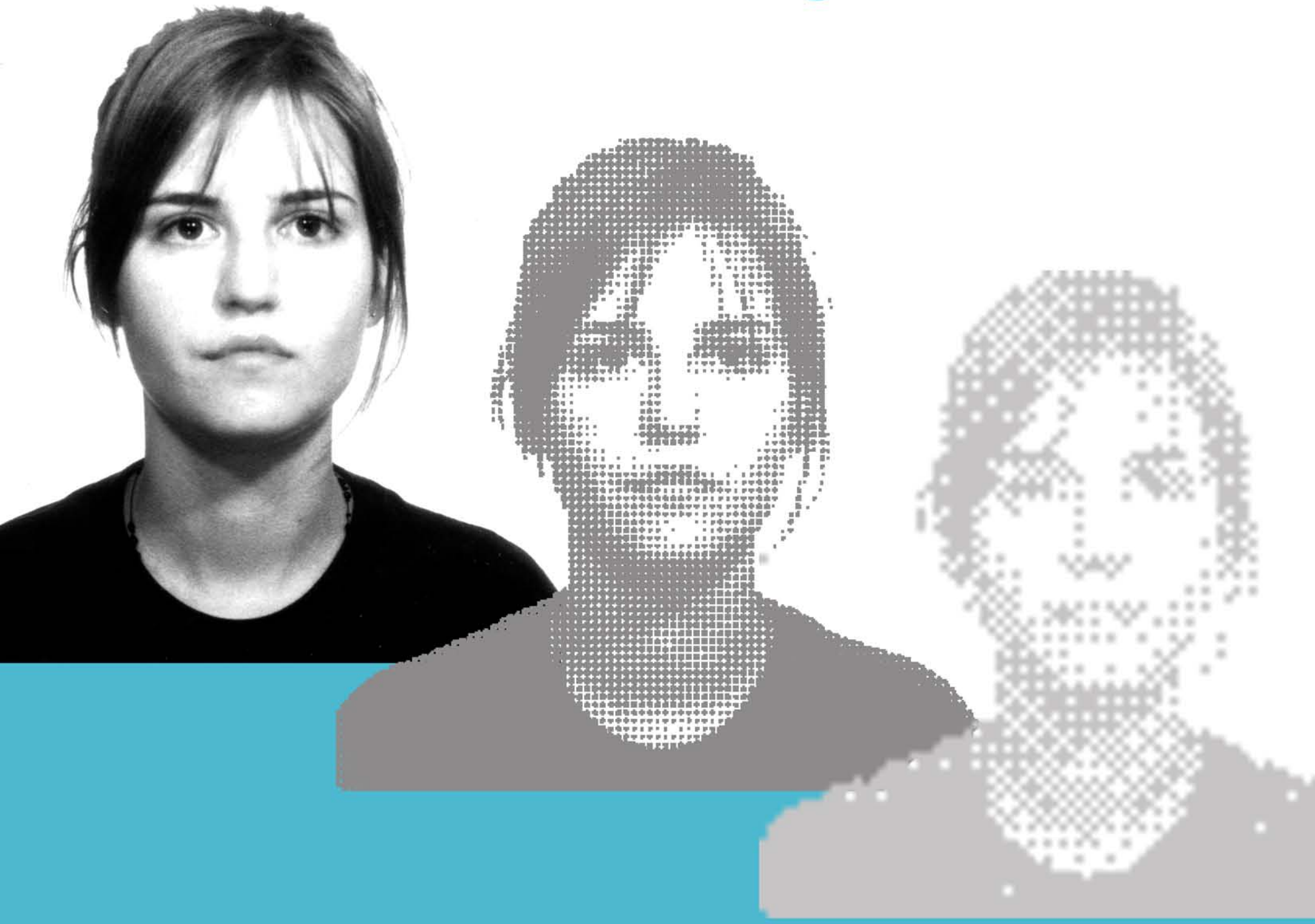
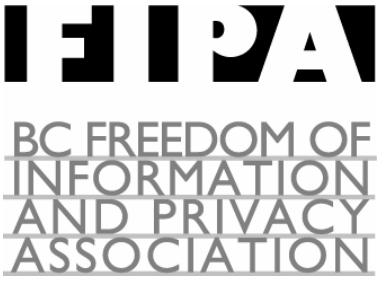
PIPEDA and Identity Theft



Solutions for Protecting Canadians

FIPA
BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION



PIPEDA and Identity Theft: Solutions for Protecting Canadians

This research report was funded by a generous grant from the Office of the Privacy Commissioner of Canada, under the Contributions program launched in 2004

April 30, 2005

The following people played key roles in this research project:

Darrell Evans, Executive Director BCFIPA	Administrator
Stephanie Perrin, Digital Discretion	Research Project leader
Philippa Lawson, Director, Canadian Internet and Public Policy Initiatives Centre	Researcher
Jennifer Manning, CIPPIC intern	Researcher
Leila Pourtavaf	Research Assistant
Robert Gellman, in association with Digital Discretion	Researcher

The following individuals kindly agreed to interviews and discussions about the topic:

Beth Givens	Privacy Rights Clearinghouse
Chris Hoofnagle	EPIC
Daniel Solove	Georgetown Law School, author of Digital Persona
Tom Oscherwitz	ID Analytics, former legislative Counsel to Senator Diane Feinstein
Peter Cassidy	Anti Phishing Working Group

All errors are my own.

Stephanie Perrin, Principal Researcher

FIPA wishes to gratefully acknowledge the Law Foundation of British Columbia for their ongoing support of FIPA's activities in the areas of law reform, research and public education

---

103 - 1093 West Broadway, Vancouver, BC V6H 1E2
Ph: 604-739-9788 • Fax: 604-739-9148 •
Email: info@fipa.bc.ca • Web: www.fipa.bc.ca

PIPEDA and Identity Theft: Solutions for Protecting Canadians

Introduction

When the B.C. Freedom of Information and Privacy Association applied for this grant in the summer of 2004, ID theft was a hot issue. Since then, it has exploded.

There has been a flurry of activity in Canada and the United States, as regulators and companies alike struggle to keep up with the rapid growth in this white collar crime. Consequently, while the research has progressed, it has been a constant struggle to keep up with the fast-breaking news events and the subsequent policy and legislative responses of governments. We have focused on providing advice and analysis on how to protect the rights of the individual, through the use of existing law, policy, standards, and management practices.

During 2004-2005, the following key developments took place, and are briefly summarized in this report:

1. The Bi-national Working Group on Cross-Border Mass Marketing Fraud released *A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States*, in October 2004.[1] The report made numerous recommendations. A federal/provincial/territorial Council on Identity is tasked with drafting and Identity Policy Framework, and is chaired by Foreign Affairs Canada.
2. Justice Canada released a consultation document seeking input on possible changes to the Criminal Code and other legislation, to stiffen penalties for the possession of documents which contribute to ID theft, and facilitate prosecution of the criminals.
3. A flurry of legislation was proposed in Congress and at the State level in the US, to respond to the scandal surrounding a number of leaks of data, and the successful operations of a criminal ring which purchased information on the open market from ChoicePoint and used it to perpetrate ID theft on a grand scale.
4. A routine arrest by Edmonton police resulted in them finding bags of ID documents, which they turned over to the Alberta Privacy Commissioner. Commissioner Work conducted the first major investigation of such criminal activity under the new private sector privacy legislation.[2]

In particular, the ChoicePoint scandal has precipitated a rethinking of the lax attitude which has prevailed concerning the free availability of identity information, especially in

[1] http://www.psepc.gc.ca/publications/policing/identity_theft_e.asp
[2] http://www.oipc.ab.ca/ims/client/upload/NR_P2005_IR_00123.pdf

the United States. Because Canadian data overwhelmingly flows to the United States, this is of key interest to us and we will devote some time to it in this report. Attempts to fill the legislative gaps that exist in the US with respect to data protection have yielded innumerable fine-grained regulatory approaches to ID theft. In Canada many issues have been solved through our privacy laws, but it is worthwhile sifting through these proposals for fresh ideas.

1. Background and History

In May 1997, the principal investigator met Beth Givens, founder of the Privacy Rights Clearinghouse and one of the pioneers in the field of ID theft and of providing assistance to victims. Despite the fact that this was a growing problem with credit issuance at the time, Beth Givens was struggling to get the issue on the agenda of the US Government and Credit grantors. A brief look at this history, the slow development of regulatory response, and the abandonment of individual victims and their need to have some control over the use of their very identity helps put this whole project in some perspective.

In 1992, Beth Givens had started a small consumer complaints office in San Diego, California. Funded originally by fines levied on a telecommunications company that had not lived up to its terms of service, the office of Privacy Rights Clearinghouse was staffed by two people. Sometime in 1993, she started hearing from consumers about complaints that were different; instead of the usual credit card fraud from a lost or stolen wallet, consumers were complaining that someone had opened up accounts in their names, but they had not lost their cards or documents. She investigated, discovered a newspaper article that dubbed the phenomenon "Identity Theft", and started using the term. The name has stuck, and the problem has become enormous. Not only has a large proportion of the Privacy Rights Clearinghouse's business become assisting consumers to deal with identity theft, they have trained victims who have opened up their own consumer assistance centres (see http://www.idtheftcenter.org/index.shtml).

Governments and business were slow to respond to this new problem. Firstly, most victims did not find out their identities had been stolen until they applied for credit or tried to get a mortgage. Then they would discover they had a bad credit report, and often big debts they had not incurred. Proving you are not the one who has incurred a bill is a difficult job at the best of times. Companies were anxious to get their money, and not inclined to help victims once it had been established that the individual was not at fault. In the early years, it was very difficult just to get fraud alerts put on credit reports, to stop new accounts being opened by the thief. Thieves went from state to state, complicating prosecution. Although the Privacy Rights Clearing House early on had put out a number of excellent publications and fact sheets to educate consumers and help walk them through the process, the government had not moved to help and the public education was focussed on what consumers could do to protect themselves, not what business could do to stop the spread of ID theft.

The problem has grown, aided by the Internet and the fact that so few individuals are ever charged and convicted of ID theft. It has become the perfect non-violent yet highly lucrative crime. The Los Angeles and San Diego police report that fewer than 5% of cases that cross their desks are even investigated. Although the situation has been much less serious in Canada than in the United States over the past decade, we are catching up.

Phonebusters, the centre run by the Ontario Provincial Police, the RCMP, and the Competition bureau to combat telemarketing fraud, was set up in 1993. Recently, it has been receiving complaints about ID theft, and is now set up to collect statistics and assist victims by providing a 12 page victim statement to send to all creditors. The most recent statistics on their website show complaints rose from 8187 in 2002 to 13359.in 2003; this compares to 653,000 reports to the Federal Trade Commission reporting centre.

Both in the US and Canada, governments have stepped in to deal with the problem. The US Federal Trade Commission has set up an ID theft resource centre at http://www.consumer.gov/idtheft/. They provide victim affidavits for download, and have prepared guidance for businesses when they realize there has been a breach of the confidentiality of customer information. There is a model letter for notifying consumers of a breach, and a publication on ID theft and how to watch for it to send to individual consumers they notify. Action was required pursuant to the changes in the Fair Credit Reporting Legislation of 2003, and amended guidance takes effect May 2 2005.[3] With all this activity, is there a need for more action? We think so, and the following chapters detail what could be done.

[3] http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/05-8376.htm

2. The Current Crisis and Response

ID Theft Stats Report: the Scope of the Problem

Identity theft is the misappropriation and unauthorized use of an individual's identity in order to gain some advantage (usually financial) by deception. Differences in the definition of Identity Theft have confused the reporting and statistics, because normal fraud such as credit card fraud or cell phone fraud has sometimes been counted with instances of true identity theft, where a victim's identity has been stolen by the perpetrator to start new accounts or cover their tracks. We will attempt in this report at least to distinguish between the two by talking about appropriation of existing accounts (e.g. using credit cards in a stolen wallet until they bounce) as theft or fraud, and preserve the term ID theft for the more concerted efforts to become the target individual through misappropriation and use of ID documents and credentials. There is an enormous difference in the impact on victims; fraud is usually covered by the credit card company, or in the case of debit card fraud, is detected and the cards cancelled. When an individual persists in impersonating a victim and opening new accounts in their name, sometimes the only suggestion authorities have been able to offer is for the real person to change her name. That is certainly a theft of your identity.

Canada

In 2003, PhoneBusters received 13,359 identity theft-related complaints from Canadians, reflecting reported losses of more than CAN$21.5 million. This is an increase from the 8187 complaints received by PhoneBusters in 2002, which cost over CAN$11.7 million. Statistics gathered by PhoneBusters in 2003 and the first half of 2004 indicate the largest number of complaints about identity theft relate to credit cards or false application for a credit card (32 percent) and cell phones or false application for a cell phone (10-12 percent).[4]

2003		
PROVINCES	**VICTIMS**	**$ LOSS**
ON	5772	$12,682,218.64
BC	1829	$1,808,318.45

[4] www.phonebusters.com

AB	1079	$1,282,716.71
MB	195	$194,718.93
SK	202	$687,992.85
UNKNOWN	34	$5,640.02
NB	200	$261,206.11
NS	223	$273,347.29
NF	94	$115,993.06
PE	14	$2,150.00
NT	2	$0
QC	3711	$4,246,801.90
YT	2	$0
NU	2	$3000
TOTALS	**13359**	**$21,564,103.96**

In a Fraud Awareness study commissioned by Industry Canada and conducted by The Strategic Counsel in March 2003, 15% of respondents said that they had been victims of identity theft.5 Identity theft was defined as "the unauthorized collection and use of personal identification, such as name, date of birth, address, credit card information, or social insurance number."6 84% responded that they had never been victims of identity theft. 751 respondents were interviewed across 5 regions (Atlantic, Ontario, Manitoba/ Saskatchewan, Alberta and British Columbia.) The sample was weighted to reflect the actual distribution by sex and age within the regions, resulting in a weighted sample of 756.7 The objective of the survey was to establish a benchmark for incidence, concern and awareness of telemarketing fraud, identity theft, as well as awareness of fraud prevention campaigns and awareness of PhoneBusters.

Of the respondents that have been victimized by identity theft, 24% responded that they didn't take any action to resolve the incident. Those that did take action either complained to the police or to their credit card company. Interestingly, none of the

[5] The Strategic Counsel, "Fraud Awareness Study: A Report to Industry Canada, Competition Bureau." (March 2003) [unpublished].
[6] *Ibid.* at page 32. Please note, we find this definition to be too broad to be useful.
[7] According to the survey, a weighted sample has a margin of error of +/- 3.6 percentage points, 19 times out of 20.

victims contacted any of Canada's major credit agencies (Equifax, Experian and TransUnion). Only 32% of those surveyed were aware of organizations that deal with identity theft. Out of the 15% of respondents that have been victims of identity theft, 4% of thefts occurred in the last 6 months, 2% occurred between 6 and 12 months ago, 3% occurred between 12 and 18 months ago, and 6% occurred over two years ago.

In a 2002 survey conducted for Industry Canada by Environics Research Group Limited, 3% of respondents had been a victim of identity theft in the last 12 months.[8] Identity theft was defined in the study as occurring when an individual's personal information, such as their name, social insurance number, driver's license, debit card or other identifying information is used without permission to commit fraud or other crimes. The survey consisted of 2,002 respondents from across Canada; 247 were from the Atlantic Provinces, 500 from Quebec, 563 from Ontario, 464 from the Prairie provinces and 228 were from British Columbia. From this sample, 66 respondents reported that they had been victims of identity theft.

The 66 respondents who had been victims of identity theft experienced it in a variety of different ways:[9]

- 39 experienced charges on their credit card,
- 13 noticed withdrawals from their bank account,
- 12 had their card or card number stolen
- 8 had their computer hacked or stolen
- 6 had stolen cheques cashed on their accounts
- 4 had their health care card number used
- 2 had a loan or line of credit set up in their name

When asked how they thought the identity thief got their personal information:

- 21 cited lost or stolen identity documents
- 17 cited information obtained during an electronic financial transaction
- 12 cited theft from a computer or PDA (handheld computer)
- 7 cited theft from a company database
- 7 cited their mail being stolen or redirected
- 5 cited being tricked into some sort of scam (fake website, fake survey etc…)
- 2 cited a friend or relative misusing their account

When asked how they found out their identity was stolen:

- 18 found unauthorized charges on their account
- 13 were notified by the company where the fraud or theft occurred
- 11 were notified by their bank
- 10 lost money
- 8 were called by a credit card company

[8] Environics Research Group Limited, "Focus Canada Report 2003-4"
[9] Victims may have experienced identity theft in more than one way, bringing the number to over 66.

- 5 received a letter from Revenue Canada
- 4 were called by the Police Department
- 3 were notified in the mail
- 3 noticed unauthorized transactions on their utility bills
- 3 were called by a collection agency
- 2 noticed their mail stopped arriving

What remains unclear from this survey is what methods the identity thieves used to steal the victims' personal and financial information. A breakdown of how many obtained the information through dumpster diving, spyware programs, phishing etc would be helpful. Equifax and Trans Union, the two major Canadian credit bureaus, indicate that they receive approximately 1400 to 1800 Canadian identity theft complaints per month.[10] The Canadian Council of Better Business Bureaus estimates consumers, banks, credit card firms, stores and other businesses lost CAN$2.5 billion to the perpetrators of identity theft in 2002.

United States

The FTC reports that from January-December 2003, Consumer Sentinel (the complaint database the FTC maintains) received 542,378 consumer fraud and identity theft complaints.[11] 323, 611 were identity theft-related. Of those, 66% (214, 905) were complaints, while 33% (108, 706) were requests for information, and 214, 905 were identity theft reports. 33% of identity theft victims reported that identity thieves used their information for credit card fraud. 16% reported that their identifying information was used for fraud in ordering phone service.
For 2004, the calls went up to 635, 173, of which 39% related to ID theft, and 246,570 were actual reported cases.

