IDENTITY THEFT AND CONSUMER PROTECTION: FINDING SENSIBLE APPROACHES TO SAFEGUARD PERSONAL DATA IN THE UNITED STATES AND CANADA

by

Kamaal Zaidi

INTRODUCTION

In the information age, advances in technology have allowed commercial transactions to be conducted with greater ease and efficiency. In particular, online transactions often require an exchange of personal data among consumers, businesses, government agencies, and financial institutions. However, the dissemination of personal data in the marketplace allows strangers to acquire personal identifying information from consumers or institutions, often without their knowledge. Standing in the place of the consumer, these identity thieves can use this information for personal gain, giving rise to crimes known as identity theft. Identity theft is one of the fastest growing crimes in society, and is becoming a major public policy concern for consumers and legislators. New protective measures are being introduced, both as legislative reforms and technological innovations, to protect ordinary consumers. As part of these safety measures, many financial institutions handling personal data of the victimized consumer now issue credit reports on their behalf, or provide advance notice and an opportunity to correct the nature of personal information when there is suspicious handling activity of the consumer's personal data.

This paper examines identity theft in the United States and Canada, and how various jurisdictions are dealing with this emerging crime. More specifically, the paper intends to provide a comparative perspective with respect to legislative frameworks and technology-driven consumer strategies (such as online techniques) of reporting crimes and restricting access to personal data. As will be seen, modern identity theft legislation (often couched in the context of privacy legislation) provides a bundle of rights to consumers to shield themselves from those individuals acquiring sensitive personal data

in order to assume their identities. The author argues that vigilance through legislative and technology-driven approaches will ultimately protect the personal data of consumers under varying circumstances, and will serve as a foundation for pragmatic consumer protection policies in the future.

Part I defines identity theft in all its forms, and how it is adversely affecting people in society. In particular, shoulder surfing, dumpster-diving, and online methods of acquiring personal identifying information are discussed. Part II discusses the typical scams that are utilized by identity thieves to persuade consumers to divulge their personal data. Part III describes identity theft's impact on the economy in terms of its effects on the daily lives of consumers and various institutions handling personal data of consumers. Part IV discusses current trends of identity theft in the United States, and analyzes the relevant federal and state legislation designed to protect consumers. Part V examines current trends of identity theft in Canada, carefully noting various identity theft statutes and applications in selected jurisdictions. Finally, Part VI reveals common safeguards recommended under various privacy regimes in the U.S. and Canada to help consumers avoid identity theft when divulging personal data on a daily basis. Here, a non-exhaustive list contains helpful strategies to counteract against the theft of one's personal identifying information.

I. IDENTITY THEFT: DEFINITION AND FORMS

Identity theft is a crime committed by those obtaining personal identifying information from another person or group for wrongful purposes such as fraud or deception, which usually results in some personal gain.[1] Personal identifying information generally includes an individual's name, address, phone number, credit card number, checking or savings account, and Social Security or Social Insurance numbers.[2] Group identifying information includes the theft of vital information from financial institutions, government agencies, or businesses.[3] The most notable feature of identity theft is that

[1] U.S. Dept. of Justice, Identity Theft and Fraud, *available at* http://www.usdoj.gov/criminal/fraud/idtheft.html (last visited Mar. 1, 2006) [hereinafter DOJ Theft and Fraud].
[2] *Id.*
[3] *Id.*

vital information is wrongfully used for one's benefit (known as an identity thief) by assuming another person's identity without their knowledge or consent. This produces very disturbing trends for innocent consumers who are dependent upon others to handle their personal information, especially during commercial transactions. Aside from losing personal wealth and confidence in the marketplace, identity theft soils the reputation and livelihood of the consumer. As such, identity theft covers a broad range of commercial activities from online commercial transactions to telephone solicitation of consumers.

Various forms of identity theft exist in society. First, identity theft may involve *skimming*, whereby an identity thief steals personal data from another by capturing the information on a data storage device.[4] Here, the skimming process involves the attachment of a storage device with an ATM machine that consumers normally utilize.[5] By using the device as a fake ATM machine that reads the magnetically-encoded stripe on the back of an ATM card, the identity thief can withdraw funds directly from the consumer's bank account. Second, *shoulder surfing* involves those individuals who carefully watch or hear others providing valuable personal information over the phone, who type in numbers on e-machines, or who disclose vital information to others in person at a financial institution or store.[6]

Third, *dumpster-diving* (or mail theft) involves those individuals who sort through garbage bins to search for documents with valuable financial information such as credit card numbers and bank accounts, or any other record showing one's name, address, and telephone number.[7] In this way, identity thieves steal newly issued cards from the mailbox. This is especially true when pre-approved credit card forms are thrown away, only to be recovered and used by the identity thief. This is why credit card companies often require activation of credit cards from specific phone numbers as a precautionary measure. Fourth, *criminal identity theft* involves the disclosure of another individual's identity by an accused when the accused is questioned during arrest or detention

[4] Public Safety and Emergency Preparedness Canada, How Identity Theft Occurs, *available at* http://www.psepc-sppcc.gc.ca/prg/le/bs/consumers-en.asp (last visited Mar. 7, 2006).
[5] Federal Trade Commission for the Consumer, Facts for Consumers, *available at* http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm (last visited Mar. 5, 2006).
[6] DOJ Theft and Fraud, *supra* note 1.
[7] Public Safety Canada, *supra* note 4.

procedures.[8] Here, an imposter will use another individual's personal data such as their name, driver's license number, or Social Security number, and disclose this information to law enforcement authorities. If there is a requirement to appear in court or fulfill necessary procedures for minor violations or crimes, the identity thief may create and assume a false identity when appearing in court.[9] When the court appearance is due and the accused does not appear, a bench warrant or other court order will call for the victim's name instead of the imposter.

Fifth, identity theft of personal data from *government and places of employment* may occur by online hacking, or theft of hard drives from offices.[10] Here, identity thieves acquire sensitive information from important databases storing relevant data that exposes any employee's background. Sixth, *phishing* is an attempt to induce innocent on-lookers to provide their personal data in response to attractive offers that are fraudulent in nature.[11] Lately, spam e-mail has received considerable attention to the extent that many legislatures have enacted laws designed to curb misuse of consumer's personal data, especially for those consumers who open fraudulent e-mails, and are unaware of the dangers in responding to such spam e-mails. In this case, the danger refers to the disclosure of their personal data to individuals who become unjustly enriched.

Seventh, cleverly disguised schemes through e-mail and websites may entice consumers to disclose sensitive personal data to seemingly legitimate businesses in a process known as *spoofing*.[12] Spoofing makes the consumer believe that a genuine advertisement is offered from financial institutions or online sites.[13] An unsophisticated

---

[8] Privacy Rights Clearinghouse, *Fact Sheet 17(g): Criminal Identity* Theft, *available at* http://www.privacyrights.org/fs/fs17g-CrimIdTheft.htm (last visited Mar. 2, 2006) The Privacy Rights Clearinghouse allows enforcement agencies in using a single national database, whereby the FTC accepts complaints regarding identity theft, both from other state and federal agencies, and through its online complaint form. The FTC publishes annual charts showing the incidence of identity theft by states and cities. See generally http://www.ftc.gov/os/testimony/040615idtheftssntest.pdf (last visited Mar. 9, 2006) [hereinafter Clearinghouse].

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] Identity Theft Resource Center (ITRC), Scams and Consumer Alerts, *available at* http://www.idtheftcenter.org/alerts.shtml (last visited Mar. 4, 2006). The Identity Theft Resource Center is a national non-profit organization that focuses on identity theft. Founded in December 1999 by Linda and Jay Foley, this San Diego-based group provides a web-based forum for consumer to lodge complaints or seek information that prevents others from stealing personal data from ordinary consumers. In 2004, the ITRC received the U.S. Dept. of Justice's National Crime Victims Service Award [hereinafter ITRC].

