- Don't send private information to a link outside the business you are dealing with.
- Know whom you're dealing with. ID thieves sometimes create Web sites to capture personal information – for example, fake job postings and marketing non-existent products.
- Watch out for any Web site that asks you to send personal or financial information before disclosing an offer.
- Only shop on sites that have a privacy policy. Know how your personal information will be handled.
- Look for online seals that indicate the seller is deemed trustworthy by independent bodies such as the Better Business Bureau – but be careful. These seals can be copied and used maliciously by ID thieves as noted in the earlier discussion of eBay "spoofing".
- Avoid posting personal information on publicly accessible Web sites and online bulletin boards.
- Don't include your SIN and other sensitive personal information in online resumes.
- Try not to store sensitive personal information on a laptop computer or PDA. Laptops and PDAs are vulnerable to theft. If you do store sensitive personal information, use a

[244] "Identity thieves plunder the Net", The Globe and Mail, June 28, 2002, p. E1.

strong password to log-in – a combination of upper and lower case letters, numbers, and symbols. Consider encrypting sensitive information.
- Before disposing of a computer, delete personal information. This requires the use of "wipe" software – not just deleting files with mouse and keyboard commands.

Credit reports

Credit reports are important tools for consumers to ensure their credit information is accurate. Credit reporting agencies – also known as credit bureaus – prepare credit reports. According to Equifax, a major credit bureau:

> "A credit report is a history of how consistently you pay your financial obligations. A credit report is created when you first borrow money or apply for credit. On a regular basis, the companies that lend money or issue credit cards to you (banks, finance companies, credit unions, retailers, etc.) send the credit reporting agencies specific and factual information about their financial relationship with you – when you opened up your account, if you make your payments on time, if you miss a payment, or if you have gone over your credit limit, etc. Equifax Canada receives this information directly from the financial and retail institutions and retains it to help other lenders make decisions about granting you credit. Because your credit report contains all the information received from your lenders and provides a picture of your financial health, other lenders will request your report when they are determining whether or not to grant you a loan. Your credit report is a history that will help them determine what kind of lending risk you are – if you are likely to repay your obligation on time or not."

- Review your credit report at least annually to ensure it is accurate. Credit bureaus will provide a free credit report by mail. (It is little-known that provincial credit reporting legislation generally does not limit the number of times per year you may request your credit report free. If you are concerned there has been a compromise of your personal information you should check your credit report more frequently). They also provide online access to credit reports for a fee. Look for errors, including evidence of ID theft – for example, credit card and bank accounts that you did not open and NSF cheques that you did not issue. The credit report will show who has requested your credit report and when for three years. Contact the credit bureaus to correct errors.
- The three national credit bureaus are Equifax, Trans Union of Canada Inc. (Trans Union) and Northern Credit Bureaus Inc. (Northern).[245] Equifax's toll-free voice number is 1-800-465-7166; the company's Web site is www.equifax.ca. Trans Union's toll-free voice number is 1-866-525-0262; the company's Web site is www.tuc.ca. Northern has a toll-free fax number 1-800-646-5876; the company's Web site is www.creditbureau.ca. Northern's address is 336 Rideau Boulevard, Rouyn-Noranda, QC J9X 1P2.

[245] Northern has 22.9 million credit files for all of Canada (www.creditbureau.ca).

- Obtain your credit report from each bureau because they may have different information.

Other tips

- Before you reveal any personal information, find out how it will be used and if it will be shared.
- If the envelope containing new cheques from your bank has been tampered with, contact your branch right away.
- If your cheques are stolen, notify your bank to close your account.
- Secure personal information in your home if you have roommates, employ outside help or are having service work done in your home.
- Keep your purse, wallet or PDA in a safe place at work.
- If your driver's licence is lost or stolen, contact your local driver and vehicle licence office and report the incident to the police.
- At the time you move, be sure to notify and complete proper change of address notifications for all government agencies, creditors and other important correspondents, giving effective dates.
- If you're an important person or an aspiring important person, try to minimize the personal information included in "who's who" and other directories. These directories often include the birth names of spouses and mothers, employment histories, and other information used in granting credit, providing services, and issuing government documents. This information can be the starting point for an ID thief before he or she trolls the Internet and other sources for bits and pieces of personal information to complete an ID theft.
- The Government of Canada has a Web site {http://canada.gc.ca/cdns/wallet/wallet_e.html} that helps you find out how to apply for or replace government identification cards, including SIN cards, passports and provincial cards such as birth certificates, health cards, and drivers' licences.

APPENDIX C - WHAT TO DO IF YOU ARE AN IDENTITY THEFT VICTIM

Consumers who are ID theft victims face an average loss of over $1,000. A consumer will also likely incur costs to deal with the damage to their accounts and reputations – for example, notaries and faxes. Non-monetary harm is also a major problem – for example, the denial of credit and other financial services and the time lost to resolve problems. Victims also report being harassed by collection agencies and retailers over bad cheques. Other victims experience difficulty obtaining housing due to the perpetrator's eviction history. Arrest warrants have been issued for some victims based on a perpetrator's speeding tickets. What can a consumer do to clear his or her name?