Harris Interactive conducted a Privacy and American Business survey[12] from May 19 to 27, 2003. The survey defined identity theft 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. 3,462 adults were interviewed. 16% responded that they were victims of ID theft. The survey found that some common reasons for committing identity theft are: financial gain, to obtain publicly-funded benefits or services to which they would not otherwise be entitled, and to hide from law enforcement.

In 2003, the Federal Trade Commission sponsored a survey conducted by Synovate published in September 2003.[13] 4,057 adults were interviewed, chosen using a random digit dialling service. 4.6% of those surveyed said that their personal information had been misused in some kind of fraud over the last year. Within that 4.6%, 1.5% represents victims who had their personal information misused to open new credit accounts, new

[10] *Supra* note 1.
[11] http://www.consumer.gov/sentinel/pubs/Top10Fraud2003.pdf
[12] Harris Interactive, "Identity Theft New Survey and Trend Report" (August 2003) [unpublished]. Available online at http://www.bbbonline.org/idtheft/IDTheftSrvyAug03.pdf
[13] http://www.ftc.gov/os/2003/09/synovatereport.pdf

loans, new telephone accounts and other fraud. 2.4% represents victims who had their information misused to commit fraud using their existing credit cards.

The amount of time victims spent resolving their claims was influenced by the type of fraud committed. Overall, victims spent approximately 30 hours resolving their claim, while victims of identity theft committed through "new accounts and other fraud" spent approximately 60 hours.

The information was used for financial gain, such as opening new credit accounts or taking out loans. It was also used to obtain medical care or rent an apartment. Only 25% of the victims in the survey reported the crime to the police. Only 22% reported the crime to one or more major credit agencies. 26% of victims knew who had misused their personal information. Of those, 35% reported that the perpetrator was a close friend or family member.

Judith Collins, director of Identity Theft Partnerships in Prevention program at Michigan State University, randomly selected 1,037 cases from around the country. She found that employees were responsible for stealing the victim's identity in 50 percent of the cases. Most cases involved temporary workers, often in health care or financial companies.[14]

The Ponemon Institute conducted an Identity Management Survey from September 7-30, 2004.[15] The surveys were based on 1,041 adults from across the United States.[16] The survey found that more than 70% of respondents would disclose personal information such as their name, phone number or account number, or would answer security questions in response to unsolicited phone calls or e-mails. 61% of respondents did not want to change their passwords periodically, even if such a practice would enhance their security. 57% of consumers did not want their accounts locked down after three failed attempts to provide identification verification information.

According to the Identity Management Survey, most consumers do not appear to be interested in being slightly inconvenienced for the sake of protecting their identity and personal information. Many (69%) are open to other forms of identity verification, such as biometrics. 84% are interested in voice recognition as better methods of biometric identification due to speed and convenience. Approximately 75% of consumers are of the view that a single secure and private identification credential issued by a trusted organization would ensure convenience in establishing their identity in multiple contexts. No survey has followed up this observation by testing individuals' understanding of how such a credential would be issued and protected, but many security experts believe such a card would compound, not ameliorate, the problem.[17]

---

[14] http://www.msnbc.msn.com/id/5015565/. (Note: Judith Collins has been contacted for a copy of her report).

[15] The survey was commissioned by EDS and the International Association of Privacy Professionals (IAPP). A copy of the survey can be accessed at http://www.eds.com/services/innovation/downloads/privacy_survey.pdf

[17] see Bruce Schneier and Stefan Brands, www.idcorner.org

Phishing Statistics

Phishing, a relatively new but fast growing phenomenon, involves duping internet users into providing passcodes or credit card information which is then used for fraud or ID theft. It is perpetrated either through email or website spoofing; further details of techniques will be explored in the next section. The average monthly growth rate in the number of phishing attacks (measured by counting new bogus websites) is an alarming 28%. The Antiphishing working group provides detailed monthly reports at www.antiphishing.org.

It is hard to glean from all of these disparate surveys and metrics exercises exactly what is happening except that numbers of victims are going up. Particularly alarming is the rise in fraud perpetrated on the internet, because the phishing and spam phenomena are bound to shake the confidence of users in doing business, banking, and government activities over the Internet. Governments have recognized that this could be a wall-hitting experience for the burgeoning digital economy, and are turning their attention to the challenge.

3. Methods of Identity Theft

Techniques Used by Identity Thieves

Identity thieves use a variety of techniques to steal identity or use someone else's credentials. Some involve stealing personal information or misusing information in their custody or control, in order to pose as the individual whose information is targeted. Simple fraud, such as using a credit card or bank card that is found or stolen, is often labelled as identity theft, although this kind of fraud has existed for decades and rarely threatens the identity of the person concerned. Credit card companies have for many years limited liability in such instances to $50, so while fraud rates are high and push up the cost of credit, individual consumers have not felt the pinch. Debit card fraud is more problematic because there is technically no limit to consumer liability, but banks have not enforced this systematically. If more consumers were actually aware of their liability in Internet banking, they might not do it.[18] One of the societal dangers in unchecked identity theft, is an exodus from e-commerce and the productivity increases we could gain from it.

Other techniques involve creating new identities, taking over a person's identity by changing address information on existing accounts, or opening new accounts and loans. To do this, ID thieves use stolen personal information, stolen cards and identity documents, or passwords and information necessary for security controls. The two types of ID theft should be distinguished, and for the purposes of this report we shall refer to simple fraud as fraud or theft (e.g. using a credit card, emptying an account through a debit card, or using an individual's online account to order something and deliver it to the thief's address. We shall reserve the term ID theft for situations where an individual takes over the identity of the person to open new accounts, an activity which creates real problems for the honest individual to substantiate their own identity.

Part of the reason for the confusion in reporting, is that in order to do either, thieves may use any of the following methods:

- Using cards and documents in lost or stolen wallets, or home safes
- Using personal information found in computers, Personal Data Assistants (PDAs), phones
- Setting up fake ATM terminals
- Installing surveillance devices to intercept passwords and the digital stream from bank cards and credit cards
- Setting up fake websites on the internet, and encouraging individuals through e-mail to visit the site and login with their login ID and passwords (Phishing).

[18] See Foundation for Information Policy Research, a paper on the risk of fraud in e-commerce (www.FIPR.org, E-Commerce, Who Carries the Risk of Fraud? Linking to http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/bohm/)

- Calling people on the telephone and encouraging them to provide personal information (sometimes referred to as "social engineering").
- Gathering information from discarded documents in personal garbage, or in garbage from business
- Corrupting employees with insider access to information
- Purchasing personal information on the black market
- Purchasing personal information on the open market
- Counterfeiting cards, ID documents, or other legal documents
- Redirecting mail, either through contacting the companies, putting in fake change of address cards at the post office, or stealing apartment and multiple mailbox keys

Examples of ID Theft Techniques

1) Physical Theft of ID Documents and Credentials

For years fraudsters have stolen purses or wallets, using the credit cards in them. Mail theft went on in individual mailboxes, and when runs of quantities of cards arrived for sorting. Credit card companies limit consumer liability to $50, but usually waive this fee if the loss is reported immediately. Phone lines to report lost or stolen cards are one of the rare instances of excellent customer service, as they operate on a 24 hour basis and can be found in local phone books around the world, usually with a toll free number. Theft of cards for the purposes of ID theft is more problematic, because thieves are now smart enough not to use the cards, but rather to wait and use documents found in the wallet as credentials when opening new accounts.

Since much ID theft, sadly, takes place within closed or trusted groups (the family, the workplace) some lost documents do not get reported as stolen. Solutions to the problem must accommodate the fact that being alert to strangers may not be sufficient.

2) Dumpster Diving

Some identity thieves, known as "dumpster divers," will rummage through trash to pick out bank and credit card statements, looking for pre-approved credit cards, bank statements, void cheques or any other form of identifying documents. There is a street market for such items as valid credit cards with expiration dates, taken from imprints or carbon papers. Credit card companies have attempted to keep up, by getting rid of the carbon paper that used to be in card receipts and removing the centre numbers from credit card slips. Older systems do not yet do this, however. Simple credit card fraud is different from identity theft though, and documents gathered for the purposes of creating duplicate or composite identities could include all kinds of personal information that individuals might toss away without thinking. Shredding documents with a simple and inexpensive cross cut shredder solves this problem for individuals, companies need larger volume systems.

Various marketing practices aggravate this problem, notably the practice of sending "convenience cheques" drawn on credit cards, to pay off unpaid balances on other cards, and sending pre-approved credit applications in the mail.

3) Debit and Credit Card Fraud

Credit card fraud takes many forms:

- Lost and stolen cards are used before they are reported and frozen
- Numbers are obtained with expiration dates and used for phone or online purchases
- Vendors themselves add fictitious charges, or increase the amount when they print the credit card slip, from what the bill said.
- New cards are made by capturing electronic information from the card, as well as the required imprint.

Debit card fraud requires a Personal Identification Number (PIN number) and a card, so the above methods for manufacturing a card or using a stolen one only work if the pin can be obtained. The same applies to telephone card fraud. By installing a fake ATM device that reads the card's encoded data, or by distracting a customer and swiping the card through the thief's own reader hooked to a database, the information required for the card to be counterfeited can be obtained. Sometimes cards are switched and the individual does not notice; once the customer is out the door it does not take long to counterfeit the card.

Skimming is the term used to describe making an illegal copy of a credit or bank card when the original was being used correctly. A typical skimming method involves using a reader that reads and stores all the information that the original card contains. Some consumers have a policy of never allowing a card to be out of sight. There have been instances in the United States where organized crime has blackmailed or threatened restaurant staff to swipe cards through their readers, so this may be a useful tip for consumers to always keep their cards within view or control.

4) PIN Number Theft: Shoulder Surfing (credit/debit/telephone card fraud)

Shoulder surfing occurs when thieves look over the victim's shoulder or from a nearby location as the individual enters a PIN at an ATM machine, debit card reader, or telephone. Sometimes thieves use cameras to capture PINs from up close or at a distance. Thieves can then use the PIN to drain the bank account or run up purchases without the account holder's knowledge. When PIN numbers are typed into telephones, audible tones can be captured by sensitive recording equipment, a technique sometimes used at airport pay phones, for instance, where customers are frequently using long distance cards. Wherever credit or telephone card numbers must be typed in rather than swiped, there is additional risk.

Intercepting the digital stream to get the card's electronic data and the PIN requires some kind of wiretap, usually involving insider abuse.

5) Phishing

Phishing is a new term to describe the act of sending an email falsely claiming to be from a legitimate institution in order to convince the individual to divulge personal information that can be used to commit fraud (usually credit card fraud or internet banking scams). Sometimes the personal information is used to steal the identity and commit fraud in the name of that individual. The emails often direct the user to a fake website, set up only to capture information. Phishing is remarkably successful, and sometimes the sites are only up for a matter of hours or minutes, making it really difficult to investigate the perpetrators.[19]

Spoofing is one element of phishing. Spoofing is an old hacking technique where individuals send email with forged headers, to create the illusion the email originated at another location, usually a legitimate enterprise (like a bank or online store). Email spoofing has gone on for years, but is now being used by organized crime to hide the traces of how identity theft is taking place through Phishing attacks. Spoofing refers to the switching of the headers, not the content of the email itself. The immediate victim is the organization whose email address has been spoofed, not the individual. If the attack successfully fools the individual into giving up their personal information, they are the second victim.

In January 2005, spoofed emails began to appear after the tsunami disaster in December 2004. The emails ask for relief for victims of the disaster, and direct the user to a fake website where they can send donations online.

Companies that have been subject to recent phishing attacks are mostly large institutions with strong trademarks.[20] For example, on November 17, 2004 Citibank customers received an email which stated that Citibank© is currently performing regular maintenance of their security measures. The individual was told that his account was randomly selected for maintenance, and placed on Hold status. Customers were supposed to reset their passwords by entering the correct account information or by answering some personal security questions.

A common phishing attack asks customers to verify their account information, such as the email that eBay customers received on November 19, 2004. Customers received an email saying that their account had been suspended due to a violation of a policy of the site, by falsifying or omitting their name, address and telephone number.[21] Users were asked to verify that information in order to have their account considered for reinstatement.

Security companies have been tracking phishing attacks as they occur. For instance, on February 21, 2005 Secunia reported a flaw in Microsoft's Internet Explorer (IE6) and

[19] see http://www.wwwcoder.com/main/parentid/472/site/4692/266/default.aspx
[20] Companies that have recently been the victims of phishing attacks include Citibank, Sun Trust, eBay, PayPal, Sovereign Bank, AmericaOnline, Earthlink, Washington Mutual and BankOne. For a list of recent phishing attacks, see the Anti-Phishing Working Group, www.antiphishing.org
[21] http://www.antiphishing.org/phishing_archive/11-18-04_Ebay/11-18-04_Ebay.html

Windows XP SP2 that would allow fraudsters to launch phishing attacks through pop-up boxes which appear over long URLs.[22] The weakness has been confirmed even in fully patched systems, so the only solution is not to enter sensitive information in pop-up boxes. These constantly evolving Internet threats are hard for the average consumer to follow with any degree of confidence.

Canadian companies are not immune to phishing attacks. On December 13, 2004, the Canadian Internet Registration Authority (CIRA) warned dot.ca registrants not to respond to emails requesting verification of account information. An unidentified user was sending false emails that requested user names and passwords in order to verify account information and prevent domain name suspension.[23]

In June 2004, Royal Bank of Canada notified customers that fraudulent emails purporting to originate from the Royal Bank were being sent out asking customers to verify account numbers and personal identification numbers (PINs) through a link included in the email. The fraudulent email stated that if the receiver did not click on the link and key in their client card number and pass code, access to their account would be blocked. These emails were sent within a week of a computer malfunction that prevented customer accounts from being updated.[24]

According to a recent study by the Anti-Phishing Working Group conducted between August and November, 2004, financial services remains the most targeted industry sector for phishing attack (approximately 75% of hijacked brands were from financial institutions). ISPs were the second most hijacked brand (such as Earthlink and American Online), comprising approximately 16% of brands hijacked in November 2004.[25]

6) Pharming

Pharming is a new term used to describe the establishment of realistic fake websites which trap unwary consumers into providing personal information. The practice of grabbing common misspellings as domain names has been in use for many years by the pornography industry, to trap people onto porn sites when they are searching for other sites. Recent examples include “Gooogle.com” instead of “Google”. While large companies might be well advised to register all common misspellings of their names, this is prohibitively expensive for small business, and the domain name registry business is reluctant to take on the task of policing this. Since the thieves are usually gone quickly once they have made a reasonable take, and the domain abandoned, it is not clear how this problem could be solved.

[22] http://secunia.com/advisories/14335/
[23] A copy of the email can be found at http://www.cira.ca/news-releases/139-1.html
[24] http://www.psepc-sppcc.gc.ca/publications/policing/identity_theft_e.asp
[25] The Retail industry was third, ranging from 6-7% of hijacked brands between August and November. “Miscellaneous” brands made up between 0 and 7%. A copy of the results can be found at http://www.antiphishing.org/APWG%20Phishing%20Activity%20Report%20-%20November%202004.pdf

Phishing and Pharming Statistics

Redirection techniques used by pharmers are detailed at the Anti-phishing Working Group website at www.antiphishing.org. The APWG is a group of companies that have banded together to combat Phishing and Pharming. It is difficult for companies individually to come forward and discuss the problem, because the most proactive companies will be the ones to frighten consumers. There is safety in numbers, and the group have done good work in pooling information on the actual attacks they are suffering, and working to go after the perpetrators. There are substantial numbers now: the group's March 2005 survey shows an average monthly climb in the number of attacks since July 2004 as 28%. Seventy-eight brands were hit in March, and the average site is up for 5.8 days before it is detected and removed. The number of phishing attacks reported to the APWG has jumped from 28 reports in November 2003 to 1,125 a month in April 2004, and 2870 in March 2005.

A study conducted by Gartner Research Group of 5,000 adult internet users found that 3% had provided their personal or financial information in response to a phishing attack.

According to an October 2004 survey conducted by Truste and marketing company TNS, about six in ten consumers (58%) said they might reduce their online shopping during the holiday season of 2004 because of identity theft and other privacy concerns, up from 49 percent who expressed this view a year ago.[26] Half of the 1,071 people in the United States surveyed this year planned to limit their holiday online shopping to some extent. Eight percent were so concerned that they did not plan to shop online at all, up two percentage points over last year. The survey was conducted online between October 15 and 20, 2004.

7) Stealing ID From Personal Computers

Spyware

Spyware is a term to describe computer programs or software that can be used to transmit or initiate transmission of user information without his or her knowledge. Spyware programs have a range of functionality: logging keystrokes, scanning files on a hard drive, reading cookies and caches, and installing other more malicious programs (often termed malware) which destroy files or transmit viruses, often propagating themselves through the victim's address books.

Because of spyware's ability to retrieve information covertly, it can easily be used by an identity thief to steal an internet user's personal information. Identity thieves can use spyware to access information about anything a user does online, including retrieving their bank account and credit card information, pin numbers, passwords and tracking their online shopping purchases.

In November 2004, Sophos (an antivirus company) issued a warning that online customers of the British banks Abbey, Barclays, Egg, HSBC, Lloyds TSB, Nationwide

[26] http://www.identity-theft.org.uk/

and NatWest were being targeted by Banker-AJ Trojan, a Trojan horse that affects Microsoft Windows users.[27] Once customers would login to their bank accounts, Banker-AJ Trojan would capture passwords and take screenshots of the session. The information is then transferred back to the hacker, where it can be used to access a user's personal information. There have been no reports yet of AJ-Trojan being used to steal someone's identity, but this would be difficult to trace back if thieves were careful.