[13] Public Safety Canada, *supra* note 4.

consumer may be tempted to provide personal data such as their name, address, credit card information, insurance policy numbers, and Social Security numbers in responding to this elaborate scheme created by the identity thieves.

The mere disclosure of only a handful of information may be enough for an identity thief to find more valuable personal information from the consumer, a process that adversely affects the consumer's credit history, while contributing to the free-flow acquisition of goods and services in the marketplace for the benefit of the identity thief. Typical indicators of identity theft affecting a consumer include: (1) verification from creditors or credit card statements that a new account has been approved; (2) approval from creditors for a credit card a consumer never applied for; (3) notice from collection agencies that they are collecting an overdue debt from an account the consumer never used; and (4) no longer receiving financial statements.[14]

II. TYPICAL SCAMS THAT INDUCE CONSUMERS TO DIVULGE PERSONAL DATA

Although many consumers are vigilant in guarding against suspect commercial activities, others fall victim to creative scams that result in the disclosure of sensitive personal data. These scams generally include: (1) telephone solicitation or verification of credit card information; (2) phishing; (3) free gifts and investment deals; (4) e-mail chain letters and pyramid scams; and (5) charity scams. These scams do not necessarily represent an exhaustive list, but they are modern examples of how identity thieves acquire information from unsuspecting consumers. Thus, a brief examination of these scams would be useful in understanding the degree of complexity involved in identity theft.

[14] PhoneBusters, The Canadian Anti-Fraud Call Center, Recognize It, Identity Theft: Could it Happen to You?, *available at* http://www.phonebusters.com/english/recognizeit_identitythe.html (last visited Mar. 4, 2006). PhoneBusters is a Canadian anti-fraud call center located in Ontario. Established in 1993, PhoneBusters is a joint program between the Ontario Provincial Police and the federal Royal Canadian Mounted Police. The company's objective is to educate consumers about fraudulent telemarketing schemes, and help gather evidence for victims by collecting statistics, documentation, tape recordings to be made available to law enforcement agencies. This is an example of how the private industry and government cooperate to inform and protect ordinary consumers from instances of identity theft.

A. Credit Card Companies

Many phone calls that appear to be from reputable credit card companies such as VISA and Mastercard have persons posing as representatives to discuss unusual spending activity with consumers. Usually portraying the call as an anti-marketing device to protect consumers, this seemingly professional representative will ask for the bar code on the back of a consumer's credit card to verify their account.[15] The so-called representative conveys the impression to the consumer that the company is protecting their credit account from suspicious spending activities. However, the only purpose is to extract personal identifying information to be used for wrongful purposes.

B. "Phishing" Scams

Phishing (or brand spoofing) refers to the sending of an e-mail to a user falsely claiming to be a legitimate business with the intent to persuade the consumer into divulging personal data to be used for unlawful purposes.[16] Here, the false business directs a consumer to a seemingly popular and trusted website in order to update or modify their personal data that a legitimate business would already have in their possession. *Phishing* thus allow parties to masquerade as trustworthy businesses, only to steal personal information from unsuspecting consumers.[17] For example, in 2003, correspondence from a website assuming the identity of PayPal targeted consumers by claiming to suspend their account unless they clicked on various website links to update sensitive information such as credit card numbers and bank account numbers.[18] Governments, financial institutions, and online auction sites are frequent targets of *phishing*.[19]

Typically, the copycat or spoofed website involves some form of a fraud alert that requires consumers to modify their personal data, especially when online purchases are made from specific websites. For instance, on July 9, 2003, the Massachusetts State

---

[15] ITRC, *supra* note 12.
[16] Webopedia, *available at* http://www.webopedia.com/TERM/p/phishing.html (last visited Mar. 4, 2006).
[17] Public Safety and Emergency Preparedness Canada, Archive, Background, *available at* http://ww3.psepc-sppcc.gc.ca/opsprods/info_notes/IN04-002_e.asp (last visited Mar. 7, 2006) [hereinafter Public Safety].
[18] *Id.*
[19] Royal Canadian Mounted Police, Phishing or Brand Spoofing, *available at* http://www.rcmp-grc.gc.ca/scams/phishing_e.htm (last visited Mar. 7, 2006).

Lottery Commission's website was spoofed by informing visitors to provide their credit card and Social Security numbers, and to pay a processing fee of $100 U.S.[20] In response to these types of phishing, in early 2005 Attorney General of Massachusetts, Tom Reilly, issued a warning to consumers within the state to be wary of phone solicitors posing as U.S. government representatives.[21] The scheme involved a promise to provide generous government grants in exchange for a processing fee requiring an automated debit or withdrawal from the consumer's checking account.[22] The processing fee was estimated to be in the hundreds of dollars range. The result was no actual government grant being received by consumers paying this processing fee. Instead, only pamphlets and booklets listing various government agencies and programs were received by the consumers.

C. Free Gifts and Investment Deals

Many companies offer free gifts or bogus investment deals to attract consumers to disclose sensitive information. Often times, a consumer will receive a phone call or e-mail about the free offer where the consumer would be required to give personal data to conduct the promised commercial service. The famous *Nigerian/West African* business letter scam involved members posing as government or business officials offering to transfer millions of dollars to potential investors.[23] This scheme had unsolicited letters in the form of "urgent" business proposals from supposedly legitimate Nigerian civil servants. The consumer recipient was directed to open a bank account at a Suffolk England bank, and was given a link to their website.

Unfortunately, it was a replica website of the bank, and within hours a balance of a few million dollars in the newly-created online bank account appeared to be deposited. After the consumer recipient attempted to withdraw this money, a notice was received by

---

[20] Public Safety, *supra* note 17.

[21] The Office of Massachusetts Attorney General Tom Reilly, Media Center, *AG Reilly Warns Consumers to Beware of Bogus Government Grant Scams, available at* http://www.ago.state.ma.us/sp.cfm?pageid=986&id=1360 (last visited Mar. 7, 2006). According to the AG of Massachusetts, the U.S. government does not solicit government grants or loans over the telephone. Rather, there is an official application process when consumers apply for loans or grants from the federal government.

[22] *Id.*

[23] RECOL.ca, *available at* https://www.recol.ca/scams/advance_fee.aspx (last visited Mar. 11, 2006). See also Internet Crime Complaint Center, Alert (Mar. 7, 2006), Nigerian 419 Scam, *available at* http://www.ic3.gov/media/2006/060307.htm (last visited Mar. 12, 2006).

the consumer to pay various "fees" to Africa prior to completing the transaction. The sender of this letter claimed to obtain consumers' names and background from the Chamber of Commerce or International Trade Commission.[24] From here, lucrative contracts related to oil and gas products (and other commodities) were offered to consumers, persuading them to deposit money into their personal accounts. After a period of time, the promised money that was in the Central Bank of Nigeria would be transferred to the consumer's personal account, but only after they provide personal data such as their bank name, address, telephone and fax numbers, and bank account numbers.[25]

D. E-mail Chain Letter/Pyramid Scams

Several websites offer financial incentives in the form of money or gifts to consumers by helping track people's e-mails. These pyramid scams replace the traditional postal chain letters, and promises that once the consumer's e-mail will be successfully forwarded to their friends or relatives, those consumers will be compensated for their efforts. Some websites even go as far as claiming that the Federal Trade Commission approves of this practice.[26] Like other scams, this activity normally involves an advance fee to be paid by the consumer, particularly with advertisements that offer loan guarantees when consumers have a poor credit history or no credit-rating at all.[27] Such advance fees involve several hundreds of dollars, only to result in distributing no service to the hopeful consumer. Often, consumers with poor credit ratings are usually targets.