As soon as you know or suspect that you are an ID theft victim, contact the credit bureaus. Your goal is to stop the perpetrator from opening new accounts and to correct your credit reports if the perpetrator has damaged your credit record.

A consumer must act quickly upon learning that he or she is the victim of credit identity theft. Acting quickly will help prevent the thief from making further use of the victim's credit identity, and may make the process of restoring the victim's credit standing less burdensome.

> "Unlike victims of other crimes, who generally are treated with respect and sympathy, identity theft victims often find themselves having to prove that they're victims, too – not deadbeats trying to get out of paying bad debts." US Federal Trade Commission report.

A victim should keep a log of the date, time and substance of all personal and telephone conversations regarding the theft. The log also should include the name, title and telephone number of each person to whom the victim speaks. The victim should follow up each telephone call with a letter that confirms the conversation and any agreed upon action. The victim should send all correspondence by registered mail, return receipt requested, and keep a copy of each letter and each return receipt.

Credit bureaus

Request a copy of your credit report from each credit bureau. Check each credit report carefully. Look for accounts that you have not applied for or opened, charges that you have not incurred, inquiries that you have not initiated, and defaults and delinquencies that you have not caused. Check your identifying information carefully – particularly your name, address and SIN.

If you think that you have been a victim of ID theft, ask the credit bureau to put a "fraud alert" on your file. This will alert credit grantors who check your credit file to the possibility that the person claiming to be you is not you. The credit grantors will then take extra precautions to verify that the person requesting credit is in fact you.

Request each credit bureau to remove all information that appears in your credit report as a result of the theft of your personal identification and credit information. It may take

some time to have all of this erroneous information removed from each of your credit reports. Obtain copies of your corrected credit reports.

If you have a police report, send copies to the credit bureaus. A police report may also be useful in dealing with credit grantors.

Affidavits

Be prepared to complete affidavits to establish your innocence with banks, credit bureaus, credit grantors, and recipients of bad cheques. A centralized affidavit service for ID theft victims does not yet exist in Canada.

Credit cards

Call each of your credit card issuers to report that you are the victim of ID theft. Ask each credit card issuer to cancel your card and provide a replacement card with a new account number. Immediately follow up each telephone call with a letter that confirms the conversation and the action that the credit card issuer has agreed to take.

Ask each credit card issuer about the status of your account. Ask if the card issuer has received a change of address request, or a request for additional or replacement credit cards. If you have not filed a change of address request or requested additional credit cards, instruct the card issuer not to honor these requests.

Call each credit card issuer or creditor that has opened a new account that you did not authorize or apply for. These accounts probably will be listed in your credit reports. Explain that you are an ID theft victim, and ask each issuer and creditor to close the account immediately. Some credit card issuers and creditors may ask you to sign an affidavit or to submit a copy of the police report on the theft of your personal identification information. Ask each issuer and creditor to inform each credit bureau that the account was opened fraudulently and has been closed.

With respect to credit grantors who will not dismiss debts, attempt to obtain the paperwork from them that proves you did not make the transactions. Provide an affidavit and, if available, a copy of the police report. Once a credit grantor has dismissed your debt, obtain a letter from the credit grantor that they have closed the disputed accounts and have discharged you of the fraudulent debts. This letter will be useful in dealing with credit bureaus and debt collectors. It is also helpful if errors reappear or your personal information is recirculated for fraudulent purposes.

Banks

If your bank account information or checks have been stolen, or if a fraudulent bank account has been opened using your identification, notify the bank. Close your checking and savings accounts and obtain new account numbers. Ask the bank to use a new unique identifier for your accounts. Do not use your mother's maiden name, since this information is often available in public records. Call the payees of any outstanding checks that you have written. Explain to each payee that you are an ID theft victim and that you have closed your checking account for that reason. Ask each payee to waive any late payment or returned check fee. Then send each payee a replacement check drawn on your new account and stop payment on the check that it replaces. It's a good idea to enclose a note with each check explaining why you are sending a replacement check and reminding the payee that the payee has agreed to waive the late payment or returned check fee if the payee has agreed to do so. Get a new ATM card and PIN. Do not use your old password or PIN.

Utilities

Notify your gas, electric, and water utilities that you are the victim of ID theft, and alert them to the possibility that the thief may try to establish accounts using your identification information. Provide similar notice to your local, long distance and cellular telephone services. Ask the utility and telephone services to use a new unique identifier for your accounts. If your long distance calling card or PIN have been stolen, cancel them and obtain a new account number and PIN.

Government identification cards

The Government of Canada has a Web site {http://canada.gc.ca/cdns/wallet/wallet_e.html} that helps you find out how to apply for or replace government identification cards, including SIN cards, passports and provincial cards such as birth certificates, health cards, and driver’s licences.

You must report the loss or theft of your Social Insurance Number card to the police and obtain a copy of the police report that will indicate your card has been lost or stolen. Request a replacement card or a new Social Insurance Number from HRDC.