However, spyware has been used to retrieve financial information. An ID thief covertly installed spyware that logged keystrokes onto computer kiosks at Kinko's. He was finally caught in 2003, after capturing 400 names and passwords over the course of a year. The information was used to access and open new bank accounts, or sold over the internet.[28] The growing black market for identity information is one of the most worrying aspects of the problem, because it provides a secondary market after a thief has perpetrated his primary theft.

On October 21, 2004, a US District Court in Concord N.H. issued a restraining order against self-proclaimed "Spam King" Sanford Wallace and his two companies. Wallace has been operating for many years with impunity, because of the difficulty to prosecute his activities under US law. Wallace was given 24 hours to remove any script that exploits vulnerabilities in Web browsers in order to install, deposit or download software without notifying the user. Wallace is responsible for removing the script on any website, bulletin board or Internet server controlled by him or one of his companies.[29]

Perhaps this successful prosecution of Sanford Wallace will help de-legitimize spyware. It has been a long struggle to get the problem recognized and prosecuted, partly because many mainstream companies use software that is remarkably similar for reasonable marketing purposes, and it has been difficult to draw the line between criminal intent and marketing intent. Although a spyware trade association has now disbanded[30], websites still abound with spyware software.

8) Stealing ID from Corporate and Government Databases

Identity thieves often turn to corporate and government databases to gather information, usually involving employees. Their level of access and knowledge of passwords provides them with significant amounts of personal and financial information, particularly if access controls are set too broadly, which is often the case.

In June 2004, an AOL employee stole the identity of another AOL employee and used their personal information to access AOL's member list, which includes phone numbers and zip codes and the types of credit cards that members use to pay their bills. The list,

[27] According to webopedia, a Trojan horse is "[a] destructive program that masquerades as a benign application… one of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer." http://www.webopedia.com/TERM/T/Trojan_horse.html

[28] http://www.microsoft.com/smallbusiness/issues/technology/security/danger_danger_5_tips_for_using_a_public_pc.mspx

[29] http://news.com.com/2102-1030_3-5425421.html?tag=st.util.print

[30] http://www.infoworld.com/article/05/02/08/HNcoastfallsapart_1.html

containing 93 million email addresses, was sold to spammers for approximately $100,000. AOL maintains separate storage for email addresses and credit card numbers, and none of this information was compromised.

In September 2003, A Seattle man (Eric Drew) had his identity stolen by a hospital technician (Richard Gibson) while undergoing bone marrow transplants. Gibson claims to have found Drew's information from his paperwork that was lying on the hospital floor. Drew filed a lawsuit against Gibson and was awarded $15,000 in restitution. Gibson was sentenced to 16 months in prison.[31]

Phillip Cummings was arrested in January 2003 as part of what may have been then the largest reported identity theft case to that date. [32] Cummings worked as a customer service representative in New York for a company that provides software for credit agencies to keep track of consumer credit. Using his company password, he was able to get access codes that other companies use to conduct credit checks. The credit reports include Social Security numbers, credit card numbers and other personal information. Cummings sold the information to criminals, who then used it to defraud 30,000 victims across Canada and the United States.[33] Cummings was part of a 4-person identity theft ring that sold each victim's personal information for approximately $60.00.

In 2002 Ligand Pharmaceuticals in San Diego reached a confidential settlement with 14 former employees.[34] A laboratory employee had discovered personnel records in a storage closet. The files included names, addresses, Social Security numbers, and the employee used them to rent several apartments, open 20 cellular phone accounts and 25 credit card accounts, which were used to purchase $100,000 in goods.

In December 2002, a temporary replacement worker assigned to the office of MD Management Inc., a national financial services company in Ontario stole the profiles of 80 doctors from the company database. The profiles that were stolen contained complete financial data on the doctors and their families. The information was used to acquire credit cards in the victims' names, which were then used to their maximum limit.

In 1993, Adelaide Andrews discovered that the receptionist at her Santa Monica, California doctor's office had stolen Andrews' social security number. The receptionist used the SSN to rent an apartment while attempting to open new credit accounts.[35] The credit agency, TRW, matched Andrews' social security number with her last name and first initial and disclosed her credit history to the creditors. Andrews alleged that TRW's failure to confirm that she was involved in the transactions was a violation of the FCRA, and that TRW facilitated the theft of her identity. The case ended up at the Supreme Court of the United States on an issue over when the two year statute of limitations period of the FCRA

[31] http://seattlepi.nwsource.com/local/198499_cancerid06.html
[32] http://www.fbi.gov/page2/oct04/uncoveridt101504.htm. For a copy of the Department of Justice press release, see http://www.usdoj.gov/usao/nys/Press%20Releases/SEPTEMBER04/Cummings%20Plea%20PR.pdf
[33] http://archives.cnn.com/2002/TECH/11/26/hln.wired.id.theft/
[34] http://www.shrm.org/hrmagazine/articles/1202/1202covstory.asp
[35] http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=000&invol=00-1045

began. The Supreme Court held that the statute of limitation period should start to run on the date that TRW made the inaccurate disclosure. In response to the Supreme Court's finding, Congress passed the Identity Theft Victims Assistance Act of 2002.

In cases such as these, it is hard to imagine what the consumer can do to ensure their information is protected, other than to ask for the policies of the companies involved, and ask questions on a regular basis.

9) Physical Theft of Computers – Stealing Personal Information

In January 2003, a hard drive was stolen out of an ISM Canada facility (an IBM subsidiary). The drive belonged to Co-operators Insurance, who outsource some of their IT functions to ISM. It contained personal information of approximately 180,000 customers. While some of the files contained only names and addresses, others contained bank account information.36 However, there is no evidence that the information was used for a fraudulent purpose.37

On December 10, 2004, a computer was stolen during a mobile blood drive being conducted by Delta Blood Bank in California. The computer was being used for donor registration, and contained the donors' names, addresses, date of birth and social security numbers. Delta responded by sending a letter to the donors, notifying them that the computer had been stolen and advising them to register fraud alerts with credit reporting agencies.[38] Delta will no longer require donors to provide their social security numbers.

In October 2004, Wells Fargo computers were stolen from a company that prints loan statements for the bank.[39] The computers contained customers' names, addresses, customer account numbers and social security numbers. Wells Fargo issued a warning letter to customers whose information was stored on the computers. There is no indication that any of the information was compromised.

10) To Steal ID From Intermediaries

One possible way for identity thieves to obtain information is through insecure e-commerce transactions or lax corporate practices. For example, in March 2004, criminals posing as credit grantors gained access to the credit files of approximately 1,400 Canadians.[40] Fraud alerts were placed on all of the files, and it does not appear that any of the information was used to commit identity theft.

In September 2003, a Toronto man purchased two computers from a firm in Mississauga that sells used computer parts. Both computers contained Bank of Montreal customers' names, addresses and account balances. No information was compromised, and the

[36] http://www.cbc.ca/story/business/national/2003/01/30/cooperators030130.html
[37] A copy of the warning sent out by Co-operators can be accessed at: http://sask.cbc.ca/documents/images/co-operators.jpg
[38] A copy of the letter can be accessed at http://www.deltabloodbank.org/letter.htm
[39] http://www.siliconvalley.com/mld/siliconvalley/news/editorial/10079221.htm
[40] http://edmonton.cbc.ca/regional/servlet/View?filename=ed_idtheft20040317

computers were picked up by the Bank's computer security team.[41] Simson Garfinkel and Abhi Shelater drew attention to this rather well known security risk in 2002, by systematically purchasing computers from EBay and other second hand sources, and checking for personal data using commonly available forensic tools.[42]

[41] http://www.cbc.ca/stories/2003/09/15/Consumers/bmo_computers030915
[42] Simson Garfinkel and Abhi Shelat, Remembrance of Data Passed: A Study of Disk Sanitization Practices, IEEE Security and Privacy, http://csdl.computer.org/comp/mags/sp/2003/01/j1017abs.htm

4. Legal Issues

One of the reasons that ID theft has become epidemic is that the law has not responded quickly to defend the rights of victims. Another is that prosecution is difficult, for a variety of reasons. Possession of identity documents that do not belong to you has not hitherto been illegal, so police have to catch ID thieves in the middle of a fraudulent act. Operations now can be set up and closed down quickly, as much of the data necessary for large scale scams can fit on a laptop, sometimes even a datakey, and thieves are highly mobile, going from state to state or province to province. Internet scams are often perpetrated from remote countries, Nigeria and Moldovia being famous examples. Global electronic commerce has facilitated the use of credit cards online, from any remote location. We explore these legal problems below, in the global perspective.

1. Prosecution of Identity Thieves

In October 2004, US Attorney General John Ashcroft indicted 19 members of shadowcrew.com for offences ranging from conspiring to commit identity fraud to trafficking in credit card numbers, and exchanging forged and stolen identification documents. [43] According to the indictment, shadowcrew was an international network with 4,000 members who collaborated to steal personal information in order to commit credit and debit card fraud. The suspects were charged with:

1. transferring an identification document, authentication feature, or false identification document while knowing that it was stolen pr produced without lawful authority, violating Title 18, United States Code, Section 1028(a)(2);
2. knowingly transferring or using a means of identifying a person without lawful authority, and with the intent to commit, aid or abet unlawful activity, violating Title 18, U.S.C., Section 1028(a)(7)

The suspects accessed the personally identifiable information by hacking into the computer networks of legitimate retailers and using the electronic credit card verification system to swipe stolen credit cards and make sure they were still valid. This is one of an extremely small number of prosecutions. One survey stated that only 1 in 700 cases is brought to justice, and the Los Angeles Sheriff's Department and the San Diego police have stated that fewer than 5% are investigated.

Some of the reasons for this are:

- the law does not give clear cases to prosecute, and needs to be supplemented and amended
- investigation falls on local authorities, who do not have sufficient training and skill to build a successful case

[43] A copy of the indictment can be found at http://www.cybercrime.gov/mantovaniIndictment.pdf

- this is a cross-border crime, sometimes even a trans-continental crime
- people are often not aware that they are victims until they are denied credit, and delays inhibit good investigation
- there is insufficient public pressure on authorities to prosecute, so resources go to investigating more violent crimes
- credit card fraud rates are a huge and growing problem, but as a percentage of the enormously high use of credit in North America the cost has been manageable and has not prompted bank action. Consumers pay in the form of higher interest rates.

Justice Canada issued a consultation document in fall 2004 to examine legislative changes necessary to deter ID theft. The highlights of the report are detailed at the end of this chapter.

2. Lack of Agreed Security Standards and Protocols

The literature and the law is full of language about taking "reasonable precautions" and "reasonable care", but nowhere is that fully described. This situation is not unique to the ID theft issue, but all e-commerce and Internet issues are fraught with discussion and controversy about how best to maintain adequate security. Sadly, identity thieves have been able to exploit a number of well know vulnerabilities to perpetrate fraud, and it is harder to remedy the situation once the information is gone, than it would have been to protect it in the first place.

The generally accepted management standard for security will soon be passed as an ISO standard, ISO 17799, Developed principally from the British Standards Council's BSS 17799 which was accepted as a national standard during the 1990s, this standard sets out the various parameters of what ought to be considered in the development of security policies and procedures. We have not found a comparable document which describes what precautions have been taken to protect individuals from having their information used in ID theft, so have analysed the current draft standard and provided specific application to this issue in Chapter 9. Current criticism of ISO 17799 is that the document contains only recommendations, and is too high level to be useful. In fact, some security professionals prefer a code of practice which has been published by an IT security association called the IT Security Forum, *The Standard of Good Practice for Information Security*, [44]

It might be argued that this is a security, not a legal issue. This is not true, because there is a common law duty of care in all relations with customer data, there is a smorgasbord of data protection law which applies and which specifically requires reasonable care and compliance with accepted safeguards, and in many cases telecom regulations, banking regulations, and consumer protection legislation including fair credit reporting law have requirements to maintain confidentiality or ensure adequate protection. The problem appears to be in establishing what those acceptable standards must be, in such a rapidly evolving threat model.

[44] see www.securityforum.org

3. Misplaced Liability

Many privacy experts have stated that the central problem is one of misplaced pain or liability. Victims bear the brunt of the damage in ID theft. If a company recklessly gives out credit to a thief, the first recourse is to recover the loss from the individual whose ID was stolen. The threshold of proving innocence is a high one, and some individuals give up and pay bills that are not their own rather than waste their time. In the event that the company has to swallow the loss, it is written off on the backs of all the honest customers. A recent case in South Carolina demonstrates this problem rather eloquently**.**

In 2003, the South Carolina Supreme Court decided a question that illustrates some of the difficulties of using existing principles of tort law to deter credit grantors from issuing credit to identity thieves in the name of other individuals. The case is Huggins v. Citibank. The decision can be found at http://www.sclawyersweekly.com/archives/sc/opin/sup/25691.htm.

The plaintiff, Kenneth Huggins, asserted that Citibank and others negligently issued a credit card to an unknown impostor ("John Doe") who claimed that he was Huggins. Huggins alleged the defendants were negligent by:

1) issuing the credit cards without any investigation, verification, or corroboration of Doe's identity;
2) failing to adopt policies reasonably designed to verify the identity of credit card applicants;
3) adopting policies designed to result in the issuance of credit cards without verifying the identity of applicants; and
4) attempting to collect Doe's debt from Huggins.

Huggins said that as a result of the Banks' issuance of credit cards to Doe, Huggins' credit was damaged, he was hounded by collection agencies, he was distressed and embarrassed, and he expended much time and effort attempting to rectify the damage, with only partial success. In other words, Huggins was a classic victim of identity theft, and he wanted to hold the credit grantor accountable.

Huggins sued in federal court, but the case turned on the law of the state of South Carolina. The federal district court asked the South Carolina Supreme Court to resolve a specific question of state law. The question was whether South Carolina recognizes the tort of negligent enablement of impostor fraud and, if so, what are the elements of the tort and does the complaint state an actionable claim for the tort?

The South Carolina Supreme Court's decision reads like a syllogism. An essential element in a cause of action for negligence is the existence of a legal duty of care owed by the defendant to the plaintiff. In a negligence action, the court must determine, as a matter of law, whether the defendant owed a duty of care to the plaintiff. A duty arises from the relationship between the alleged tortfeasor and the injured party. In order for negligence liability to attach, the parties must have a relationship recognized by law as

the foundation of a duty of care. In the absence of a duty to prevent an injury, foreseeability of that injury is an insufficient basis on which to rest liability.

In the end, however, the court declined to recognize a duty of care between credit card issuers and those individuals whose identities may be stolen. It found that the relationship, if any, between credit card issuers and potential victims of identity theft is far too attenuated to rise to the level of a duty between them. Even though it is foreseeable that injury may arise by the negligent issuance of a credit card, foreseeability alone does not give rise to a duty.

Interestingly, the court expressed great concern about identity theft and financial fraud. It also asserted that some identity theft could be prevented if credit card issuers carefully scrutinized credit card applications. However, the court would not go beyond the traditional confines of existing tort law. Its decision cited cases in New York and Missouri that reached similar results.

The result in these cases could be overturned by statute, and it is possible that another court could extend the common law to allow identity theft victims to recover from credit grantors. Some believe that liability to victims would provide an extra incentive to credit grantors to be more careful in granting credit.

At present, credit grantors bear losses from transactions of the identity thief. However, credit grantors bear significant losses anyway when extending credit, and the losses to identity thieves may not be sufficiently large to induce them to increase scrutiny over credit applicants. Another reason may be that the profits lost by an inability to grant credit easily may outweigh the financial losses incurred by the credit grantor from identity theft. The costs borne by identity thief victims do not presently factor into the decisions by credit grantors. The Huggins litigation attempted to change how credit grantors act, but it failed. Whether legislatures will step in remains to be seen.

In the meantime, if companies can operate as free actors, jeopardizing the credit and even the identity of innocent individuals whether they are customers or not, there is little or no incentive for them to do a better job of protecting individuals other than damage to their own reputations. In Canada, data protection law provides more remedies. We will discuss this is chapter 9.

5. The US Situation: Legal Responses to a Growing Problem

This chapter offers a selective inventory of U.S. laws addressing identity theft. In the United States, many laws have been passed in an effort to prevent identity theft, assist its victims, improve prosecution of criminals, and otherwise address the problems of identity theft. Laws at both the federal and state levels are largely products of the 21st century.

This inventory is far from complete, but it includes examples of as many different types of legislative responses as could be readily identified in the available time. A complete inventory of state and federal laws relevant to ID theft would contain hundreds of laws and thousands of separate provisions.

Some laws can be readily characterized as responses to identity theft because the legislation or its history specifically identifies its purposes. In other cases, the nexus between a law and identity theft may not be overtly apparent, but the law may nevertheless have been motivated at least in part by a desire to address identity theft.

Other laws may provide useful responses to identity theft even though the law was passed for entirely different purposes, such as criminal laws that pre-exist identity theft which can be used to prosecute perpetrators. For example, the criminal penalty for wrongful disclosure of information included in a 1996 federal law designed to address the privacy of health information was recently used to prosecute a health worker who used a patient's health data to engage in identity theft. General purpose privacy laws passed decades ago may also provide direct or indirect assistance in the battle against identity theft by imposing some elements of fair information practices on record keepers.

This inventory focuses primarily on recent laws or parts of laws passed with a known or likely legislative intent to respond to identity theft. The inventory does not include rules and regulations issued by government agencies. In some instances, identity theft laws authorize administrative agencies to issue rules, regulations, or other administrative devices to address identity theft.