E. Disaster Relief/Charity Scams

Natural disasters are usually followed by a mass appeal for donations either through websites or telephone representatives.[28] In the context of identity theft, many artificial websites have direct links for consumers to click on to make out donations. But, to process these online donations, credit card numbers are often required to be entered

[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] RECOL.ca, Advance Fee, *available at* https://www.recol.ca/scams/advance_fee.aspx (last visited Mar. 11, 2006).
[28] *Id.*

onto the website. These situations have prompted consumer advocates to recommend consumers to survey legitimate websites such as the Federal Trade Commission or the Red Cross prior to sending donations.[29] These websites list secure and official websites to donate funds through proper channels. The recent Hurricane Katrina disaster in the southern U.S. has seen many new websites posing as charities to acquire personal data from persons intending to donate in good faith.[30] More specifically, these charitable websites would take on the identity of reputable organizations like the Red Cross or Salvation Army, and request personal e-mails from unsuspecting visitors. Thus, in order to donate online it is recommended to visit the organization's official website that refers to specific individuals and procedures when making donations for various causes.

What is a Consumer Report?

A consumer report is defined as a collection of sensitive personal information relating to credit history, general reputation, character, and lifestyle.[31] For identity theft, a consumer report allows a consumer to monitor any changes or suspicious activity related to their personal information. As such, the consumer report may reveal changes to the personal account activity of a consumer, when and where the account was used, and whether any new form of credit is being pursued. By reviewing a consumer report, a consumer is permitted to correct any information, and to confirm their present status with the financial institution. This report is usually prepared by a consumer reporting agency for distribution to either consumers or other businesses seeking information for verification purposes. The standard practice is to offer a free initial credit report for the benefit of consumers.

A consumer report is often requested by employers for the purpose of screening potential employees (this may involve investigative consumer reports, which include interview accounts from the employee's family, friends, and associates).[32] Jurisdictions

---

[29] *Id.*
[30] The Office of Massachusetts Attorney General Tom Reilly, Media Center, *Hurricane Katrina Spawns Phishing Scams – Don't Take the Bait*, *available at* http://www.ago.state.ma.us/sp.cfm?pageid=2185 (last visited Mar. 7, 2006).
[31] Federal Trade Commission, Facts for Businesses, *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/credempl.htm (last visited Mar. 26, 2006).
[32] *Id.*

with identity theft legislation have clearly enunciated the use of consumer reports for conducting credit checks of individuals acting as consumers or potential employees. In many instances, relevant provisions in privacy statutes define the scope of content permitted in consumer reports in order to provide valuable information, verify the accuracy of a consumer's identity, or help employers hire employees with responsible financial backgrounds.

III. THE IMPACT OF IDENTITY THEFT ON THE ECONOMY AND THE CONSUMER

Commercial activity between buyers and sellers in the marketplace normally requires some exchange of information that completes a transaction or series of transactions. As such, a number of problems arise from anyone interested in taking advantage of another's personal data. First, the assumption of one's identity for another person takes away the credibility and confidence of that consumer. An innocent consumer may lose their reputation because of an identity thief's misuse of financial assets. Second, the theft and misuse of personal data such as banking information can cause severe economic hardship for consumers who accumulate debts as a result of the identity thief's unjust enrichment. In 2004, the Federal Trade Commission estimated that identity theft produced losses of over $48 billion for businesses, over $5 billion for individual consumers, and over 300 million hours spent by victims of identity theft attempting to restore their identity.[33]

Accumulation of debts in the form of bills, credit cards, bad checks, and negative tax implications may result after the identity thief's misuse of personal data.[34] Here, aside from the out-of-pocket expenses associated with the unlawful use of banking information, there are additional expenses for restoring one's reputation by pursuing legal remedies through court orders, or confirming that one's identity is not related to crimes with law

[33] Prepared Statement of The Federal Trade Commission on Identity Theft and Social Security Numbers, Before the Subcommittee on Social Security of the House Committee on Ways and Means (June 15, 2004), *available at* http://www.ftc.gov/os/testimony/040615idtheftssntest.pdf (last visited Mar. 9, 2006) at 2.
[34] Office of the Privacy Commissioner of Canada, *Identity Theft: What it is and what you can do about it*, *available at* http://www.privcom.gc.ca/fs-fi/02_05_d_10_e.asp (last visited Mar. 3, 2006). Like the U.S. Department of Justice, this Canadian federal agency offers consumers valuable tips to avoid the common problems of identity theft. Here, key privacy issues such as online data brokers, video surveillance, and mail issues.

enforcement agencies from active databases. Third, unauthorized use of another individual's personal data may result in the refusal of credit or loan applications from legitimate consumers and businesses, along with creating bad credit ratings for consumers and businesses.[35] In the context of general business applications, usual forms of identity theft include: (1) false applications of credit cards and loans; (2) fraudulent withdrawals from bank accounts; and (3) fraudulent use of telephone credit cards.[36]

Fourth, consumers and businesses may incur extra expenses for building and maintaining adequate security measures designed to filter incoming information.[37] Personal data that is lost to identity thieves may affect the client's confidence in the business' ability to manage their personal information. Moreover, consumers may have to purchase identity theft insurance from various companies offering policies to cover clients' costs for long-distance phone calls, receiving documentation, postage, lost wages, and hiring a lawyer.[38] For instance, some identity theft insurance polices in the U.S. cover up to and between $10,000 and $15,000.[39] However, according to the National Association of Insurance Commissioners, most identity theft insurance policies do not cover direct monetary losses.[40] Therefore, inadequate security in any given business may result in huge economic losses due to liability issues, fines, and loss of clientele.

Fifth, as mentioned supra criminal identity theft involves the improper use of someone else's personal identity in order to exonerate oneself during criminal investigations. Thereafter, the victim's name drawn from this crime is entered into a county or state identity theft database. This creates two major problems for the consumer: (1) the expense incurred in clearing one's name from the county or state identity theft database, and (2) the victim's potential for seeking future employment.[41] For the latter, a victim of criminal identity theft may not be offered employment or may be terminated from their job because the employer conducts a criminal background check only to find

---

[35] Federal Trade Commission for the Consumer, Facts for Consumer, *available at* http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm (last visited Mar. 5, 2006) [hereinafter FTC Consumer].
[36] *Id.*
[37] Identity Theft Resource Center, In the Workplace, *available at* http://www.idtheftcenter.org/workplace.shtml (last visited Mar 4, 2006).
[38] Gail Liberman and Alan Lavine, BostonHerald.com. Insurers Cover Identity Theft, *available at* http://business.bostonherald.com/businessNews/view.bg?articleid=129049 (last visited Mar.5, 2006).
[39] *Id.*
[40] *Id.*
[41] Clearinghouse, *supra* note 8.

the victim's name on criminal databases.[42] Thus, there is an impact upon the consumer in both an economic and reputation sense. Unless the consumer clears their own name by making court appearances and filing relevant documentation that proves their innocence, the prospects for future employment may be dismal.

The most common response from consumers who discover their personal data is being misused is to contact consumer reporting agencies. Consumer reporting agencies include credit bureaus (such as *Equifax*, *Experian*, and *TransUnion*) and other specialized agencies that sell personal data such as medical records, mortgage, and loan information. Consumer reporting agencies normally collect information about a consumer's credit-worthiness from financial institutions, public records, and other sources.[43] Such personal information is significant when a consumer applies for any form of credit, such as a loan, mortgage, or credit card. Those creditors that issue credit to a consumer often rely upon the accuracy and depth of credit information supplied by consumer reporting agencies.[44]

[42] *Id.* The Fair Credit Reporting Act (FCRA) is a federal statute that requires employers to conduct an accurate background check of potential employees. This accuracy depends upon information supplied by consumer reporting companies. Since the 1997 amendments, Congress has ensured increasing legal obligations on employers such that the FCRA prevent innocent victims of identity theft from being denied reasonable opportunity for seeking employment or being promoted because of their name being improperly disclosed by criminal suspects. These amendments include: (1) that persons are aware that consumer reports are used for employment purposes and agree to this use, and (2) that persons are notified immediately when consumer reports reveal information resulting in negative employment decisions.
[43] National Association of Federal Credit Unions (NAFCU), Fair Credit Reporting Act, *available at* http://www.nafcu.org/Content/NavigationMenu/Legislation_Regulation/Legislation/Fair_Credit_Reporting_Act1/Fair_Credit_Reporting_Act.htm (last visited Mar. 11, 2006). Founded in 1967 and headquartered in Arlington, Virginia, NAFCU is a trade association that represents the interests of federal credit unions before the federal government and public. It provides representation, information, and education to meet the challenges faced by cooperative financial institutions in the marketplace. See generally About NAFCU, *available at* http://www.nafcu.org/Template.cfm?section=About_NAFCU (last visited Mar. 11, 2006).
[44] *Id.* Approximately 180 million credit files are maintained by consumer reporting agencies across the U.S., and track more than 2 billion transactions per month.