The inventory organizes laws into these categories: criminal penalties; jurisdiction; collection and use restrictions; victim assistance; administrative requirements and remedies; security measures; and general privacy laws. The categories are arbitrary. Other categorizations would be equally valid. Some laws that might fall into several categories are assigned here to a single category. Laws containing multiple provisions have, in some instances, been broken into component elements and each element has been placed in an appropriate category.

Finally, the inventory does not discuss every element in an identity theft law or every feature of the provisions described. The descriptions cover only those provisions that are representative of a type of law. The descriptions omit some technical and other details.

Inventory of U.S. Laws Addressing Identity Theft

A. Criminal penalties

This section includes laws that define the elements of crimes generally considered to be identity theft, establish penalties, and identify conduct that does not constitute identity theft.

US: The Identity Theft and Assumption Deterrence Act of 1998 (Public Law 105-318) amended the federal criminal code provision on fraud and related activity in connection with identification documents and information to define as a separate crime by a person to "knowingly, and with the intent to commit unlawful activities, possess, transfer, or use one or more means of identification not legally issued for use to that person." [18 U.S.C. § 1028(a) (7)].

US: The Internet False Identification Prevention Act of 2000 (Public Law 106-578) updated existing law against selling or distributing false IDs to include those sold or distributed through computer files, templates, and disks. [18 U.S.C. § 1028(c) (30(A), (d) (1)].

Arizona: A 2004 amendment states that a person commits criminal possession of a forgery device if the person makes or possesses any material, good, property or supply designed or adapted for use in forging written instruments or with the intent to aid or permit another person to use it for the purpose of forgery. [Ariz. Rev. Stat. § 13-2003].

Michigan: The 2004 Identity Theft Protection Act prescribes a criminal penalty for committing identity theft or obtaining or attempting to obtain another person's personal identifying information in order to commit identity theft or another illegal act. [Mich. Stat. § 445.65].

Mississippi: A 2004 amendment provides a lesser penalty for identity theft in cases involving a lesser amount of money (less than $250). [Miss. Code § 97-45-19(2)(b)]. The same statute [2004 Miss. Laws 526] defines "identity theft" to include crimes already defined by law to include those that relate to: false information [§ 97-9-79], fraud by mail or other means of communication [§ 97-19-83], fraudulent use of identity social security number, credit card or debit card number or other identifying information [97-19-85], or obtaining personal identity information of another person without authorization [§ 97-45-19].

Missouri: A law defining identity theft lists the improper use of "means of identification" as elements of the crime. The means of identification include but are not limited to: (1) Social Security numbers; (2) Drivers license numbers; (3) Checking account numbers; (4) Savings account numbers; (5) Credit card numbers; (6) Debit card numbers; (7) Personal identification (PIN) code; (8) Electronic identification numbers; (9) Digital signatures; (10) Any other numbers or information that can be used to access a

person's financial resources; (11) Biometric data; (12) Fingerprints; (13) Passwords; (14) Parent's legal surname prior to marriage; (15) Passports; or (16) Birth certificates. [Mo. Stat. § 570.223 (1), (2)].

Missouri: A law defining identity theft makes it a class A misdemeanor when the identity theft results in the theft or appropriation of credit, money, goods, services, or other property valued at less than $500; makes attempted identity theft a class B misdemeanor; makes identity theft a class D felony when the value of the stolen property is more than $500 but does not exceed $1,000; makes identity theft a class C felony when the value of the stolen property is more than $1,000 but does not exceed $10,000; makes identity theft a class B felony when the value of the stolen property is more than $10,000 but does not exceed $100,000; makes identity theft a class A felony when the value of the stolen property exceeds $100,000; makes identity theft a class A felony when the identity theft is performed for the purpose of committing a terrorist act, makes identity theft a class C felony when the identity theft is performed for the purpose of committing an election offense. [Mo. Stat. § 570.223(3)].

Missouri: The identity theft criminal statute does not apply to a person who: (1) obtains the identity of another person to misrepresent his or her age for the sole purpose of obtaining alcoholic beverages, tobacco, going to a gaming establishment, or another privilege denied to minors; (2) obtains means of identification or information in the course of a bona fide consumer or commercial transaction; (3) exercises, in good faith, a security interest or right of offset by a creditor or financial institution; (4) complies, in good faith, with any warrant, court order, levy, garnishment, attachment, or other judicial or administrative order, decree, or directive, when any party is required to do so; (5) is otherwise authorized by law to engage in the conduct that is the subject of the prosecution. [Mo. Stat. § 570.223 (9)].

Virginia: A law makes it unlawful identity theft for any person without authorization and with intent to defraud to: 1) obtain, record or access identifying information which is not available to the general public that would assist in accessing financial resources, obtaining identification documents, or obtaining benefits of such other person; 2) obtain goods or services through the use of identifying information of such other person; 3) obtain identification documents in such other person's name; or 4) obtain, record or access identifying information while impersonating a law-enforcement officer or an official of the government of the Commonwealth. [VA. Code § 18.2-186.3].

B. Jurisdiction

This section includes laws that define jurisdiction to hear cases, conduct investigations, or file charges; laws pertaining to service of process; and laws pertaining to who may prosecute cases.

Arizona: A 2004 law allows prosecutors to file a complaint charging multiple identity theft violations in any county in which a violation is alleged to have occurred. [Ariz. Rev. Stat. § 13-2008(B)].

California: A 2003 law specifies that the statute of limitations for crimes involving the unlawful use of personal identifying information and procuring or offering a false or forged instrument commences when the crime was discovered instead of when it was committed. [Cal. Penal Code § 803].

California: A 2004 law specifies that a foreign corporation's irrevocable consent to service of process includes service of search warrants in addition to those already specified for information concerning applications or accounts in the name of a victim of identity theft. [Cal. Corp. Code § 2105(a)(5)(B)].

Maryland: The law provides that the Department of State Police may initiate investigations and enforce this section throughout the State without regard to any limitation otherwise applicable to that department's activities in a municipal corporation or other political subdivision. The law also allows a law enforcement officer of the Maryland Transportation Authority Police, the Maryland Port Administration Police, or a municipal corporation or county to investigate violations of this section throughout the State without any limitation as to jurisdiction and to the same extent as a law enforcement officer of the Department of State Police. A 2004 amendment authorizes a state's attorney or the attorney general to investigate and prosecute offenses relating to personal identifying information fraud; authorizes the attorney general to exercise all the powers and duties of a state's attorney to investigate and prosecute specified violations; and establishes that a prosecution for a violation of specified offenses relating to personal identifying information fraud or other crimes based on a violation may be commenced in a county in which an element of the crime occurred or in which the victim resides. [Md. Code § 8-301].

Michigan: A 2004 law allows a law enforcement agency or victim of identity theft to verify information from a vital record from a local registrar or the state registrar. [Mich. Stat. § 445.73(1)].

Michigan. A 2004 law amends the Code of Criminal Procedure to specify that a violation of the Identity Theft Protection Act could be prosecuted where the offense occurred, where the information that had been used to commit the violation was used illegally, or where the victim resides. If a person is charged with more than one violation and the violations could be prosecuted in more than one jurisdiction, than any of the above jurisdictions would be considered a proper jurisdiction for all the violations. [Mich. Stat. § 762.10c].

Mississippi: A 2004 law provides for aggregation of amounts in determining the amount of an offense. [Miss. Code § 97-17-41(2)(c)].

Mississippi: A 2004 law grants subpoena power to the attorney general in conducting investigations of identity theft. [2004 Miss. Laws 526, § 6].

Missouri: A 2004 law clarifies that a criminal prosecution for identity theft may be conducted in any county where a victim or defendant resides, where the stolen property was located, or in any county where an element of the crime was committed. [Mo. Stat. § 541.033].

C. Collection and Use Restrictions

This section includes laws that impose collection and use restrictions on personal data; laws that block or freeze credit files; laws limiting credit grantor activity; and laws restricting spyware.

US: The Social Security Number Confidentiality Act of 2000 requires the Secretary of the Treasury to ensure that Social Security account numbers (including derivatives of such numbers) are not visible on or through unopened mailings of checks by the federal government.
[31 U.S.C. § 3327].

US: The Fair and Accurate Credit Transactions Act of 2003 prohibits any person that accepts credit cards or debit cards for the transaction of business from printing more than the last 5 digits of the card number or the expiration date upon any receipt provided to the cardholder at the point of the sale or transaction. [15 U.S.C. 1681c(g)].

US: The Fair and Accurate Credit Transactions Act of 2003 permits a consumer to ask a consumer reporting agency (credit bureau) to truncate disclosures of Social Security Numbers to the first 5 digits. [15 U.S.C. 1681g(a)(1)(A)].

US: The Fair and Accurate Credit Transactions Act of 2003 requires a consumer reporting agency (credit bureau) to block the reporting of any information in the file of a consumer that the consumer identifies as information that resulted from an alleged identity theft. [15 U.S.C. § 1681c-2].

US: The Fair and Accurate Credit Transactions Act of 2003 requires that a person that A furnishes information to any consumer reporting agency (credit bureau) must have in place reasonable procedures to respond to any notification that it receives from a consumer reporting agency relating to information resulting from identity theft and to prevent that person from refurnishing the blocked information. [15 U.S.C. 1681s-2(a)(6)(A)].

US: The Fair and Accurate Credit Transactions Act of 2003 prohibits a person from selling, transferring, or placing for collection a debt that the person has been notified has resulted from identity theft. [15 U.S.C. 1681m(f)].

US: The Fair and Accurate Credit Transactions Act of 2003 requires that a debt collector that is notified that information pertaining to a debt may be the result of identity theft must notify the third party and provide information to the consumer if the consumer wished to dispute the debt. [15 U.S.C. 1681m(g)].

Arizona: A law restricts use of Social Security Numbers by prohibiting 1) intentional communication of a SSN to the general public; 2) printing a SSN on any card that an individual requires to receives a product or service; 3) transmission of a SSN over the Internet unless the connection is secure or the SSN is encrypted; 4) requiring a SSN to

access an Internet web site unless a password or unique identification number is also required; 5) printing a SSN on any materials mailed to the individual, unless required by state or federal law. [Ariz. Rev. Stat. § 44-1373(A)].

California: A 2002 law requires product warranty cards to clearly state that the consumer is not required to return the card for the warranty to take effect. [Cal. Civ. Code § 1793.1].

California: A 2003 law establishes a procedure to keep Social Security numbers confidential in court filings for legal separation, dissolution or nullification of marriage. [Cal. Fam. Code § 2024.5].

Colorado: A 2004 law requires a creditor or charge card company that offers credit or a charge card by mail, and that receives an acceptance of an offer that lists an address for the applicant that is different from the address where the offer of credit or a charge card was sent, to verify that the person accepting the offer is the person to whom the creditor or charge card company made the offer of credit or a charge card. [Colo. Rev. Stat. § 5-3.7-101].

Rhode Island: A law states that unless required by federal law, no person shall require that a consumer of goods or services disclose a Social Security Number incident to the sale of consumer goods or services. The law allows insurance companies, health care, or pharmaceutical companies to require the consumer to furnish a social security number. A consumer may also be required to furnish a SSN when applying for a credit card. [R.I. Gen. Laws Section § 6-13-17].

Vermont: A 2004 allows a person who has been a victim of identity theft to place a security freeze on the credit report if the consumer submits a request along with a valid copy of a police report, investigative report, or complaint the consumer has filed with a law enforcement agency about unlawful use of his or her personal information by another person. A credit reporting agency (credit bureau) may not charge a fee for placing or removing a security freeze. [9 V.S.A. § 2480h].

Washington: A law requires a credit reporting agency (credit bureau) to block inaccurate information resulting from an identity theft upon receipt of a police report. [Rev. Code Wash. § 19.182.160].

D. Victim Assistance

This section includes laws that provide identity theft victims some type of assistance, help with debt collectors, or rulings of innocence.

US: The Fair and Accurate Credit Transactions Act of 2003 requires the Federal Trade Commission to prepare a model summary of the rights of consumers for remedying the effects of fraud or identity theft involving credit, an electronic fund transfer, or an account or transaction at or with a financial institution or other creditor. If any consumer

contacts a consumer reporting agency (credit bureau) and expresses a belief that the consumer is a victim of fraud or identity theft involving credit, an electronic fund transfer, or an account or transaction at or with a financial institution or other creditor, the consumer reporting agency must provide the consumer with a summary of rights that contains all of the information required by the model summary. [15 U.S.C. 1681g(d)].

US: The Fair and Accurate Credit Transactions Act of 2003 requires a business entity to provide to a victim of identity theft a copy of application and business transaction records in the control of the business entity that contain evidence of transactions alleged to be the result of identity theft. [15 U.S.C. 1681g(e)].

US: The Fair and Accurate Credit Transactions Act of 2003 requires the Federal Trade Commission to establish and implement a media and distribution campaign to teach the public how to prevent identity theft. [Public Law No. 108-159, § 151(b)].

US: The Fair and Accurate Credit Transactions Act of 2003 allows a consumer who suspects that she or he has been or is about to become a victim of identity theft to direct a consumer reporting agency (credit bureau) to place a fraud alter on the file of that consumer. The consumer reporting agency must refer information about the fraud alert to other agencies ("one-call fraud alert"). A consumer who places a fraud alert on his or her file may request a free copy of the consumer's file. The fraud alert for a consumer who submits an identity theft report to a consumer reporting agency can be up to seven years, and the consumer is entitled to two free credit reports during the year after submitting the report. [15 U.S.C. § 1681c-1].

US: The Fair and Accurate Credit Transactions Act of 2003 requires credit reporting agencies (credit bureaus) to provide free annual credit reports ("annual disclosure") to each consumer who requests a report through a "centralized source" required to be established by the agencies under the Act. [15 U.S.C. 1681j(a)].

Arizona: A 2004 law requires a peace officer to take a report on the request of any person or entity whose identity has been taken. [Ariz. Rev. Stat. § 13-2008(B)

California: A 2003 law requires a debt collector to stop collection when an alleged debtor furnishes a police report of identity theft and other information on his status as an identity theft victim. If a collector ultimately determines that the information fails to establish that the consumer is not responsible for the debt, the collector has to notify the consumer of that determination and its basis before proceeding with collection. The law also helps identity theft victims clear up their records by requiring debt collectors who cease collection activities to notify the creditors and consumer credit reporting agencies to which the collector previously provided adverse information. [Cal. Civ. Code § 1788.18].

California: A 2003 law requires a credit issuer using a consumer credit report who discovers that key identifying information (first and last name, address, SSN) on an application for credit does not match the information in the credit report, to take reasonable steps to stop and verify the accuracy of the information on the application. [Cal. Civ. Code § 1785.20.3].

California: A 2003 law provides that when the property or things to be seized consist of any item or constitute any evidence that tends to show a violation of specified identity theft crimes, a magistrate may issue a warrant to search a person or property located in another county if the person whose identifying information was taken or used resides in that other county. [Cal. Penal Code § 1524].

California: A 2003 law expands the rights of a person who is a victim of identity theft to obtain information used by the unauthorized person to open and account or service and a record of transactions and charges. The 2003 law expands the rights to include applications and accounts regarding mail receiving or forwarding services and office or desk space rental services. [Cal. Penal Code § 530.8].

California: A 2003 law amended a previous law that allowed consumers to place a freeze on their credit files. The 2003 law capped the fees that can be charged for a freeze and for a thaw. [Cal. Civ. Code § 1785.11.2(m)].

California: A 2003 law requires credit reporting agencies to notify consumers when fraud alerts expire. [Cal. Civ. Code § 1785.11.1(g)].

California: A law allows a person who reasonably believes that he or she is the victim of identity theft to petition a court for an expedited judicial determination of his or her factual innocence. [Cal. Penal Code § 530.6(b)].

California: A 2003 law establishes a procedure for an identity theft victim to contest a charge by submitting a thumbprint for comparison with the thumbprint of the thief taken at time of arrest. Upon comparison of the thumbprints by prosecuting attorney and conclusion of non-match, the court may issue a finding of factual innocence and notify the Department of Motor Vehicles. [Cal. Penal Code § 853.5].

California: A 2003 law requires any credit card issuer that receives a change of address request from a cardholder who orders a replacement credit card, and any business entity that provides telephone accounts and receives a change of address request from an accountholder who orders new service, to send a change of address notice to the previous address of record. [Cal. Civ. Code § 1799.1b].

California: A 2002 law assists victims of criminal ID theft in rectifying criminal records wrongfully associated with their name, by allowing a court or a prosecuting attorney to move for an expedited judicial determination of factual innocence. The law allows the court to order the removal of incorrect references to the victim's name and personal information in court records and files. [Cal. Penal Code § 530.6].

California: A 2001 law requires a consumer credit reporting agency to disclose, upon request of the consumer, the addresses and, if provided by the sources and recipients of the consumer's credit information, telephone numbers identified for customer services for the sources and recipients. [Cal. Civ. Code § 1785.10(c)].

Michigan: A 2004 law prohibits denying credit to, or reducing the credit limit of, a person because he or she was a victim of identity theft. [Mich. Stat. § 445.71].

Mississippi: A 2004 amendment authorizes the attorney general to provide assistance to victims of identity theft in clearing their records. [Miss. Code § 97-45-19(5)].

Mississippi: A 2004 amendment clarifies that perpetrators of identity theft shall pay restitution to victims. [Miss. Code § 97-45-19(6)].

Mississippi: A 2004 amendment allows a person who has petitioned the court to expunge any charges, arrest record or conviction falsely entered against the person as a result of the appropriation of his information may submit to the Attorney General a certified copy of a court order obtained. The Office of the Attorney General may issue an "Identity Theft Passport" verifying that such order has been entered. A person who has filed a police report alleging that the person's name or other identification has been used without the consent or authorization by another person may submit a copy of the police report to the Attorney General. The Office of the Attorney General may issue an "Identity Theft Passport" stating that such police report has been submitted. [2004 Miss. Laws 526, § 5(1) & (2)].

Missouri: A 2004 amendment makes an identity thief liable to the victim for civil damages of up to $5,000 per incident or three times the amount of actual damages, whichever is greater. A victim may also seek a court order restraining the identity thief from future acts that would constitute identity theft. [Mo. Stat. § 541.033(5)].

Missouri: A 2004 amendment clarifies that the estate of a deceased person may pursue civil remedies when the estate is a victim of identity theft. [Mo. Stat. § 541.033(6)].

E. Administrative Requirements and Remedies

This section includes laws that direct government agencies to take actions designed to prevent, prosecute, or reduce identity theft and its consequences.

US: The Fair and Accurate Credit Transactions Act of 2003 requires the Secretary of the Treasury to conduct a study of the use of biometrics and other similar technologies to reduce the incidence and costs to society of identity theft by providing convincing evidence of who actually performed a given financial transaction. [Public Law No: 108-159, § 157].

US: The Identity Theft and Assumption Deterrence Act of 1998 makes the Federal Trade Commission a central clearinghouse for identity theft complaints. The Act requires the FTC to log and acknowledge such complaints, provide victims with relevant information, and refer their complaints to major national consumer reporting agencies and other law enforcement agencies. [Public Law No. 105-318, § 5].

US: The Internet False Identification Prevention Act of 2000 requires the Attorney General and the Secretary of the Treasury to establish a coordinating committee to ensure, through existing interagency task forces or other means, that the creation and distribution of false identification documents is vigorously investigated and prosecuted. [Public Law No. 106-578, § 2].

Virginia: A 2004 law requires the Department of Motor Vehicles upon notification from the attorney general that an Identity Theft Passport has been issued to a driver, to note the same on the driver's abstract. [Va. Code § 18.2-186.5].

California: A 2001 law addresses the risk of identity theft created when veterans file their discharge papers (DD214s), which contain their SSN, with their county recorders. The law requires county recorders to provide any military veteran who does so with a written form indicating that the document becomes public when it is recorded. The veteran must sign the form in acknowledgement. [Cal. Gov. Code § 27337].

California: A 2002 law requires the implementation of an electronic death registration system by January 1, 2005. This law was intended to improve the timeliness and efficiency of California's death registration process, thereby expediting the State's ability to curtail the fraudulent use of both the birth and the death record through the timely application of the birth/death cross-matching. [Cal. Health & Safety Code § 102778].

California: A 2002 law sought to reduce the fraudulent use of birth certificates in identity theft by establishing authorization requirements for applicants to obtain certified copies of birth and death certificates. The law also requires State and local registrars that issue copies of birth certificates to non-authorized applicants to print the words "informational, not a valid document to establish identity" on the copy issued. [Cal. Health & Safety Code § 103526]

California: A 2002 law exempts birth and death indices from disclosure under the California Public Records Act and requires the State Registrar to establish separate non-comprehensive indices, which do not contain Social Security numbers or mother's maiden name, for public release. Requesters of the indices would be required to provide proof of identity and sign a standard form certifying, under penalty of perjury, that they will comply with prescribed guidelines for use of the indices. [Cal. Health & Safety Code §§ 102230-32].

California: A 2000 law creates in the Department of Justice a database of identity theft victims who have had a criminal record falsely created using their identifying information. [Cal. Penal Code § 530.7(c)].

California: A 2000 law established within the Department of Consumer Affairs the Office of Privacy Protection. [Cal. Bus. & Prof. Code § 530].

F. Security Measures

This section includes laws that address security requirements, disposal of information, and notices of security breaches.

US: The Fair and Accurate Credit Transactions Act of 2003 requires federal banking agencies and the Federal Trade Commission to jointly 1) establish and maintain guidelines for financial institutions and creditors regarding identity theft; 2) prescribe regulations requiring financial institutions and creditors to establish reasonable policies and procedures for implementing the guidelines, to identify possible risks to account holders or customers; and 3) prescribe regulations for card issuers to ensure that, if a card issuer receives notification of a change of address for an existing account, and within a short period of time receives a request for an additional or replacement card for the same account, the card issuer may not issue the additional or replacement card, unless the card issuer notifies the cardholder of the request at the former address of the cardholder and provides to the cardholder a means of promptly reporting incorrect address changes. [15 U.S.C. 1681m(e)].

Virginia: A 2004 law directs child day programs that reproduce or retain documents of a child's proof of identity required for the child's enrollment to destroy them upon the conclusion of the period of retention. The procedures must include all reasonable steps to destroy such documents by shredding, erasing, or otherwise modifying the Social Security numbers in those records to make them unreadable or indecipherable by any means. [Va. Code § 63.2-1809].

California: A 2004 law requires a business that owns or licenses personal information about a California resident to implement and maintain reasonable security procedures and practices to protect personal information from unauthorized access, destruction, use, modification, or disclosure. The law also requires a business that discloses personal information to a nonaffiliated third party, to require by contract that those entities maintain reasonable security procedures. [Cal. Civ. Code § 1798.81.5].

California: A 2004 law authorizes the Department of Motor Vehicles to require fingerprints and associated information from employees whose duties include access to certain confidential information, including credit card numbers and Social Security Numbers. [Cal. Govt. Code § 1040].

California: The 1004 Consumer Protection Against Computer Spyware Act prohibits an unauthorized person from knowingly installing or providing software that performs certain functions on or to another user's computer located in California. The prohibited software functions are (1) taking control of the computer, (2) modifying certain settings on the computer, (3) collecting personally identifiable information, (4) preventing a user’s reasonable efforts to block its installation or disable it, (5) misrepresenting that it will be uninstalled or disabled by a user’s action, or (6) removing or rendering inoperative security, anti-spyware or anti-virus software on the computer. [Cal. Bus. & Prof. Code § 22947].

California: The 2003 Identity Theft Prevention and Assistance Act prohibits bars, car dealers and others from collecting information by swiping driver's licenses for any purpose other than verifying age or authenticity of the license, check verification or when legally required. [Cal. Civ. Code § 1798.90.1].

California: A 2003 law requires a business or a State agency that maintains computerized data that includes specified personal information to disclose any breach of the security of that data to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. [Cal. Civ. Code § 1798.29].

California: A 2000 law requires businesses that are no longer retaining customer records containing personal information to destroy the records by shredding, erasing, or otherwise modifying the customer record to make information therein unreadable or undecipherable through any means. [Cal. Civ. Code §§ 1798.80-.82].

G. General Privacy Laws

This section includes some federal privacy laws that include privacy protections. Many of these laws pre-date the birth of identity theft, but the law may include some provisions that are useful to prevent identity theft or aid its victims.

US: The 1970 Fair Credit Reporting Act establishes privacy rules for consumer records maintained by consumer reporting agencies (credit bureaus). The law has been amended numerous times, most recently by the Fair and Accurate Credit Transactions Act of 2003. [15 U.S.C. § 1681 et seq.].

US: The 1974 Fair Credit Billing Act establishes procedures for resolving billing errors on credit card accounts and limits a consumer's liability for fraudulent credit card charges. [15 U.S.C. §1666 et seq.].

US: The 1977 Fair Debt Collection Practices Act prohibits debt collectors from using unfair or deceptive practices to collect overdue bills that a creditor has forwarded for collection. [15 USC 1692 et seq.].

US: The 1978 Electronic Fund Transfer Act provides a basic framework establishing the rights, liabilities, and responsibilities of participants in electronic fund transfer systems. The primary objective of the law is the provision of individual consumer rights. [15 U.S.C. §1693].

US: The 1994 Driver’s Privacy Protection Act prevents the States from disclosing driver’s license and motor vehicle information about individuals except in specified circumstances or with the consent of the individual. [18 U.S.C. § 2721 et seq.].

US: The 1996 Health Information Portability and Accountability Act of 1996 establishes criminal penalties for the wrongful disclosure of individually identifiable health information. The Act also requires the Department of Health and Human Services to issue rules regulating the security and confidentiality of patient information. [42 U.S.C. §§1320d-6, 1320d-2 note].

US: The 1998 Children's Online Privacy Protection Act limits the ability of an operator of a website or online service directed at children from collecting personal information about a child. [15 U.S.C. § 6501 et seq.].

US: The 1999 Gramm-Leach-Bliley Act (Financial Services Modernization Act) includes a variety of provisions addressing privacy protection by requiring several federal agencies to issue regulations ensuring that financial institutions protect the security and privacy of consumers' personal financial information. The institutions must develop and give notice of their privacy policies to their own customers at least annually, and before disclosing any consumer's personal financial information to a nonaffiliated third party, must give notice and an opportunity for that consumer to "opt out" from such disclosure. [15 U.S.C. §§ 6801-6809].

6. The Database Industry: The ChoicePoint Scandal and the Regulation of an Information Age Industry

ChoicePoint is one of the largest data service providers in the U.S. The Georgia based company emerged in 1997 with a specific focus on providing data to the insurance industry. However, the company has seen tremendous growth in the past 8 years and now provides services to all sorts of businesses, as well as federal, state and local government agencies. Today the company possesses billions of records about people and has over 50 000 clients. Efforts are underway with Civil Liberties Groups in Canada to find out exactly what data the information brokers in the United States have about Canadians, but at the moment we have no data to report.

ChoicePoint is one of a type of company known as data brokers who gather and analyze public records and sell the data to corporations, employment firms, marketers, the police, national security agencies and other government agencies. In a sense, these companies act as privatized intelligence agencies since they not only gather the information, they also analyze it[45]. ChoicePoint is among the largest and most powerful of these data service providers in part because the company has bought out several of its competitors in recent years[46.] Many of these companies have close ties to the government. The EPIC (Electronic Privacy Information Center) website reports that ChoicePoint sells a wide range of information to the government including:

- Credit headers, a list of identifying information that appears at the top of a credit report. This information includes name, spouse's name, address, previous address, phone number, Social Security number, and employer.
- Workplace Solutions Pre-Employment Screening," which includes financial reports, education verification, reference verification, felony check, motor vehicle record, SSN verification, and professional credential verification.
- Asset Location Services.
- The ability to engage in "wildcard searches," which allows law enforcement to "obtain a comprehensive personal profile in a matter of minutes" with only a first name or partial address.
- The use of "Soundex" queries, which allow searches on personal information based on how names sound, rather than how they are spelled.
- Information on neighbours and family members of a suspect[47.]

[45] Senator Patrick Leahey, in a speech at the 10th Anniversary of the Centre for Democracy and Technology, Washington D.C. March 9, 2005 described these companies as privatized intelligence agencies.
[46] Refer to the EPIC website for a list of all the companies that ChoicePoint has acquired <http://www.epic.org/privacy/choicepoint/>
[47] http://www.epic.org/privacy/choicepoint/

In the post 9/11 era, commercial information services are playing a central role in government intelligence services now clustered in the Department of Homeland Security. The agencies now united at DHS rely on these services for public records, identity verification, and automated analysis. In fact, ChoicePoint currently employs a team of homeland security advisors, many of whom were previously government officials.

As journalist Robert O'Harrow has pointed out:

> ChoicePoint and other private companies increasingly occupy a special place in homeland security and crime-fighting efforts, in part because they can compile information and use it in ways government officials sometimes cannot because of privacy and information laws.[48]

While government authorities have claimed that the services provided by companies such as ChoicePoint are essential for national security in the current climate, privacy advocates argue that there is a lack of regulations, restrictions and oversight in place to ensure that individuals' civil liberties are protected. In fact, there are virtually no restrictions in the private sector in the US that address the collection, use, and disclosure of this personal information.

In December 2004, EPIC filed a complaint with the Federal Trade Commission. The document, authored by Chris Hoofnagle of EPIC and George Washington law professor Daniel Solove, claimed that the compilation and sale of personal information by data brokers such as ChoicePoint should be considered a "consumer report" for the purposes of Fair Credit Reporting Legislation (as amended by FACTA) and therefore both the seller and buyer of the information should be subject to regulations including Fair Information Practices regulations.

ChoicePoint has also been criticized for its background-checking services. There have been several lawsuits and consumer complaints in recent years which accuse the company of providing inaccurate and out-of-date information in its criminal background checks, resulting in unfair job losses for applicants, who have scant opportunity to get redress. A presentation by Pam Dixon at the Computers, Freedom and Privacy Conference of 2005 documents problems in accuracy and transparency throughout the employee search and screening process in the United States, and much of the information comes via ChoicePoint and Acxiom, another large data broker that has expanded operations since 911.

There is currently a federal law in place requiring consumer reporting agencies to either verify the data they give employers or notify the applicants if they are providing outdated or false information to an employer. A recent article by Kim Zetter in Wired magazine claims that ChoicePoint appears to be doing neither in many cases[49]. Zetter reports that the company was found guilty in one case where an applicant lost a job based

[48] http://www.msnbc.msn.com/id/6846357/
[49] http://www.wired.com/news/privacy/0,1848,66983-3,00.html?tw=wn_story_page_next2

on faulty information, but there are several other cases which have been settled out of court or are still being investigated.

What does this have to do with a Canadian report on ID theft? Firstly, we are uncertain whether ChoicePoint or any of its subsidiaries holds data about Canadians. This is true for other giant data brokers as well. It seems highly unlikely that they do not, since the border is utterly transparent for the financial, telecommunications, and retail sector, i.e. Canadian traffic on these networks is seamless with that of the United States. Secondly, ChoicePoint now has the distinction of being the site of the biggest case of ID theft in history. The way this theft was perpetrated should give pause to all who think we are making headway in fighting this scourge.

ChoicePoint made the news on February 18, 2005 when the Wall Street Journal reported that the company had sold private information of about 145,000 U.S. residents to criminals who posed as legitimate businesses. The reason the company went public on the breach, long after learning of it, is that California's law requiring notification of security breaches to the individuals whose data was compromised came into effect in January 2005. The company rather cavalierly responded to the press that they did not intend to extend the notification to victims outside California, and the story has rolled downhill like a snowball since then. So far 750 of those people have reported being victims of fraud and identity theft. The incident involves the sale of a wide range of data including names, addresses, Social Security Numbers, and credit reports.

This is not a new problem for ChoicePoint. In 2002, an individual who used personal information obtained from ChoicePoint was sentenced to 5 1/2 years in federal prison for committing identity theft. However, the scale of the current breach has surpassed any previous cases.

California is the only state with a law that requires companies to disclose such incidents to consumers when they are discovered, and ChoicePoint has thus far only notified between 30,000 to 35,000 California residents that their personal data may have been accessed by an un-authorized party. However, as Bob Sullivan has pointed out, such data theft incidents are rarely limited to a single geographic area[50]. Once again, consumer and privacy advocates have called for federal oversight and regulations for data brokering businesses and hearings are being scheduled on the issue. Currently, the Securities and Exchange Commission and the Federal Trade Commission have launched investigations of ChoicePoint.

In order to address the situation, ChoicePoint has hired Carol A. DiBattiste, previously a deputy administrator of the Transportation Security Administration, and appointed her as the company's Chief Privacy Officer. It has also contributed one million dollars over four years to fund the Identity Theft Resource Centre, a tiny NGO in San Diego started by ID theft victims, to assist other victims.[51]

[50] http://www.msnbc.msn.com/id/6969799/
[51] see www.identitytheftresourcecenter.org

Daniel Solove and Chris Hoofnagle, who have written about ChoicePoint and the inadequacy of US data protection law, have written an article proposing new regulation to govern data brokers[52]. The central problems in the free flow of personal information throughout public records and the private sector in the United States will be extremely difficult to combat. While PIPEDA may have its problems, Canadians should be thankful that we are not in quite as bad a situation as our friends in the United States. However, because Canadian data is now flowing across the border through airline and custom systems, and data brokers such as ChoicePoint have a mandate from the government to collect data for security purposes, these issues demand our attention. We discuss the particular problems of data brokerage and the proposal for regulation in the following section.

Solove's and Hoofnagle's Model Privacy Regime for the United States

In response to widely publicized security breaches by ChoicePoint and other organizations, Daniel J. Solove and Chris Jay Hoofnagle proposed a Model Regime of Privacy Protection with the goal of sparking a discussion of concrete legislative solutions to privacy problems. Solove is an Associate Professor of Law at the George Washington University Law School, and Hoofnagle is the Director of the Electronic Privacy Information Center West Coast Office. The Model Regime is a work in progress that the authors plan to update in response to comments and suggestions from others.

Despite its expansive title, the focus of the Model Regime is limited. It is a response to the ill-defined industry of data brokers whose activities largely fall outside the regulatory scheme of the Fair Credit Reporting Act, a law that regulates narrowly defined consumer reporting agencies or credit bureaus. Solove and Hoofnagle observe that the government is increasingly relying on data brokers to supply and analyze personal data for intelligence and law enforcement purposes. Federal agencies operate under the privacy restraints of the Privacy Act of 1974, but the government's use of data brokers appears to fall largely outside the scope of the Privacy Act. As a result, a major activity affecting individuals and their privacy interests and involving both the federal government and significant private sector data processors does not appear to be covered by any existing U.S. privacy law. Recourse to such data brokers has replaced collection by government itself, and has been explicitly noted by the Office of Management and Budget as falling outside the scope of the Privacy Act because it is not a "collection".

Solove and Hoofnagle organize their 16 proposals into five categories. The first covers notice, consent, control, and access. In general, data brokers operate without any legal requirement to:

- provide data subjects with information about their data activities
- obtain any form of consent for processing of personal data
- permit opt-out of processing by data brokers
- offer rights of access or correction
- assume liability for errors that harm individuals

[52] see http://papers.ssrn.com/sol3/papers.cfm?abstract_id=699701

The Model Regime outlines legislative responses to cure all of these shortcomings in existing law, including the ability to freeze credit reports and free credit monitoring services for all consumers who request it.