IV. CURRENT TRENDS TO REGULATE IDENTITY THEFT IN THE UNITED STATES

United States

The Role of the Federal Trade Commission

Identity theft is one of the fastest growing crimes in the United States. In 2002, approximately 43 percent of all complaints received by the Federal Trade Commission (FTC) related to identity theft.[45] In 2004, the FTC reported that over 10 million consumers were victims of some form of identity theft crime in the U.S.[46] In response, at the federal level, the U.S. Department of Justice (DOJ) works closely with other federal agencies such as the Federal Bureau of Investigations (FBI), the U.S. Secret Service, the Social Security Administration's office of the Inspector General, and the U.S. Postal Inspection Service to investigate and prosecute crimes related to identity theft.[47] At the state level, several states have introduced legislation to prompt local authorities, including the police, financial institutions, and credit reporting companies to carefully monitor suspicious activities when dealing with consumers' personal information. These federal and state agencies actively coordinate with one another by exchanging relevant information in order to adduce evidence of potential wrongdoing against a victim of identity theft.

The DOJ offers valuable tips to consumers to avoid problems related to identity theft. These tips include requesting a written application from someone who offers credit cards over the phone (instead of disclosing personal data over the phone), asking the post office to hold mail when traveling, and careful inspecting financial statements from banks, insurance companies, or other financial bodies.[48] Likewise, the FTC provides a web-based national resource on identity theft for consumers, which offers a portal for consumers to take corrective action when they believe their personal data has been stolen

[45] California Dept. of Consumer Affairs, Office of Privacy Protection, *available at* http://www.privacy.ca.gov/cover/identitytheft.htm (last visited Mar. 8, 2006).
[46] Prepared Statement of The Federal Trade Commission on Identity Theft and Social Security Numbers, Before the Subcommittee on Social Security of the House Committee on Ways and Means (June 15, 2004), *available at* http://www.ftc.gov/os/testimony/040615idtheftssntest.pdf (last visited Mar. 9, 2006) at 2.
[47] *Id.*
[48] *Id.*

or misused.[49] In particular, the FTC offers consumers the option of filing an online formal complaint, which is conveniently stored on a database that law enforcement agencies use for investigative purposes.[50] In this way, federal and state authorities integrate knowledge services to track specific wrongdoings by identity thieves, while ensuring a set of measures designed to safeguard the personal data of innocent consumers.

The FTC also provides a consumer kit called the *Information Compromise and the Risk of Identity Theft: Guidance for your Business*.[51] This kit provides guidance on contacting consumers, law enforcement agencies, and the three major credit reporting agencies of *Equifax*, *Experian*, and *TransUnion*. The FTC, in conjunction with consumer advocates and creditors, also created the *ID Theft Affidavit* as a means of allowing consumers to report potential abuse of their personal information to financial institutions where their account is located.[52] Prior to initiating a formal investigation, there are two parts of the affidavit that need to be completed: (1) *ID Theft Affidavit*: where you report

[49] Federal Trade Commission (FTC), Your National Resource on Identity Theft, *available at* http://www.consumer.gov/idtheft/ (last visited Mar. 1, 2006). The website provides useful information about identity theft, and the measures that should be taken by victims of identity theft. Such measures include contacting three consumer reporting bureaus (Equifax, Experian, and TransUnion) in order to place a fraud alert on your credit report. The credit report tells you what information the bureau has about your credit history, judgments, and collection activity. The fraud alert requires creditors to contact the victim of identity theft when they open a new account or change an existing account. Once a fraud alert is placed, the consumer is entitled to free copies of the credit report. The consumer may even request that only the last four digits of their Social Security number appear on credit reports. It suffices if the victim of identity theft contacts only one of these consumer reporting companies. Thereafter, one of these companies is required to report the fraud alert to the other two companies. Typically, these consumer reports prepared by consumer reporting agencies must satisfy provisions under the Fair Credit Reporting Act (FCRA). A consumer report contains information about one's personal and credit background, character, general reputation, and lifestyle. See generally http://www.ftc.gov/bcp/conline/pubs/buspubs/credempl.htm (last visited Mar. 2, 2006).

[50] The FTC allows victims of identity theft to file a complaint on their Complaint Input Form, *available at* https://rn.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03 (last visited Mar. 1, 2006). More specifically, the form indicates various forms of identity theft, including: (1) credit cards; (2) checking or savings accounts; (3) loans; (4) phone or utilities; (5) securities; (6) internet or E-mail; and (7) government documents or benefits.

[51] Prepared Statement of The Federal Trade Commission on Identity Theft and Social Security Numbers, Before the Subcommittee on Social Security of the House Committee on Ways and Means (June 15, 2004), *available at* http://www.ftc.gov/os/testimony/040615idtheftssntest.pdf (last visited Mar. 9, 2006) at 17. The FTC is particular about how states apply identity theft measures. For instance, on January 17, 2006, the FTC fined consumer reporting agency Far West Credit, Inc. $120,000 in Utah. The FTC claimed that this agency failed to follow reasonable procedures when it sold inaccurate information of consumer reports to mortgage companies. See generally Federal Trade Commission, For the Consumer, Credit Reporting Agency Settles FTC Charges, *available at* http://www.ftc.gov/opa/2006/01/farwestcredit.htm (last visited Mar. 9, 2006).

[52] Instructions for Completing the ID Theft Affidavit, *available at* http://www.ag.state.mn.us/consumer/privacy/ID%20Theft%20Affidavit.pdf (last visited Apr. 2, 2006).

the actual theft and general information about yourself, and (2) *Fraudulent Account Statement*: where you describe the account opened in your name with each company.[53] The use of this affidavit is optional, but it helps financial institutions verify that a consumer did not create the debt on their account in the first instance. These types of applications enable consumers to file complaints easily with the FTC directly, or with an organization that is affiliated with the FTC.

Common Methods Used To Protect U.S. Consumers From Identity Theft

There are several ways in dealing with identity theft in the United States. First, online consumer complaint systems are offered by many federal and state governments (usually through the Attorney General's office), including private industry websites that are partnered with government. For instance, the Internet Crime Complaint Center (IC3) receives consumer complaints regarding cyber crime, and serves as a reporting mechanism that forwards these complaints to relevant authorities for investigation.[54] The IC3 is a partnership between the FBI and the National White Collar Crime Center (NW3C).[55] Using an encrypted secure socket layer (SSL), complaints submitted to this website are referred to federal, state, or international enforcement and regulatory agencies to conduct thorough investigations as to the source of fraud or other forms of white collar crime.[56]

---

[53] *Id.*

[54] Internet Crime Complaint Center, Welcome to IC3, *available at* http://www.ic3.gov/ (last visited Mar. 12, 2006). The IC3 initiative is meant to receive Internet-related criminal complaints, and to integrate federal, state, local, and international efforts in responding to such complaints. The bulk of complaints comprise intellectual property rights, hacking, economic espionage, online extortion, international money laundering, and identity theft.

[55] *Id.*

[56] *Id.* When fraud is suspected by a consumer, filing a complaint with the IC3 website does not serve as notice to creditors. Rather, the consumer must contact the creditor individually to inform them of potential misuse of their credit information, or to request a credit report. The encrypted secure socket layer (SSL) is a protocol developed by Netscape for transmitting information via the Internet. This system uses two keys to encrypt data – a public key known to everyone and a private key known only to the recipient of the message. Both Netscape Navigator and Internet Explorer have SSL encryption. See generally Webopedia, *available at* http://www.webopedia.com/TERM/S/SSL.html (last visited Mar. 12, 2006).

For example, the IC3 initiative recently exposed a scam for Super Bowl XL football tickets.[57] The scam involved various online auctions and classified advertisement websites, whereby potential customers were directed to a wire-transfer payment service to quickly send money to secure tickets. In some instances, the buyers were instructed to send money overseas under the impression that the seller was located outside the United States on work or vacation. However, when buyers transferred money to the seller, they never received the Super Bowl tickets.

Key Federal Privacy Statutes in the U.S.

Recognizing the growing number of economic crimes (including identity theft) throughout the U.S., Congress enacted the Gramm-Leach-Bliley Act (GLBA) in 1999 to lay the responsibilities upon financial institutions that utilize consumer personal information to provide a minimum set of commercial content safety measures.[58] Highlighting the importance of protecting consumers' personal data, section 6801 of the Act provides:

> **(a) Privacy obligation policy**
> It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.
> **(b) Financial institutions safeguards**
> In furtherance of the policy in subsection (a) of this section, each agency or authority described in section 6805 (a) of this title *shall* establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—
> **(1)** to insure the security and confidentiality of customer records and information;
> **(2)** to protect against any anticipated threats or hazards to the security or integrity of such records; and
> **(3)** to protect against *unauthorized access* to or use of such records or information which could result in substantial harm or inconvenience to any customer.[59]

---

[57] Internet Crime Complaint Center, Alert (Jan. 27, 2006), Super Bowl XL Ticket Scams, *available at* http://www.ic3.gov/media/2006/060127.htm (last visited Mar. 12, 2006). Super Bowl XL was held on Feb. 5, 2006 in Detroit, Michigan.

[58] 15 U.S.C. § 6801-6809. Privacy Rights Clearinghouse, References, *available at* http://www.privacyrights.org/fs/fs6a-facta.htm#12 (last visited Mar. 9, 2006). The Gramm-Leach-Blilely Act is also known as the Financial Services Modernization Act. More specifically, Title 5 of the Act contains provisions relating to Privacy. See generally Electronic Privacy Information Center, *available at* http://www.epic.org/privacy/glba/ (last visited Mar. 9, 2006).

[59] 15 U.S.C. § 6801(a)-(b), Cornell Law School, Legal Information Institute, Protection of Non-Public Personal Information, *available at*

As a rule, the GLBA only regulates financial institutions such as banks, insurance companies, brokerage firms, and investment firms.[60] Regardless, financial institutions are obligated to provide adequate security measures to protect consumers' personal records from "substantial harm or inconvenience to any customer".[61] Financial institutions must also provide a first-time consumer with information sharing policies, including how non-public personal information (NPI) is handled or passed on to third parties, and how personal data will be handled if the account is terminated.[62] Non-public personal information refers to applications for financial services (credit or loans) and account histories (bank or credit cards).

A consumer has the right to opt-out of procedures that would ordinarily allow the financial institution to divulge personal data of the consumer to unaffiliated companies.[63] Moreover, the GLBA prohibits financial institutions from transferring personal access codes or account numbers to unaffiliated third parties for telemarketing, direct mail marketing, or e-mail marketing.[64] Thus, the GLBA applies data-sharing restrictions to personal data such as names, addresses, telephone numbers, and Social Security numbers.[65] Apart from the GLBA, other federal privacy statutes warrant some discussion in recognizing how Congress is responding to identity theft on American consumers. Below, Table 1 shows three key pieces of federal legislation that offer protection to consumers who divulge their personal data to others in the marketplace.

---

http://www4.law.cornell.edu/uscode/html/uscode15/usc_sec_15_00006801----000-.html (last visited Mar. 9, 2006).

[60] Electronic Privacy Information Center, Privacy Protections under the GLBA, *available at* http://www.epic.org/privacy/glba/ (last visited Mar. 9, 2006).

[61] 15 U.S.C. § 6801(b)(3).

[62] *Id.*

[63] *Id.* Despite the emphasis on protecting consumer's personal data, various exemptions in the GLBA do allow financial institutions the flexibility to permit information sharing with separate companies. Here, the financial institution must show that that personal data sharing with the separate company is a necessary part of conducting financial transactions for the best interests of the customer. Additionally, financial institutions can transfer a consumer's personal record to credit reporting companies.

[64] *Id.*

[65] *Id.*

Table 1: Selected Federal Privacy Statutes in the U.S.

Federal Statute	Year Enacted	Key Provision(s)
Fair Credit Reporting Act	**1970**	**§ 602**: Congressional findings and statement of purpose (a) Accuracy and fairness of credit reporting. The Congress makes the following findings: (1) The banking system is dependent upon fair and accurate credit reporting. Inaccurate credit reports directly impair the efficiency of the banking system, and unfair credit reporting methods undermine the public confidence which is essential to the continued functioning of the banking system. (2) An elaborate mechanism has been developed for investigating and evaluating the credit worthiness, credit standing, credit capacity, character, and general reputation of consumers. (3) Consumer reporting agencies have assumed a vital role in assembling and evaluating consumer credit and other information on consumers. (4) There is a need to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy.[66]
Identity Theft and Assumption Deterrence Act	**1998**	**Title 18, U.S.C. § 003**: Identity Theft – "knowingly transfers or uses, without lawful authority, a *means of identification* of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that

[66] H.R. 2622, 108th Congress, 1st Session, *available at* http://financialservices.house.gov/media/pdf/108hr2622ai.pdf (last visited Apr. 2, 2006).

		constitutes a felony under any applicable State or local law,"[67]
Fair and Accurate Credit Transactions Act **(amends the Fair Credit Reporting Act)**	**2003**	**§ 202**: Fraud Alerts – Upon the request of a consumer who asserts in good faith a suspicion that the consumer has been or is about to become a victim of fraud or related crime, and upon receiving proper identification, a consumer reporting agency shall include a *fraud alert* in the file of that consumer. **§ 205**: Blocking of Information Resulting from Identity Theft – ". . . not later than 30 days after the date of receipt of proof of the identity of a consumer and an official copy of a police report evidencing the claim of the consumer of identity theft, a consumer reporting agency shall *block* the reporting of any information identified by the consumer in the file of the consumer resulting from the alleged identity theft, so that the information cannot be reported

As seen from Table 1, over time the three federal privacy statutes gradually incorporate newer forms of personal data protection for the benefit of consumers. The Fair Credit Reporting Act (1970) covers a broad area of personal data, focusing on credit background checks to verify personal data accuracy, and requiring that a consumer's data be provided only for legitimate business purposes. However, with the Identity Theft and Assumption Deterrence Act (1998), there is a shift in emphasis from general protection of personal data to preventing the impersonation of a consumer's identity. Finally, the Fair and Accurate Credit Transactions Act (2003) substantially amends the Fair Credit Reporting Act by including modern applications of consumer credit information through fraud alerts and blocking of personal data. Today, these three federal statutes serve as the main foundation of consumer protection in the U.S. marketplace by protecting the substantive content of personal data, while streamlining commercial activity.

[67] National Check Fraud Center, Identity Theft and Assumption Deterrence Act of 1998, *available at* http://www.ckfraud.org/title_18.html (last visited Apr. 1, 2006). The Identity Theft and Assumption Deterrence Act became effective on October 30, 1998.