The second set of proposals addresses security. Solove and Hoofnagle propose the use of passwords that are not based on publicly available personal information and that can be easily changed. The proposal would exclude the use of Social Security Numbers and biometrics. A second security proposal would require that data subjects be notified of security breaches. The law in California and a few other states already requires notices, but there is no federal requirement.

The third set of proposals would increase regulation of business access to and use of personal information. At present, data brokers are generally not subject to any privacy regulation. Solove and Hoofnagle would:

- prohibit private sector companies from using Social Security Numbers for identification purposes
- restrict access to public records (mostly held by the states) and allow the records to be used only for defined purposes
- limit the use of background checks to fiduciary relationships or other specifically defined activities
- establish minimum standards for state licensure and oversight of the private investigator industry.

The fourth set of proposals would regulate government access to and use of personal data. These proposals would:

- require that the government obtain a court order based on probable cause and particularized suspicion that any personal information sought from third parties involves evidence of a crime
- prevent data mining from becoming a dragnet search for prospective crimes by requiring greater judicial supervision and more public accountability
- update the Privacy Act of 1974 to limit disclosures, cover the outsourcing of personal information processing to private sector businesses, and improve enforcement.

The last set of proposals covering privacy innovation and enforcement would:

- preserve the ability of the states to develop legislative responses to privacy problems through federal legislation that establishes floors of privacy protection but that does not preempt the states from enacting stronger laws
- improve sanctions on privacy violators and provide better remedies to data subjects, including minimum liquidated damages.

The Model Regime is useful on its own terms as a possible if limited legislative agenda for the U.S. Congress and for the states. It is also a reflection of existing privacy laws in

the United States and the gaps in those laws. Many of the elements of the Model Regime are already features of general privacy law in Canada, EU Member states, and other countries around the world. Solove and Hoofnagle would largely continue the so-called sectoral approach that has characterized privacy American law for three decades, an approach they must appreciate is piecemeal, but have adopted for purposes of expediency in terms of catching the boat that appears to leaving for Congress right now, in the wake of all the data breach disclosures.

The Model Regime does specifically focus on the problems of identity theft, although some of its proposals would have an effect on the availability, security, or use of personal information. Proposals for increased use of password and free credit watch services are the most likely to make life harder for some identity thieves or to make it easier for consumers to determine if they have been a victim of identity theft.

7. PIPEDA: What Protection Does it Offer?

While many privacy advocates are currently pushing for stronger provisions in PIPEDA because of frustration with results in the first five years of implementation, it must be said that the legislation is far from useless in the fight against ID theft. We have only to look across the border at the plethora of rules and legislation, to recognize that holistic privacy legislation, particularly where matched with similar legislation in the provinces, addresses a few of the management problems. However, there are certainly gaps that should be addressed. The following section examines what PIPEDA provides and where action needs to be taken, both in terms of implementation and legislatively.

PIPEDA is unique in terms of data protection legislation in that it specifically requires adherence to a management standard for privacy protection, in the belief that addressing privacy as a set of management practices simplifies implementation. Other provisions in the legislation provide more precise requirements, particularly with respect to obtaining the consent of the individual, and set out the powers of the Commissioner. We will address the provisions of the standard first, including directly relevant provisions in the legislation, and then address the powers of the Commissioner and discuss a few possible actions she might take which could help in the current crisis.

It should be noted that other legislation in Canada has a direct bearing on ID theft, notably provincial credit reporting and consumer protection legislation, federal banking regulations, and provisions respecting the use and protection of the social insurance number (SIN). While abuse of the SIN is not as rampant as abuse of the SSN is in the United States, the Auditor General noted in a report on the SIN in 1998 that its use could be better controlled, and indeed banned in the private sector except for legitimate federal purposes associated with its original intent. Human Resources and Skills Development Canada (HRSDC) is responsible for the SIN database and legislation.

Finally, while we are not reviewing provincial data protection law, the law in Alberta is well worth mentioning, because the particular clauses which address the issue of ID theft under protection of information (section 34) has recently been used in the findings against three companies whose practices exposed customers to the risk of identity theft. It is encouraging to privacy advocates to see that the Alberta Commissioner is working closely with police who find stolen data now, because until we have better Criminal Code provisions to address information theft, there is not much the police can do about these caches of personal information

Note that we have added emphasis in certain sections by **bolding** mandatory requirements. If some of these provisions were implemented and enforced, a great deal could be done to ameliorate the situation with ID theft. While analyzing the impact of PIPEDA on the problems, keep in mind the following potential stakeholders:

- Victims (seeking credit, access to banking or telecom services, jobs, security clearances, right to travel, etc)
- Perpetrators (for purposes of defending against, and prosecuting)
- Companies that hold personal information but are not the locus of the ID theft or fraud (telecom companies, banks, direct marketers, credit reporting companies, Canada Post)
- Companies where a fraudulent activity has taken place (retailers, credit grantors, banks, airlines etc.)
- Third party companies who process or pass on information (ISPs, domain name registrars, safe storage or document destruction firms, IT service companies)
- Employees of all of the above, who may be subject to enhanced scrutiny

Principle 1 — Accountability

> ***4.1*** *An organization is responsible for personal information under its control and* ***shall designate an individual or individuals who are accountable*** *for the organization's compliance with the following principles.*[53]

One of the most striking problems in the whole ID theft debate is the lack of accountability of the organizations which handle the personal data of ID theft victims. This includes:

- Businesses which do not protect personal information in the management cycle, and through whom identity thieves get the personal information necessary to conduct ID theft or fraud
- Credit grantors, who do not verify the identity of those posing as the individual
- Companies which attempt to cover their losses by pursuing the victims of ID theft, rather than the thieves themselves from whom they failed to secure accurate information or guarantees.

All three categories are covered by the first principle. It should also be noted that companies cannot escape accountability for personal information that belongs to someone who is not their customer, as in the South Carolina case cited in the preceding chapter, because the Challenge Principle (10) provides that anyone may challenge compliance to these principles, not just someone whose information is handled by the company. The duty of care is to follow this code of fair information practice for all personal information, not just that of a customer.

> ***4.1.2*** *The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.*

53 The Personal Information Protection and Electronic Documents Act, Statutes of Canada,

Another problem victims often complain about is the inability to find someone to help them. The name and coordinates of the designated officer, now often termed a Chief Privacy Officer, must be available on request.

> ***4.1.3*** *An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization* ***shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.***

This clause clearly establishes that an organization must take steps that have legal force, to transmit its responsibilities under this standard to any agents or third parties. "Comparable level of protection" should be better defined and understood for the purposes of the standard, but certainly for the management of information which constitutes a risk factor for identity theft, specific guidelines should be developed. Generally companies have a tendency to establish contracts with their business partners that stipulate the company will "adhere to all applicable law" or some other such phrase. Some might specifically name PIPEDA or other data protection law. However, in the context of rampant ID theft, what is required is a code of recommended practice for ID theft risk management, or specific security measures appropriate in each circumstance.

Clause 4.1.3 is also important because it is the only area in the Act where transborder dataflow issues are addressed. An organization remains responsible for information in its possession or custody, including information that has been transferred to a third party for processing, notably overseas or in the United States. We will discuss this further in Chapter 9 on the BC Maximus Contract Provisions.

> ***4.1.4*** *Organizations shall implement policies and practices to give effect to the principles, including*

This means all of the principles, including the safeguards principle. That ought to be construed as requiring a security policy, wherever ID information is held. The policy then dictates a set of management practices, which should be audited internally on a regular basis by the CPO or designate.

> *(a) implementing procedures to protect personal information;*

This includes various security practices, such as two factor authentication for clients wishing to change address or other data, clearing staff, establishing audit trails for access to information, restricting access to need to know, ensuring rotation of staff, etc.

> *(b) establishing procedures to receive and respond to complaints and inquiries;*

Since a lot of grief is occasioned by not having adequate systems to assist ID theft victims, this clause is critical. Clearly, it can be read to include setting up systems to assist those whose personal information has been either compromised by the company or

its associates, or to assist those who are alleging that accounts have been opened or abused by others.

> *(c) training staff and communicating to staff information about the organization's policies and practices; and*
>
> *(d) developing information to explain the organization's policies and procedures.*

This would include information about how individuals can protect their personal information, such as how to defend against Phishing and Pharming. A recent study done in Britain indicates that most individuals tested to see if they could detect phishing attacks were fooled; if companies are going to use the Internet for supplying services or billing, they must help their customers comply with safe computing practices. Such a high rate of failure indicates that awareness levels of risk are not keeping up with the threats. Customers, for their own safety, have to understand the procedures of the bank in order to differentiate them from the latest phishing attacker.[54]

Principle 2 — Identifying Purposes

> ***4.2*** *The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.*

As Perrin states in *The Personal Information Protection and Electronic Documents Act: An Annotated Guide (Irwin Law, 2001):*

> The standard requires that organizations identify the purposes for which they are collecting, using, and disclosing personal information, but is silent on the issue of whether those purposes are legitimate, fair, lawful, or acceptable to the individuals whose information is involved.

This situation has been rectified by section 5 of the Act, known as the reasonable person test, which states: "An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances." It is perhaps worth pointing out here that the reasonable purpose clause is not likely to help prosecute criminals with caches of personal information, because the Act does not apply to individuals, only organizations, and criminal rings are unlikely to declare themselves as such for the application of PIPEDA.

This should however act as a constraint on the wholesale and promiscuous gathering and use of personal information, which puts the individual at risk of ID theft. Unfortunately, this does not seem to solve the problem of data aggregators or brokers, whose very purpose is to gather every shred of data they can about an individual in order to sell it to clients, often for security purposes. Security, law enforcement, and fraud investigation usually trump data protection statutes, allowing collection without consent and often

[54] see www.bullguard.com

maintenance with no right of access for individuals. Just as credit reporting bureaus are covered by specific legislation, it is hard to see how data aggregators can stay in business if they are not to be constrained by specific legislation. In the meantime, at least they are under the oversight of the Privacy Commissioner in Canada and could be audited. Such an audit would yield useful information such as:

- The extent to which data brokers are operating in Canada
- The extent to which Canadian personal data is flowing into the hands of data brokers in the US or elsewhere
- The state of safeguards, security controls, and contractual provisions which pass on rights to the individuals
- Facts on which to base recommendations for sector specific regulation

Principle 3 — Consent

> ***4.3*** *The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.*
>
> ***4.3.1*** *Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).*
>
> ***4.3.2*** *The principle requires "knowledge and consent." 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.*** *(emphasis added)*
>
> ***4.3.3*** *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.*

The issue of consent is rarely helpful in the matter of ID theft, since usually data breaches, where they are the cause of the theft, involve information for which the individual has freely consented to collection, use and disclosure. Certainly, it would help if individuals became more activist, and refused to surrender information that is not necessary, or disclose it in ways that threaten its safety. A few examples may help illustrate this point.

While working on this project, the principal researcher tried out the application for a particular credit card while in the secure area of the airport. She added up all the mistakes that the person who was taking the application was making, and then terminated the transaction at the end. The following narrative is only a partial list; the example is not intended to focus on a particular company, but merely to point that if this is what happens in public in a face to face situation, what could be happening behind closed doors, or in another far distant jurisdiction? It was beyond the scope of this study to do a few "mystery shopper" exercises, but it would be an interesting exercise.

> The agent wrote out the application, making errors and asking me to spell out critical information such as name, address SIN number, in full hearing of others in the airport. Security inside the airport? She pointed to a box under the stall that held the completed applications, a box I could have walked off with when she went to the washroom. The secret suggested for recognition purposes was mother's maiden name, widely recognized as unacceptable by security experts. While the agent assured me the application would be processed in Canada, it is more normal for completed applications to be scanned and inputted outside the country where labour costs are lower. The agent could not tell me the details of the credit check and any implications that this application would have on my credit rating. She needed to see my ticket, and filled out the application on that basis, denying that there was any security risk inherent in the approach (they trusted the airlines, I was who I said I was because the airlines said so. Having wandered around airports in a jet-lagged state over many years and left my tickets on the bank machine, in the bathroom, and at the duty free desk, I doubt this is a secure method.) Finally, when I decided not to go ahead with the application, she tore up the application a couple of times and stuffed it in the nearest airport garbage bin…no shredder at the desk. I retrieved the pieces to shred myself, and I interpreted the odd glances from the agent to mean that by this time she thought she was dealing with a nut. Nevertheless, this is a good example of a situation where the individual would be well advised not to consent to the collection of so much information in this manner and with this apparent lack of security. While persons are becoming conditioned to saying no to information requests because of **what** is requested, or **what** it is to be used for (e.g. Marketing) they must also learn to say no because of **how** it is treated.

Individuals are well advised to stop consenting to the gathering of information over the internet, because of concerns about their ability to detect phishing or pharming scams. It is time to start asking companies to phone when there are problems with account information, and test them with a few questions only a bank or the particular retailer would know, such as credit limit, last major purchase, details of an older transaction, etc.

Unsolicited credit card applications and "convenience cheques" could be sent back in shreds with a demand for postage to be refunded. These marketing efforts put the individual at risk. Previous efforts of consumers to be compensated for the use of their marketing information, or for the waste of their time have not been particularly

successful. However forcing the burden of document destruction on consumers for junk mail they never wanted to receive in the first place is adding insult to injury.

> ***4.3.4*** *The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.*

Here we have an issue that is begging for complaints to be filed. One of the central complaints of advocates for victims' rights in the US, is that companies do not bother doing due diligence to ensure that someone who is applying for credit is who they say they are. They accept any old consent for the collection of personal information (the filling out of an application, in other words. The same is true for accepting address changes, although in the United States legislation is coming in some states which addresses this problem.) This paragraph dictates that organizations give due consideration to the sensitivity of the information collected, and take appropriate measures to get the right type of consent. We normally think of this in terms of opt-out boxes or requiring a written signature, but as ID theft grows, it seems clear we should also be thinking about requiring positive identification with the signature, and a verification process for the critical information such as address. The consent principle in PIPEDA is not just about whether you say yes, it is whether anyone else could say yes for you.

> ***4.3.5*** *In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained.* ***Consent shall not be obtained through deception.***

One of the problems here is that society as a whole has not caught up with the information industry. Even extremely well educated people working in the field were not aware of the existence of ChoicePoint, or how the database industry functions. Most people have no clue how the insurance industry works or credit reporting. Therefore the reasonableness test is a bit problematic; the fact is the general population cannot pass a basic facts test on what is happening with their information. This is an area that needs to

be rectified through consumer education. In the meantime, it would be helpful if people used the rights available to them under the openness principles and insisted on knowing where their data is going , who it is being shared with, and how long it will be kept. Then they can evaluate whether this meets their expectations.

The law can certainly, in our view, be read to require organizations to be absolutely explicit about what they are doing with information, in order that consumers are not deceived into giving information when it could be exposed to risk.

> ***4.3.8*** *An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.*

Many individuals have attempted, usually unsuccessfully, to withdraw their consent for the use of information once they have become ID theft victims. Once an organization is owed money, the victim is guilty until proven innocent. This makes sense, because if we considered the alternative, namely the ability for the thief to expunge records on the file which would incriminate them, there really is not a lot of choice in the matter. Issues surrounding free access to the files and ability to notate and send on the notations to other parties offer redress for this issue and will be discussed in the relevant sections of the law.

Principle 4 — Limiting Collection

> ***4.4*** *The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.*
>
> ***4.4.1*** *Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Clause 4.8).*
>
> ***4.4.2*** *The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.*
>
> ***4.4.3*** *This principle is linked closely to the Identifying Purposes principle (Clause 4.2) and the Consent principle (Clause 4.3).*

These requirements are quite clear and strong, and when applied to Phishing, Pharming, and spyware attacks, indicate that perpetrators are breaking the law in the following respects:

- Collecting too much information

- Collecting without authority, legitimate purpose
- Misrepresenting the identity of the collector
- Lying to the customer
- Failing to be transparent

Complaints could be filed, and cases taken to the Federal Court with a request for punitive damages. Not as satisfying as Criminal Code provisions, perhaps, but better than nothing. Anyone can file a complaint, so a Chief Privacy Officer of one of the many companies whose brands have suffered at the hands of these pirates could file a fairly impressive and well documented case. Whether the perpetrators could be actually found and prosecuted of course is another issue. It is unlikely they could be found to be engaged in commercial activity, but there may be situations where individuals are working for an organization that comes within the scope of PIPEDA.

With respect to the practices of legitimate companies, there is an issue here with respect to over-collection. If a company collects too much information, and keeps it all in one place, the risk of ID theft goes up tremendously. Process control would dictate that not all information be collected at once, lest there be a leak in that chain, and indeed in some of our examples, companies lost tapes or databases but there was no risk to consumers because the files were incomplete and had to be matched with other critical elements kept separately.[55]

Principle 5 — Limiting Use, Disclosure, and Retention

> ***4.5*** *Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.*
>
> ***4.5.2*** *Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.*
>
> ***4.5.3*** *Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.*

This principle deals with everyday use, disclosure, and retention. It links those to the original stated purpose; any new purpose requires documentation and a new consent.

[55] See AOL case, supra note

Some would argue that keeping large amounts of information in current use, particularly if there in ID material contained in it, is a risk for ID theft. Certainly this may be the case, and several of the items of U.S. legislation address such things as not putting social security numbers on ID documents (thereby keeping the number in everyday use, when it was required initially only to authenticate the individual, or for government purposes). We can look to this clause as the basis for complaints where companies insist on keeping ID data in circulation, or retaining data that is no longer necessary. Data protection law almost never discusses active files versus dormant storage, but surely the retention schedules which are recommended in 4.5.2, and the destruction guidelines required in 4.5.3 ought to make these distinctions and lay out best practice. This is an area where a guidance note could be useful.

Principle 6 — Accuracy

> ***4.6*** *Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.*
>
> ***4.6.1*** *The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information,* ***taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.*** *(emphasis added)*

The accuracy priniciple is often overlooked, but it is important in ID theft. One of the complaints that we hear most from the United States is that the "interests of the individual" are never taken into account, particularly where credit is being granted. Customer service representatives will change address information without proof or assurance of whom they are dealing with. After an ID theft takes place, victims call back countless times trying to get the record to reflect their side of the story. Victims put blocks on their files to stop new credit being granted, yet new accounts continue to proliferate.

This clause provides a mandatory requirement that the "interests of the individual" are what is at play here, not those of the company. Clearly, a company will spend the time and effort to get information that is accurate enough for their purposes, without being told, but the law in fact curbs their tendency to do automatic updates of information they don't need in section 4.6.2. A company that is not taking steps to check the accuracy of its records, and thereby exposes an individual to ID theft, would be violating a clear provision in 4.6.1.

> ***4.6.2*** *An organization shall not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected.*
>
> ***4.6.3*** *Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate*

and up-to-date, unless limits to the requirement for accuracy are clearly set out.

Another common complaint of victims is that inaccurate information continues to pour from the originating company or the credit bureaus, to all manner of third parties, and it is next to impossible to set the record straight. Section 4.6.3, coupled with the rights of access, correction and notification laid out in section 9, provides a substantive requirement to address this problem.

Principle 7 — Safeguards

4.7 *Personal information* ***shall be protected by security safeguards appropriate to the sensitivity of the information.***

4.7.1 The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. *Organizations shall protect personal information regardless of the format in which it is held.*

This is a strong, clear, mandatory provision that covers most of the issues associated with ID theft. We have no recommendations to improve it at this time.

4.7.2 *The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.*

4.7.3 *The methods of protection should include*

(a) physical measures, for example, locked filing cabinets and restricted access to offices;

(b) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and

(c) technological measures, for example, the use of passwords and encryption.

Most data protection statutes are vague about security measures. The Health Insurance Portability and Accountability Act (HIPAA) of the U.S., authorized regulations for security of health records which just took effect in April 2005. It is difficult to be more precise than PIPEDA in a general privacy statute, and certainly lawyers have been reluctant to stride into the arena of the IT security experts. However, more precision is required if companies are to understand what is expected of them in terms of a duty of care to their customers and individuals who become victims of ID theft through their carelessness.

When the CSA Standard was drafted, this weakness, and that of its root document the OECD Guidelines, was noted. Standards refer to other standards, and a promising management standard for security was in the process of being drafted in the United Kingdom at the time, BSS 7799. The experts' committee actually looked at the standard in its meetings, and the security principle was not made more precise because it was felt that other standards would emerge to fill this gap. This has taken a very long time, but ISO 17799 is about to be approved in a new improved version, based on that original British Standard. We examine what it can do to assist in the matter of ID theft in Part II , but note that the principle states that information shall be protected through safeguards appropriate to the sensitivity of the information. ID information has now been recognized as very sensitive, because the risk continues to escalate, but what is the nature of the safeguards appropriate to such sensitive information? ISO 17799 will soon be accepted as the standard for due diligence, but critics state it is still not specific enough. We discuss the powers of the Privacy Commissioner later in the chapter, but note that issuing a guidance note on best practice to prevent ID theft is well within her competency under PIPEDA.

4.7.4 *Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.*

As Perrin states:[56]

> Clause 4.7.4 imposes an obligation to train personnel about the importance of maintaining confidentiality. This obligation adds to and provides specificity to the obligation expressed in 4.1.4 to establish procedures and to train staff. This obligation has received little focus in the debate about the legislation, but it is a substantive one and no doubt will be the focus of investigations where a security breach results in the release of personal information. This requirement will be important in the investigation of complaints, but also in the context of the Privacy Commissioner's audit powers.
>
> During the Parliamentary debate, concern was expressed over whether or not the audit powers of the Commissioner were intrusive, and the Act requires the Privacy Commissioner to have reasonable grounds to believe that the obligations of the Act are not being observed before he embarks on an audit of an organization.
>
> The Dutch Data Commissioner observed at a recent conference[57] that the way they go about doing their informal audits is by calling the company and asking a few questions of company staff concerning their policies and procedures. In the event that staff fails to get a passing grade on these questions, they say, "Well, that is not really a good answer. I think we will come in and have a look at your practices."

[56] *The Personal Information Protection and Electronic Documents Act: An Annotated Guide*, p.37
[57] Computers, Freedom and Privacy Conference (Washington, D.C., April 1999).

> Clauses 4.7.3 and 4.7.4 will give the Privacy Commissioner of Canada ample justification to do the same thing, and given the state of awareness of security measures generally and the likelihood most staff would fail such a test, it is an area that should receive immediate attention in compliance plans.

Arguably this is truer now than when written in 2001, with ID theft so rampant, and employees often being the victims of social engineering on the part of the thieves.

> ***4.7.5 Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information*** *(see Clause 4.5.3).*

This is a substantive requirement, echoing the obligations in 4.5.3 but specifically instructing organizations that they may not carelessly allow unauthorized parties to gain access to the information. This should be read as a substantive requirement to render personal information permanently illegible when disposing of all media.

Principle 8 — Openness

> ***4.8*** *An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.*

Again, quoting Perrin[58]:

> This obligation is transformative and far-reaching but has received very little publicity. The principle states the obligation to make specific information available about policies and practices relating to the management of personal information. European data protection law often contains obligations of "notification," but this provision goes much further by imposing an obligation to document policies and procedures concerning the handling of personal information, and make those policies available to the individual. The Openness principle of the OECD Guidelines merely states:
>
> > There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
>
> The standard is much more explicit.

Individuals have not taken full advantage of this clause during the first five years of the Act. Consumer groups, especially those offering services to victims, ought to systematically ask for the policies and procedures with respect to:

---

58 *Ibid.*, P. 38

- Document destruction
- Authentication requirements for access to one's own information, and to make address changes or increase credit limits
- Notification procedures in the event of disputes over fraud
- Contract clauses with third parties which stipulate obligations to protect information as it is protected in Canada under PIPEDA. It is unlikely that companies will release this information, but in the course of investigating a complaint, at least the Privacy Commissioner would have the opportunity to see if they have any specific language about protection, recognizing the risk of ID theft.
- The chain of sharing for their personal information (which companies and why, which countries)
- Case law in outsourcing venues, which would reveal evidence of successful prosecution of ID thieves.

> ***4.8.1*** *Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.*
>
> ***4.8.2*** *The information made available* ***shall*** *include*
>
> *(a) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;*
>
> *(b) the means of gaining access to personal information held by the organization;*
>
> *(c) a description of the type of personal information held by the organization, including a general account of its use;*
>
> *(d) a copy of any brochures or other* ***information that explain the organization's policies, standards, or codes; and***
>
> *(e)* ***what personal information is made available to related organizations (e.g., subsidiaries).***

Principle 9 — Individual Access

> ***4.9*** *Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.*

This is a basic right but one that has frustrated ID theft victims in the US. In particular, activists have complained that data brokers will only give access to a customer version of

what they have, while businesses get access to different databases, yielding a much longer, fuller, and potentially inaccurate report. There is no way of challenging the accuracy of reports in such a system. PIPEDA provides this right with a few hurdles specified below and in section 9 of the Act. Section 9 provides that an organization can refuse access to information if revealing it would interfere with an investigation or jeopardize national security.

> ***4.9.1*** *Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.*
>
> ***4.9.3*** *In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the* ***organization shall provide a list of organizations to which it may have disclosed information about the individual.***

Companies have argued that telling the individual who has their data amounts to releasing a customer list, and they argue that rival companies will use their employees to file access requests and find out who their customers are. This may be true, but it is certainly a lesser evil than having a citizenry who do not have to right to find out who has their personal information.

> ***4.9.4*** *An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.*

The issue of credit scoring has already come before the Privacy Commissioner of Canada. As algorithms and statistical techniques are increasingly used to score individuals across a range of variables, it is very problematic that companies may use the commercial confidentiality provisions in PIPEDA to protect their proprietary algorithms. Since rival companies consider this to be their secret to better risk analysis and therefore profitability, they will continue to protect these formulae and techniques. We would argue that when many decision making processes that affect individuals throughout society are made by software and machines, those processes have to be open. Courts of Law became open because the citizenry demanded it and it became imperative for leaders to demonstrate

fairness. The same holds true for 'code' in today's information society, to borrow Larry Lessig's famous terminology.[59]

> ***4.9.5*** *When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required.* ***Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.***

Having the records changed to reflect the reality of identity theft is one of the bigger challenges in the US, and legislation has been enacted in various states to ensure that the records actually are amended and passed on to others. This paragraph provides for all elements of that right, but it might be useful to standardize forms to ensure that all recipients of the data are following standard procedures. Furthermore, it must be recognized that all of this customer service, however necessary, has a cost and that standardized repeatable processes will bring those costs down.

> ***4.9.6*** *When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.*

In situations where the individual has failed to persuade the organization of his side of the story, it is appropriate that the dispute be placed on the file in a timely manner. This could be standardized in the case of ID theft as an alert, prior to proving the facts. However, the fraud alert system appears to be working in Canada.

Principle 10 — Challenging Compliance

> **4.10** *An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.*

The right to challenge compliance with the standard and the law is available to all individuals, not just a person whose information is at play. This effectively means that consumer advocates or security experts could complain when they find practices to be sub-standard. An ID theft resource centre could encourage victims to take cases to Court where the facts warrant it, after complaining to the Privacy Commissioner. A few damage awards might have the effect of improving adherence to best practice.

[59] Lessig, Larry: *Code and Other Laws of Cyberspace*, (Basic Books, 2000)

> **4.10.1** *The individual accountable for an organization's compliance is discussed in Clause 4.1.1.*
>
> **4.10.2** *Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.*
>
> **4.10.3** *Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist. For example, some regulatory bodies accept complaints about the personal-information handling practices of the companies they regulate.*
>
> ***4.10.4*** *An organization shall investigate all complaints.* ***If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.***

The last three sections of the standard provide that organizations must:

- put procedures in place to respond to complaints about ID theft or conditions that could lead to it, such as sloppy practices
- assist complainants and make them aware of where they can complain outside the organization, such as credit bureaus, other ombudsmen, the CRTC, or the Privacy Commissioners
- take measures to respond to well founded complaints, including amending practices

These requirements in the standard have now been reinforced in the law by sections 11(1) which provides a right to complain to the Commissioner, and 14(1) which provides the right to complain to the Federal Court upon receipt of the Commissioner's report.

It seems clear that there are a great many mandatory requirements in the standard itself, that address issues that contribute to identity theft, and provide grounds for complaint under the Act. Although the Commissioner does not have binding powers under the law, she does have a number of powers that could help in dealing with the problem, including taking a matter to Federal Court on her own, or assisting an individual in going to Court to obtain damages. The B.C. Commissioner has the power to make an order and to fine organizations, as does the Alberta Commissioner. However, if the Federal Commissioner were to act for an individual or a group of individuals and take a case to Federal Court, there is a tremendous potential for damage awards to assist consumers.

The following section addresses the powers of the Commissioner, with a few suggestions as to how the issue of ID theft could be addressed. Once again, we have quoted relevant sections of the Act that could be useful.

Section 11: Filing of Complaints

11.*(1) An individual may file with the Commissioner a written complaint against an organization for contravening a provision of Division 1 or for not following a recommendation set out in Schedule 1.*

Clearly the individual, either the ID theft victim, or an organization such as BCFIPA who could act for victims, may launch a complaint against an organization for either precipitating the ID theft through sloppy practices or failing to help in correcting information. It must be remembered that since ID thieves are rarely going to identify themselves as companies, PIPEDA will not often apply to the perpetrators. Civil liberties groups may nevertheless want to get organized to file complaints on behalf of their clients and take a case against an organization to Federal Court.

Commissioner may initiate complaint

(2) If the Commissioner is satisfied that there are reasonable grounds to investigate a matter under this Part, the Commissioner may initiate a complaint in respect of the matter.

Notice

(4) The Commissioner shall give notice of a complaint to the organization against which the complaint was made.

Section 12: Investigations of Complaints

Powers of Commissioner

12.*(1) The Commissioner shall conduct an investigation in respect of a complaint and, for that purpose, may*

(a) summon and enforce the appearance of persons before the Commissioner and compel them to give oral or written evidence on oath and to produce any records and things that the Commissioner considers necessary to investigate the complaint in the same manner and to the same extent as a superior court of record;

(b) administer oaths;

(c) receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Commissioner sees fit, whether or not it is or would be admissible in a court of law;

(d) at any reasonable time, enter any premises, other than a dwelling- house, occupied by an organization on satisfying any security requirements of the organization relating to the premises;

(e) converse in private with any person in any premises entered under paragraph (d) and otherwise carry out in those premises any inquiries that the Commissioner sees fit; and

(f) examine or obtain copies of or extracts from records found in any premises entered under paragraph (d) that contain any matter relevant to the investigation.

This is an extensive suite of administrative powers which seem adequate to investigate the circumstances of ID theft, apart from the problem of the individual thief not being covered by PIPEDA or any other provincial legislation.

> *(3) The Commissioner may delegate any of the powers set out in subsection (1) or (2)*

It is important to note here that the Commissioner may delegate to a wide variety of officials, not just members of her own staff. She could establish a joint working group to investigate ID theft and empower them to investigate complaints which come to her, under this provision of the Act. She could prepare a special report to Parliament, possibly in concert with her provincial colleagues, and seek funding to set up a working task force empowered to investigate and take to Federal Court cases that fall within her jurisdiction, seeking damages for the victims.

We will not go into detail on the Reporting powers and obligations of the Commissioner, except to state that there should be prominence and expediting processing granted to cases involving ID theft. There has been quite a bit of controversy in Canada already on the subject of "naming names" and on publishing the details of each investigation. B.C.FIPA has come out strongly in favour of publishing the details and the names of the companies, in the interests of motivating parties to achieve better compliance with the law, and where ID theft is at play, it seems obvious that there is a public interest in disclosure to protect other individuals from exposing themselves to risk.

The following provisions respecting the powers of the Federal Court and the ability of the Commissioner to go to Court either independently or to support victims of ID theft are worth exploring. There have only been 15 Federal Court cases in the first five years of application of the law. If the Commissioner were to assume a more proactive role in pursuing this avenue with respect to ID theft, it could be very powerful.

> ***Section 14: Review by the Federal Court***
>
> ***Application***
>
> ***14.****(1) A complainant may, after receiving the Commissioner's report, apply to the Court for a hearing in respect of any matter in respect of which the complaint was made, or that is referred to in the Commissioner's report, and that is referred to in clause 4.1.3, 4.2, 4.3.3, 4.4, 4.6, 4.7 or 4.8 of Schedule 1, in clause 4.3, 4.5 or 4.9 of that Schedule as modified or clarified by Division 1, in subsection 5(3) or 8(6) or (7) or in section 10.*
>
> ***Section 15: Commissioner's Application for Review***
>
> ***Commissioner may apply or appear***
>
> ***15.*** *The Commissioner may, in respect of a complaint that the Commissioner did not initiate,*
>
> *(a) apply to the Court, within the time limited by section 14, for a hearing in respect of any matter described in that section, if the Commissioner has the consent of the complainant;*

(b) appear before the Court on behalf of any complainant who has applied for a hearing under section 14; or

(c) with leave of the Court, appear as a party to any hearing applied for under section 14.

Section 16: Remedies

16. *The Court may, in addition to any other remedies it may give,*

(a) order an organization to correct its practices in order to comply with sections 5 to 10;

(b) order an organization to publish a notice of any action taken or proposed to be taken to correct its practices, whether or not ordered to correct them under paragraph (a); and

(c) award damages to the complainant, including damages for any humiliation that the complainant has suffered.

Obviously the ability of the Court to award damages has considerable interest for victims and for organizations such as the BCFIPA who would be interested in setting up victim assistance centres. At the very least, information on how to take a case to Federal Court could be made available to victims of ID theft.

Finally, the Commissioner has extensive audit powers which have not been used in the private sector. Auditing of security practices in particular would be useful, and publishing the results and recommendations stemming from such an audit would be educational for business.

Section 18: Audits

To ensure compliance

18.*(1) The Commissioner may, on reasonable notice and at any reasonable time, audit the personal information management practices of an organization if the Commissioner has reasonable grounds to believe that the organization is contravening a provision of Division 1 or is not following a recommendation set out in Schedule 1, and for that purpose may*

(a) summon and enforce the appearance of persons before the Commissioner and compel them to give oral or written evidence on oath and to produce any records and things that the Commissioner considers necessary for the audit, in the same manner and to the same extent as a superior court of record;

(b) administer oaths;

(c) receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Commissioner sees fit, whether or not it is or would be admissible in a court of law;

(d) at any reasonable time, enter any premises, other than a dwellinghouse occupied by the organization on satisfying any security requirements of the organization relating to the premises;

(e) converse in private with any person in any premises entered under paragraph (d) and otherwise carry out in those premises any inquiries that the Commissioner sees fit; and

(f) examine or obtain copies of or extracts from records found in any premises entered under paragraph(d) that contain any matter relevant to the audit.

Delegation

(2) The Commissioner may delegate any of the powers set out in subsection (1).

Once again, the Commissioner can delegate any of these powers and could enter into cooperative arrangements with other parties such as other Commissioners, auditors working for them both, or police departments to facilitate the investigation of ID theft.