Fair Credit Reporting Act (1970)

In responding to the growing number of consumer complaints relating to misuse and theft of personal data, Congress enacted the Fair Credit Reporting Act (FCRA) in 1970. Generally, the FCRA establishes the basis for financial institutions (such as consumer reporting agencies) to enforce privacy protections on behalf of consumers. In the context of identity theft, the Act protects and modifies the accuracy of consumer credit information. This statute also creates a mandatory disclosure requirement for consumer reporting agencies when a consumer requests a credit report or a review of their credit report.[68] However, the consumer reporting agency must disclose personal information of a consumer only under limited circumstances, using reasonable procedures to ensure a high degree of accuracy in reporting credit information.[69]

Under the FCRA, a consumer may place a *fraud alert* in the event they discover that their personal data is being misused by a stranger. There are two types of fraud alerts: (1) initial alert; and (2) extended alert.[70] The initial fraud alert remains on your credit report for 90 days, and is normally launched when a consumer's sensitive information is stolen within a short period of time. Here, the FCRA permits a consumer to receive a free credit report from any of the three major consumer reporting companies, such as *Equifax, Experian*, and *TransUnion.*[71] The extended fraud alert lasts for seven years after a consumer files an identity theft report with a consumer reporting agency.[72]

---

[68] The Fair Credit Reporting Act, *available at* http://www.ftc.gov/os/statutes/fcra.htm#609 (last visited Mar. 11, 2006) at § 609 (Disclosures to Consumers).
[69] *Id.*
[70] FTC Consumer, *supra* note 35.
[71] *Id.* There are many types of consumer reporting agencies, including credit bureaus and specialty agencies that sell information about financial record histories and medical records. See generally TransUnion, *available at* http://www.transunion.com/content/page.jsp?id=/personalsolutions/general/data/FCRA.xml#4 (last visited Mar. 11, 2006).
[72] *Id.* The Identity Theft Report has two parts: Part One is a copy of a report filed with local law enforcement agencies such as police, or with State Attorney General, the F.B.I., the U.S. Secret Service, the FTC, or the U.S. Postal Inspection Service. Part Two is a verification process that has any of the three major consumer reporting agencies (Equifax., Experian, and TransUnion) requiring further documentation or evidence from the victim of identity theft. A request from the consumer reporting agency for Part Two is normally required after 15 days of submitting Part One's aspect of the report. Another fifteen day period is permitted for the consumer reporting agency to work with the affected consumer in verifying their complaint by adducing more evidence. Submitting false information during this identity theft report process will subject one to criminal prosecution. The toll-free number for Equifax is 1-800-437-5120, for Experian is 1-888-397-3742, and for TransUnion is 1-800-680-7289.

The extended fraud alert allows a consumer to receive two free credit reports within a twelve-month period.[73]

Moreover, the extended fraud alert will have the consumer reporting agencies remove your name from marketing lists for pre-screened credit offers for five years.[74] The advantage of initiating these two forms of consumer alert is that when a consumer applies for credit of any kind, a business that views your name with an alert designation will be required to verify your identity prior to issuing credit. Thus, there is a protective mechanism in place to verify the identity of a consumer before any stranger can use this information for personal gain. How quickly this defense mechanism is triggered depends largely upon the consumer's vigilance. The FCRA also allows a consumer to ask for a *credit score*, which is a numerical summary of one's credit worthiness based on credit reports collected by credit bureaus.[75] This credit score will allow creditors to determine whether or not a consumer may qualify for ordinary transactions such as an application for a mortgage, credit card, or loan.

The FCRA also permits a consumer to dispute incomplete or inaccurate information by reporting these inconsistencies to a consumer reporting agency. The consumer reporting agency must investigate this consumer file, unless the dispute is frivolous.[76] As such, the consumer reporting agency must correct or delete this file, normally within 30 days.[77] This procedure is particularly relevant when a consumer seeks some form of credit. In the context of employment, the FCRA ensures that a consumer's credit report is not disclosed to their employers, unless written consent of the consumer is provided.[78] In 2003, Congress amended the FCRA into the Fair and Accurate Credit Transactions Act, which generally provides for accuracy, fairness, and

---

[73] *Id.*
[74] *Id.*
[75] TransUnion, A Summary of Your Rights Under the Fair Credit Reporting Act, *available at* http://www.transunion.com/content/page.jsp?id=/personalsolutions/general/data/FCRA.xml#4 (last visited Mar. 10, 2006).
[76] *Id.*
[77] *Id.*
[78] *Id.* If a consumer reporting agency or a user of consumer reports fails to follow these disclosure procedures, a consumer may seek damages by suing these bodies in state or federal court.

privacy of consumer credit information within the possession and control of consumer reporting agencies. [79]

Identity Theft and Assumption Deterrence Act (1998)

In 1998, Congress enacted the Identity Theft and Assumption Deterrence Act (Identity Theft Act), which clearly recognizes identity theft as a federal crime.[80] From the consumer's perspective this is significant in that traditional privacy legislation recognized only creditors as being capable of monetary loss from the misuse of information. Now, the Identity Theft Act includes consumers' right to financial compensation when their identity is stolen. Under this Act, the definition of identity theft is couched in both federal and state laws:

> knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law. [81]

The Identity Theft Act strengthens criminal laws related to identity theft, and places an emphasis squarely on consumer protection.[82] The "means of identification" refer to "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual", [83] including, names, addresses, social security numbers, driver's license numbers, biometric data, access devices (eg. credit

---

[79] TransUnion, A Summary of Your Rights Under the Fair Credit Reporting Act, *available at* http://www.transunion.com/content/page.jsp?id=/personalsolutions/general/data/FCRA.xml#4 (last visited Mar. 11, 2006). The Fair Credit Reporting Act (FCRA) was enacted by Congress in 1970, but written into law on Dec. 4, 2003. The FCRA represents the foundation of United States' national consumer credit system. It generally provides consumers with streamlining of credit reporting, and protection from inappropriate disclosure of consumer's personal credit information by consumer reporting agencies. This ensures that consumer personal data is not disseminated to third parties, who may impersonate the same consumer by unlawfully using this information for personal gain. For more discussion on the FCRA, see National Association of Federal Credit Unions (NAFCU), Fair Credit Reporting Act, *available at* http://www.nafcu.org/Content/NavigationMenu/Legislation_Regulation/Legislation/Fair_Credit_Reporting_Act1/Fair_Credit_Reporting_Act.htm (last visited Mar. 11, 2006).

[80] 18 U.S.C. §1028.

[81] *Identity Theft and Assumption Deterrence Act*, § 003 (a)(7), as Amended by Public Law 105-318, 112 Stat. (Oct. 30, 1998).

[82] Prepared Statement of The Federal Trade Commission on Identity Theft and Social Security Numbers, Before the Subcommittee on Social Security of the House Committee on Ways and Means (June 15, 2004), *available at* http://www.ftc.gov/os/testimony/040615idtheftssntest.pdf (last visited Mar. 9, 2006) at 10.

[83] 18 U.S.C. § 1028(a)(7).

cards), electronic identifying numbers, and telecommunication identifying information. The Identity Theft Act also requires the FTC to create a system for receiving consumer complaints, communicate such complaints to law enforcement agencies, and to offer consumer education and assistance.[84] Thus, the Identity Theft Act goes much further than past legislation by including the protection of consumer personal data and a remedial mechanism to report any abuse of this information to relevant authorities for appropriate investigation and action.

Fair and Accurate Credit Transactions Act (2003)

Other forms of identity theft legislation allow consumers to identify and correct errors on their credit reports. The Fair and Accurate Credit Transactions Act (FACTA) revises the Fair Credit Reporting Act in certain ways, but goes further to provide more convenient options and newer security measures to the consumer.[85] Under FACTA, consumers are entitled to annual free copies of their credit reports from *Equifax*, *Experian*, and *TransUnion* as a means to monitor the accuracy of their transactional record.[86] This is in contrast from earlier years when consumers had to pay a fee of $9.50 U.S. to receive a copy of their credit report.[87] Moreover, FACTA creates a national *fraud alert* system, and allows consumers to place fraud alerts on their credit reports if they determine that their personal identifying information is stolen.[88]

This system imposes a duty on financial institutions to add more unique and personal identifying information on behalf of a consumer in order to conduct more accurate investigations into their credit reports. It also ensures that creditors issue credit

---

[84] Prepared Statement of The Federal Trade Commission on Identity Theft and Social Security Numbers, Before the Subcommittee on Social Security of the House Committee on Ways and Means (June 15, 2004), *available at* http://www.ftc.gov/os/testimony/040615idtheftssntest.pdf (last visited Mar. 9, 2006) at 10.
[85] Prepared Statement of The Federal Trade Commission on Identity Theft and Social Security Numbers, Before the Subcommittee on Social Security of the House Committee on Ways and Means (June 15, 2004), *available at* http://www.ftc.gov/os/testimony/040615idtheftssntest.pdf (last visited Mar. 9, 2006) at 5.
[86] Eileen Alt Powell, CourierPost Online, States allow Freeze on Credit Report Data, *available at* http://www.courierpostonline.com/apps/pbcs.dll/article?AID=/20060306/BUSINESS/603050390/1003/BUSINESS (last visited Mar. 9, 2006).
[87] Privacy Rights Clearinghouse, FACTA, The Fair and Accurate Credit Transactions Act: Consumers Win Some, Lose Some, *available at* http://www.privacyrights.org/fs/fs6a-facta.htm (last visited Mar. 9, 2006).
[88] *Id.* Under Title 5, FACTA established the Financial Literacy and Education Commission, a body devoted to improving the financial literacy and education of persons within the United States. This Commission has a website available at www.mymoney.gov and a toll-free telephone number at 1-888-696-6639. See generally Federal Deposit Insurance Corporation, Consumer Alerts – Fair and Accurate Credit Transactions Act, *available at* http://www.fdic.gov/consumers/consumer/alerts/facta.html (last visited Mar. 9, 2006).

to the proper consumer, rather than granting credit arbitrarily (a common problem with identity theft crimes). As part of this fraud alert system, the FTC works in collaboration with banking regulators to institute "red flag" indicators to assist financial institutions and creditors in ascertaining identity theft patterns.[89] This form of protection serves two purposes: (1) allow consumers to detect identity theft early and correct errors on their credit reports, and (2) to prevent identity thieves to profit when they use a consumer's name to apply for credit or loans.[90]

FACTA also links the three credit reporting agencies of *Equifax, Experian*, and *TransUnion* together in the investigative phase of identity theft. Here, if one credit reporting agency receives a request from a consumer concerned with their personal data, it must share this request with the other two credit reporting agencies. In these ways, consumers avoid the cumbersome process of reporting potential misuse of their personal data to all three credit reporting agencies.

Key State Privacy Statutes

Several states have introduced privacy statutes in relation to identity theft matters. Although most states have some form of legislation covering identity theft crimes, some states offer more stringent forms of protection to both consumers and financial institutions. A few of these states include California, the District of Columbia, and Minnesota. Below, Table 2 lists the range of penalties that exist in these three states for identity theft, and illustrates how states treat such penalties under various categories of description. These penalties do not represent all forms of enforcement for identity theft crimes in the U.S., but they do highlight how local jurisdictions are dealing with identity theft. In particular, California's approach to identity theft is examined for its modern application of consumer protection.

---

[89] Federal Trade Commission, Provisions of New Fair and Accurate Credit Transactions Act Will Help Reduce Identity Theft and Help Victims Recover: FTC, *available at* http://www.ftc.gov/opa/2004/06/factaidt.htm (last visited Mar. 9, 2006).

[90] Prepared Statement of The Federal Trade Commission on Identity Theft and Social Security Numbers, Before the Subcommittee on Social Security of the House Committee on Ways and Means (June 15, 2004), *available at* http://www.ftc.gov/os/testimony/040615idtheftssntest.pdf (last visited Mar. 9, 2006) at 6.

Table 2: Privacy Statutes in Selected States Dealing With Identity Theft

State	Statute	Penalty
California	PENAL CODE SECTION 530.5 TO 530.8	Upon conviction a person shall be punished either by imprisonment in a county jail not to exceed one year, a fine not to exceed **$1,000**, or both that imprisonment and fine, or by imprisonment in the state prison, a fine not to exceed **$10,000**, or both that imprisonment and fine.[91]
District of Columbia	IDENTITY THEFT EMERGENCY AMENDMENT ACT OF 2003- SECTION 126O	Identity theft in the first degree. -- Any person convicted of identity theft shall be fined not more than (1) **$10,000**, (2) three times the value of the property obtained, or (3) three times the amount of the financial injury, whichever is greatest, or imprisoned for not more than 10 years, or both, if the property obtained or the amount of the financial injury is **$250** or more. Identity theft in the second degree. -- Any person convicted of identity theft shall be fined not more than **$1,000** or imprisoned for not more than 180 days, or both, if the value of the property obtained or the amount of the financial injury, whichever is greater, is less than **$250**. Any person who commits the offense of identity theft against an individual who is 65 years of age or older, at the time of the offense, may be punished by a fine of up to 1 1/2 times the maximum fine otherwise authorized for the offense and may be imprisoned for a term of up to 1 1/2 times the maximum term of imprisonment otherwise authorized for the offense, or both. [92]
		If: (a) Single Direct Victims, with total loss of less than $250 *Penalty*: imprisonment of not more

[91] National Conference of State Legislatures, Identity Theft Statutes, *available at* http://www.ncsl.org/programs/lis/privacy/idt-statutes.htm (last visited Apr. 1, 2006) [hereinafter National Conference Statutes].

[92] *Id.* See also An Act in the Council of the District of Columbia, *available at* http://www.usdoj.gov/usao/dc/Legislation/Identity_Theft_Emergency_Amendment_Act_2003.pdf (last visited Apr. 9, 2006).

Minnesota	IDENTITY THEFT – CHAPTER 609.527	than 90 days, or fine of maximum $700, or both (b) Single Direct Victims, with total loss between $250 and $500 *Penalty*: imprisonment of not more than 1 year, or fine of maximum $3,000, or both (c) Two or Three Direct Victims, with total loss between $500 and $2,500 *Penalty*: imprisonment of not more than 5 years, or fine of maximum $10,000, or both (d) Four or more Direct Victims with total loss more than $2,500 *Penalty*: imprisonment of not more than 10 years, or fine of maximum $20,000, or both[93]

California: The Identity Theft Registry and Bill SB 168

In 2004, California reported approximately 43,839 cases of identity theft affecting consumers.[94] New forms of identity theft such as unemployment insurance fraud and fraudulent online escrow services are finding its way into the marketplace.[95] In California, it is a felony to use the personal data of another person for any unlawful purpose without their authorization, including the obtaining of credit, goods, services, or medical information.[96] In other instances, California law requires businesses and government agencies to notify consumers if hackers are successful in obtaining personal information from unencrypted sources such as credit card numbers, personal account