Section 19: Audit Reports

Report of findings and recommendations

19.*(1) After an audit, the Commissioner shall provide the audited organization with a report that contains the findings of the audit and any recommendations that the Commissioner considers appropriate.*

Reports may be included in annual reports

(2) The report may be included in a report made under section 25.

While there are lots of press reports on ID theft occurrence, a sustained reporting on how to minimize risk could be developed by the Commissioner which would assist in remedying the situation. She could run such a watching brief on her website, adding cases as they come to her and providing new advice as new events happen, such as new phishing attacks or warnings. Her recommendations after an audit or investigation could be released either in the annual report as indicated above, in a special report to Parliament, or as a release in the public interest as indicated below. In fact, if breach disclosure legislation is not forthcoming with the Justice Canada revisions to the Criminal Code, the Commissioner at least could release situations of breach of personal information in the public interest.

Public interest

(2) The Commissioner may make public any information relating to the personal information management practices of an organization if the Commissioner considers that it is in the public interest to do so.

The following provisions are interesting in the context of the participation of the Federal Commissioner in a task force or association of parties working together to investigate, prosecute, and seek remedies for ID theft.

Disclosure of necessary information

(3) The Commissioner may disclose, or may authorize any person acting on behalf or under the direction of the Commissioner to disclose, information that in the Commissioner's opinion is necessary to

(a) conduct an investigation or audit under this Part; or

(b) establish the grounds for findings and recommendations contained in any report under this Part.

Disclosure in the course of proceedings

(4) The Commissioner may disclose, or may authorize any person acting on behalf or under the direction of the Commissioner to disclose, information in the course of

(a) a prosecution for an offence under section 28;

(b) a prosecution for an offence under section 132 of the Criminal Code (perjury) in respect of a statement made under this Part;

(c) a hearing before the Court under this Part; or

(d) an appeal from a decision of the Court.

Disclosure of offence authorized

(5) The Commissioner may disclose to the Attorney General of Canada or of a province, as the case may be, information relating to the commission of an offence against any law of Canada or a province on the part of an officer or employee of an organization if, in the Commissioner's opinion, there is evidence of an offence.

Section 23: Consultation with Provinces

23.*(1) If the Commissioner considers it appropriate to do so, or on the request of an interested person, the Commissioner may, in order to ensure that personal information is protected in as consistent a manner as possible, consult with any person who, under provincial legislation that is substantially similar to this Part, has powers and duties similar to those of the Commissioner.*

Agreements

(2) The Commissioner may enter into agreements with any person with whom the Commissioner may consult under subsection (1)

(a) to coordinate the activities of their offices and the office of the Commissioner, including to provide for mechanisms for the handling of any complaint in which they are mutually interested;

(b) to undertake and publish research related to the protection of personal information; and

> *(c) to develop model contracts for the protection of personal information that is collected, used or disclosed interprovincially or internationally.*

It is not our impression that these powers have been used extensively, and they provide a strong basis for working collaboratively across jurisdictions and with other interested parties such as the Commissioners of B.C., Alberta and Quebec, the police, the Antiphishing Working Group, and other federal parties such as the Competition Bureau. Working together and collaboratively, all of these groups could pool their knowledge and use their powers maximally to achieve some protection and redress for individuals. One of the central problems in investigating and prosecuting ID theft at the moment is the lack of criminal code provisions, which hampers the ability of law enforcement to act. Using the powers of the Commissioner to investigate personal information breaches and complaints is no substitute for necessary legislation, but it could help to put pressure on the situation at the moment. There is of course a role for public interest groups such as BCFIPA and CIPPIC to participate as well.

> *Section 24: Promoting the Purposes of the Part*
>
> ***24.*** *The Commissioner shall*
>
> *(a) develop and conduct information programs to foster public understanding, and recognition of the purposes, of this Part;*
>
> *(b) undertake and publish research that is related to the protection of personal information, including any such research that is requested by the Minister of Industry;*
>
> *(c) encourage organizations to develop detailed policies and practices, including organizational codes of practice, to comply with sections 5 to 10; and*
>
> *(d) promote, by any means that the Commissioner considers appropriate, the purposes of this Part.*

Obviously this is a broad mandate to do research and publish information that could help both consumers and business cope with the problem of ID theft. We need further research on a number of areas outlined in this report, such as:

- How improved authentication techniques could help prevent ID theft without compromising privacy
- How to detect phishing and pharming attacks
- Best practices for consumers to follow in keeping their home computers free of viruses, spyware, malware of all kinds, and how to participate in safe e-commerce and e-banking.

If the office were to perform a few security audits of companies and develop recommendations for detailed codes of practice, this could assist in raising the bar for company practices.

8. Recommendations

While there is a lot going on with respect to ID theft issues, the problem continues to grow. It seems to us that collaborative effort and full transparency of all parties is required. We simply do not have enough resources to tackle this job in an ad hoc way, as we see the United States doing, and it is possible in Canada to work together collaboratively on shared solutions to common problems. We think that the Commissioner is in a unique position to provide some leadership on three key aspects of this problem:

1. Collaboration with interested parties (the Act specifically sets it out as listed above)
2. Investigation and redress in Court for victims
3. Public Education and awareness, including providing guidance for companies on their responsibilities.

The following recommendations are an attempt to focus our observations around a few core themes. They are far from exhaustive, but if we could get concerted action in these areas we are optimistic that progress would be made.

1. Research

Do further research on company practices and ID theft risk

As indicated, our attempts to get response to a survey were not as successful as we had hoped. It is likely that other parties such as Industry Canada or the OPC could get better response rates to the questions raised in our questionnaire, because of the ability to provide assurances of confidentiality. Certainly the Commissioner is able to go in and audit or investigate in the event that companies are not interested in responding to research queries, so there is a way of getting the information in spite of initial reluctance. We would recommend that further research be done on actual company practices and security protocols. Such research could pave the way for recommendations for company best practices.

In particular, we would highlight the fact that the country appears to be pregnant with an identity card that has not yet been formally proposed or brought to Parliament, although the Citizenship and Immigration committee canvassed the idea in 2003. We would not want to see a national ID card brought in on the grounds that it will help fight ID theft. Further research on authentication techniques and identity management, in our view, would support our belief that there are many efforts to stop ID theft that are much cheaper, less privacy invasive, and ought to be tried before even suggesting a national identity card. Nevertheless, civil liberties groups across the country report that they are monitoring developments which look suspiciously like the development in incremental

steps of a national ID card and information system. The standardization of drivers' licences, RFIDS in the passport, and continuing discussions of the Citizenship and Immigration Committee on biometrics all lead us to conclude that ID card is alive and well and gestating somewhere in government.

If the national identity card is born in Canada with ID theft as a reason, we will have been remiss in our responsibilities to do the research to prove that other methods could have sufficed.

2. Collaboration

The OPC should take leadership in collaborating with other parties in investigating, auditing, and educating on ID theft, relying on the extensive powers in PIPEDA.

The Commissioner should take the lead in exploring further collaboration with her counterparts in other provinces, with any of the groups working in Canada on the ID theft issue, and with public interest and consumer groups such as BCFIPA, PIAC, Options Consommateurs and CIPPIC, to establish a task force to fight ID theft and seek redress for victims. This could stem from a workshop or conference on ID theft, which we are interested in holding in the near future. Many parties have powers that they might be able to exercise in the context of such a task force. However, at present and absent new legislation, these existing powers are not as effective as they could be if employed cooperatively. Specifically:

- Police lack information and resources to investigate each case of ID theft but possibly could act if supplied information that the commissioners developed during their own investigation
- Commissioners cannot enter a dwelling house nor find against individuals who are not part of an organization subject to privacy legislation, even if the trail leads to the door. Police might be able to assist and carry on where the Commissioners cannot.
- Commissioners are able to publicise their findings from investigation and audit, can do special reports, can publish in public interest.
- The Privacy Commissioner of Canada has a specific role to play in collaborating and consulting with other commissioners where legislation has been deemed substantially similar (Quebec, B.C. and Alberta). This provision of the act could be interpreted to facilitate the establishment of a committee rather like the European Union's Article 29 Group, or Working Party on Data Protection, which has been extremely useful in Europe in promoting the purposes of the Directive, harmonizing approaches, and influencing industry behaviour. Given the current emphasis on transborder dataflow and the fact the ID theft is a hugely transborder problem, a working group of Commissioners focussing on specific issues could be very useful.

3. Specific Guidance

Develop specific guidance on best practice for companies, emphasizing risk analysis focussed on ID theft, expected security practices following guidance as provided by ISO 17799, and compliance with the requirements of PIPEDA.

While considerable advice addressed to consumers has been published, the value of that advice to prevent ID theft has been seriously questioned. However, there is practically no guidance to companies about best practices for preventing ID theft. Educating data processors should be both easier and more effective than educating data subjects. This is a significant problem, and we believe that commissioners should be proactive in publishing guidance on what is expected of companies. The guidance could be targeted specifically to the problem of ID theft, or it could range across the broad issues that affect ID theft, such as employee clearance and accountability, security practices, etc. A few key points to address in such guidance are:

1. Security management, and specifically compliance to ISO 17799 with a view to the protection of personal information in the context of the prevailing risk of ID theft
2. How to assess ID theft risk, using the PIA process which already exists
3. Destruction of documents
4. Employee clearance, accountability, and surveillance
5. Providing assistance to victims
6. Contractual clauses for transborder dataflow (as described in Part II, many useful ideas can be gleaned from the Maximus contract provisions which resulted from the B.C. Patriot Act case)

4. Redress

Initiate legal actions to seek redress and damages for the victims of ID theft and for persons whose personal information has been recklessly exposed to risk.

The overwhelming impression we get when viewing the situation, particularly in the United States, is that absent any form of liability for companies, fundamental and effective change may be difficult to achieve. The balance sheet is still positive for companies recklessly granting credit or not protecting personal information of customers. The current spate of publicity over data breaches has been effective in bringing the issue to public attention and in punishing companies with lax security through adverse publicity. However, the publicity has not changed the indifference of many credit grantors to the financial losses from identity theft because the companies continue to be

able to recover those losses through higher rates to consumers. The credit bureaus have actually benefited when companies purchase credit monitoring services for consumers whose records suffered from security lapses. In short, market incentives to address ID theft can be unpredictable, ineffective, and counterintuitive.

We need that to change, and in Canada the Privacy Commissioner has the power to take cases to the Federal Court. Since this is a power that has not been used to date, we urge the Commissioner in the strongest terms to use it and recommend to the Court that damages be awarded to victims and individuals whose information has been compromised and who must live with the reality of looming ID theft.

5. Mandatory Breach Notification

Introduce legislation requiring mandatory breach notification in cases where consumers are at risk of ID theft.

While we thoroughly endorse the concept of breach notification to consumers, there is a risk that if consumers are notified every time a minor security breach occurs, breaches will soon cease to attract attention. Nevertheless consumers have a fundamental right to know when someone has disclosed their information, and arguably under PIPEDA one could read in a requirement to seek consent for a new purpose after the fact. When PIPEDA is reviewed in 2006, clarity could be provided through the addition of a provision to require mandatory notification when there is reason to believe a breach has occurred which puts individuals at risk of ID theft. Notice is very useful in appropriate instances, especially when accompanied by affirmative consumer assistance such as free credit reports, free credit monitoring services, and individual assistance to potential victims.

It is easy for the Commissioner to announce in the public interest when an investigation reveals a problem. Participating in collaborative efforts, as described in recommendation 2, will ensure that more cases come to her attention. She can also encourage cooperation with industry, through the Ombudsman role, and establish a common ground where leaders in the industry might agree to voluntary disclosure under agreed circumstances. This could then, if successful, be the basis for successful regulation for mandatory disclosure.

6. Public Education

Improve public education and provide advice on how individuals can seek redress and play a more active role in fighting ID theft.

Motivated consumers with a connection to the Internet can find guidance on how to protect themselves from ID theft, and we felt no need to improve on those recommendations offered on the PIAC and Privacy Rights Clearinghouse websites. Unfortunately most consumers are passive, however, and are not playing an active role in ensuring a healthy marketplace. Public education needs to be focussed on empowering

consumers, including those most at risk such as the elderly, and young people who need to be educated to enable them to be full and active participants in the information society.

ID theft attacks are becoming more sophisticated, however, and there is a continual need to keep these consumer education materials fresh. The collaborative effort mentioned in recommendation 2 could help ensure scarce public education dollars are well spent. In the meantime, there needs to be more focused advice on what consumers should be demanding from organizations, and specific advice on how to do the following:

- Report Phishing attacks
- get off mailing lists, reject convenience cheques and unsolicited credit card offers
- report bad security practices
- complain to Privacy Commissioners
- seek redress

7. Legislative Changes

Amend the Criminal Code to make the prosecution of ID thieves more achievable, including provisions concerning the possession of ID documents without a reasonable purpose. Review the various legislative provisions which could be useful in filling the identified gaps in PIPEDA and the substantially similar provincial legislation.

We have attempted in this report to list a wide variety of legislative proposals which have been brought forward to remedy specific aspects of ID theft, and provide assistance to consumers. Many of these are not necessary because we have PIPEDA and the provincial substantially similar legislation, but there are gaps. The consultation document which the Department of Justice sent out in the fall of 2004 looked at criminal code provisions, but there is a need for a task force to look at the problem holistically, identify where different types of protection may be needed, and fill those identified gaps. The Privacy Commissioners of Canada should play a key role in such a project.

8. Transborder Data Flow Issues and Mutual Assistance Treaties and Arrangements

Accelerate the establishment of mutual assistance arrangements for the prosecution of ID theft, and include mutual assistance for the investigation of privacy breaches.

The prosecution of certain types of ID theft is further complicated by the fact that the perpetrators can do the work from outside the jurisdiction where the individual resides. Because the transborder dataflow provisions of PIPEDA are weaker than those of, for

instance, the European Union, it is difficult if not impossible to do anything once data has left the country. Consumers have no effective redress where the data breaches take place outside the country, other than to sue a company in a foreign jurisdiction, a proposition which is just too onerous for the average individual to undertake. Most contractual provisions in subcontracting or outsourcing arrangements do not provide consumer rights, they mostly transfer liability from one company to another without granting status to individual consumers.

The Competition Bureau has existing arrangements with the Federal Trade Commission for the investigation of fraud and telemarketing fraud, and we understand that they are interested in working together on ID theft. These arrangements should be accelerated so that thieves can be prosecuted expeditiously. We also believe that mutual assistance agreements should be arranged to facilitate the investigation of privacy breaches involving Canadian data in the United States and anywhere it has been sent for processing through arrangements made in the United States.

Appendix A: Questionnaire for Business

In order to determine what steps businesses were taking to improve data practices, we did a telephone/email survey of a number of key players. Most representatives were not willing to have their comments on the record, because of time constraints in getting clearance from their companies, because of the extremely tense situation with respect to ID theft in the news, and because generally it has always been difficult to get companies to report on these issues. It is not an accident that we really do not have a good analysis of the risk situation for data management. It is extremely difficult to get good documentation on what is going on, probably because many data managers are not comfortable with the risk they currently are running.

Many stakeholders, from IT managers, to security professionals, to auditors and privacy commissioners, are looking for guidance on security, and recommendations with respect to what constitutes due diligence. We did not get enough response from this short survey to develop that analysis. However, the feedback on the questions is positive.

Preamble

The BC Freedom of Information and Privacy Association was one of the successful applicants for a research grant on privacy issues in 2004-5, funded by the Office of the Privacy Commissioner of Canada. The project is to analyze the risks of ID theft in Canada, to review the Personal Information Protection and Electronic Documents Act with a view to determining whether or not it is a useful instrument in protecting the individual against ID theft, and to develop recommendations for action and guidance. We are interested in hearing the views and experiences of businesses in dealing with this growing problem, and would like to ask you a few questions. The comments will be used in the report without attribution unless you specifically authorize quotation.

Definitions and Scope of the Problem:

1. Has ID theft arisen as an issue in your business, and have you taken particular initiatives to fight it? Such as:

- Education and awareness of staff
- Education and awareness of clients
- New security measures
- New ID verification measures
- Discontinuing certain practices
- Investigations and audit

2. How do you define ID theft in your organization?

3. Who is responsible for spearheading activities?

4. Have you had any particular experiences or incidents you are able to describe to us?

Risk Analysis

5. What are your biggest areas of risk for ID theft?

- Insider abuse
- Improper document disposal
- New accounts
- Account change information
- Internet attacks

6. Do you have any idea of the costs of ID theft and fraud in your organization? How are the numbers derived, and whose budget does it come from?

7. How do you do risk assessment with respect to your personal information holdings? Have you done formal Privacy impact assessments and TRAS for you data holdings? If so, please describe.

Actions

8. There are a number of activities going on in Canada and the United States to combat ID theft. Is your company involved in any of these?

- Industry Canada working group
- Federal provincial working group
- Bankers Association
- Other industry association
- Justice Canada consultation

9. Have you issued warnings or provided information to your customers? How is this managed and is it integrated with your privacy policy?

10. What steps do you take to help individuals who come to you claiming to be victims of ID theft?

11. How do you dispose of your personal information? Do you use outside shredding and disposal companies, and if so, are you satisfied with the service?

12. Have you amended your authentication procedures, either online or in person or by telephone? If so, please describe.

13. Is the SIN number a concern in your organization?

14. How do you manage your outsourcing? Is the management of personal information specifically dealt with in the contracts, and do you have any experience of auditing compliance?

Recommendations

15. Do you have any suggestions for legislative change?

16. What role do you think governments should play in re-habilitating victims of ID theft?

17. Does existing privacy law deal with the problem?

18. Do you think there is a need for a technological fix for this problem, and if so what is it?

19. Can you imagine a role for a national ID card, and if so what would its functionality be, and who would pay for it?

20. Any further comments?