[93] *Id.*
[94] Office of the Attorney General, State of California, Dept. of Justice, *available at* http://caag.state.ca.us/idtheft/ (last visited Mar. 1, 2006) [hereinafter CA Attorney General].
[95] Locking Up the Evil Twin: A Summit on Identity Theft Solutions, Perspectives and Recommendations From Governor Arnold Schwarzenegger's March 1, 2005 Summit, Sacramento, California, *available at* http://www.idtheftsummit.ca.gov/2005_report.pdf (last visited Apr. 18, 2006). The California Employment Development Department has reported that identity thieves steal identities in order to fraudulently claim unemployment benefits. Here, verifying one's Social Security Number by way of a toll-free hotline and web-based reporting system for complainants allows individuals to guard against fraudulent unemployment claims. By comparison, fraudulent online escrow services, as indicated by the California Department of Corporations (CDC), is a new online scam that involves misrepresenting oneself as a legitimate escrow company (independent third party) that acts as a medium between buyers and sellers by offering a safe means of paying for items sold on auction websites and marketplaces. These online escrow companies are set up through stolen identities and credit card numbers. These artificial websites convey the impression that they are licensed by CDC, often providing a link to the Department's website.
[96] *Id.* California's Penal Code 530.5. Under California's Constitution, Art. 1, sec.1 gives each citizen the "inalienable right" to pursue and obtain privacy. See generally California Constitution, *available at* http://www.leginfo.ca.gov/.const/.article_1 (last visited Mar. 8, 2006).

pass-codes, Social Security numbers, and driver's license numbers.[97] Given this, California was the first state to establish the Office of Privacy Protection in 2001.[98]

California also operates a five regional Hi-Tech Crimes Task Forces.[99] Here, an elaborate mechanism of detecting identity theft is firmly in place. For instance, the Attorney General of California keeps an *Identity Theft Registry* to help avoid identity theft victims from being accused of crimes committed under their names (mentioned supra as criminal identity theft).[100] This arises in instances when criminal identity theft involves the arrest of a criminal who uses another person's name.[101] This registry enables law enforcement agencies to verify whether or not a person is linked with specific crimes, or whether they are mistakenly identified on that basis.

The procedures in California has two effects: (1) either an innocent consumer may present information to law enforcement agencies verifying that their name is stolen when an arrest warrant is issued, or (2) to enter an appearance in court to determine factual innocence, to which a court may grant a court order stating that one is factually innocent, and will modify the *Identity Theft Registry*.[102] Moreover, a victim may also request a court order informally by appearing in a hearing held for the thief's case. When an innocent person discovers that their name is being used by an identity thief, they may file a petition known as the *Petition to Seal and Destroy Arrest Records* to clear their name.[103] Upon submitting proper information, the California Department of Justice will enter one's name in a state-wide database.

---

[97] *Id.* Under state law AB 1386-Peace/Chapter 915 Stats of 2002, any breach of privacy must be reported to consumers immediately after discovery unless a law enforcement agency feels that the notice would interfere with their conducting an investigation on the same matter.

[98] Office of Privacy Protection, About Us, *available at* http://www.privacy.ca.gov/cover/about.htm (last visited Apr. 18, 2006). This department is devoted to educating consumers, businesses, and others about the effects of privacy-related issues such as identity theft, and how to cushion against the effects of privacy matters on the marketplace.

[99] *Id.*

[100] *Id.*

[101] California Dept. of Consumer Affairs, Office of Privacy Protection, *How to Use the California Identity Theft Registry*, *available at* http://www.privacyprotection.ca.gov/sheets/cis8englsih.pdf (last visited Mar. 1, 2006). This registry provides consumers with guidelines to help clear their name when criminals disclose another innocent person's identity when being questioned.

[102] CA Attorney General, *supra* note 1. The court order is also known as Certificate of Identity Theft: Judicial Finding of Factual Innocence. See p. 3, *available at* http://www.privacyprotection.ca.gov/sheets/cis8englsih.pdf (last visited Mar. 1, 2006). This measure effectively guards against criminal identity theft.

[103] *Id* .California Penal Code s. 851.8.

In 2002, a California bill known as SB 168 was enacted to limit the use of Social Security numbers in the private sector, while allowing consumers to place either a fraud alert or a freeze on their credit report.[104] The SB 168 bill prevents businesses from utilizing a consumer's Social Security number after July 1, 2002 when: (1) posting or displaying Social Security numbers; (2) printing Social Security numbers on identification cards; (3) requiring a person to transmit a Social Security number over the Internet only when the connection is secure or the Social Security number is encrypted; (4) requiring a person to use passwords or other authentication devices; and (5) printing a Social Security number on materials or documents to be mailed to consumers, unless the law provides otherwise.[105]

Other portions of SB 168 allow consumers to freeze their credit record at each credit bureau.[106] The significance of credit-freezes is to prevent identity thieves from using consumers' personal data to obtain loans or credit in their name.[107] This is helpful because creditors (such as lenders, retailers, or utilities) need access to credit reports to determine whether loans or credit should be granted to a consumer. Once a credit report is frozen, it becomes difficult for the identity thief to derive any benefit because their use of a consumer's personal data will show up immediately on the credit report. This is

---

[104] Fight Identity Theft, *Identity Theft Legislation*, *available at* http://www.fightidentitytheft.com/identity-theft-laws.html (last visited Mar. 7, 2006). This bill, known as SB 168, was introduced by Senator Deborah Bowen in 2002. The Social Security Administration (SSA) may assist a consumer who falls victim to identity theft. In this case, a consumer may contact the SSA to receive a new Social Security number. The only instances where the SSA does not give new Social Security numbers is when a consumer: (1) files for bankruptcy; (2) intends to avoid the law; and (3) fails to prove that their Social Security number is being misused by another party. A consumer may contact the Social Security Administration toll-free at 1-800-772-1213. See generally Social Security Online, Electronic Leaflets, *available at* http://www.ssa.gov/pubs/10064.html#getting (last visited Mar. 10, 2006).

[105] http://www.fightidentitytheft.com/legislation_california_sb168.html (last visited Mar. 7, 2006). The Social Security restrictions generally apply to businesses as long as customers with existing accounts opened before July 1, 2002 opt-out of such uses at their request. However, the health care and insurance industries must comply with the Social Security restrictions.

[106] *Id.* California Law SB 168 (Debra Bowen) Identity Theft Prevention, *available at* http://www.fightidentitytheft.com/legislation_california_sb168.html (last visited Mar. 7, 2006). Similar credit-freezes are found in Connecticut, Illinois, Louisiana, Maine, Nevada, North Carolina, Texas, Vermont, and Washington. Any citizen of the state permitting credit-freezes may request to freeze their credit report. This process requires formal submission in writing to anyone of the three consumer reporting agencies (Equifax, Experian, and TransUnion). Normally, a consumer requesting credit freezes does not have to pay for this service. However, the consumer may have to provide documentation from a police report. See generally http://www.fightidentitytheft.com/legislation_california_sb168.html (last visited Mar. 7, 2006).

[107] *Id.* The credit report freeze provisions of SB 168 became effective Jan. 1, 2003.

precisely why a credit report obtained from the three major consumer reporting agencies become useful in guarding against identity theft.

The SB 168 bill essentially codifies the practice of credit bureaus allowing consumers to place fraud alerts on their credit reports.[108] However, despite the temporary freeze on a consumer's account, SB 168 still allows a consumer to obtain new loans or credit under their name. Here, credit bureaus must use a PIN-based system that sees a consumer provide their PIN or password to the credit bureau, while transferring their credit report to lenders for consideration.[109] The bill thus provides consumers the choice of placing fraud alerts on their credit reports, or placing credit freezes on their accounts, all the while giving consumers the freedom to pursue other forms of credit.

The difference in choice affects the degree of protection for the consumer in that once a consumer places a fraud alert, credit bureaus are obligated to provide a toll-free phone number available 24 hours a day, place the alert within 72 hours of receiving the request, hold the alert for 90 days, and provide a free copy of the credit report once the 90-day period is over.[110] The legal remedies offered by SB 168 for violations of credit freezes or fraud alerts provides a consumer who suffers loss to sue for injunctive relief and general damages, including court costs, loss of wages, attorney's fees, and, where applicable, pain and suffering.[111]

Other California identity theft laws provide consumers with greater protections from the effects of identity theft. For instance, Civil Code Section 1788.18 (Debt Collection: Identity Theft Victim Rights) offers protection for consumers who are sought by debt collectors for debts incurred by the identity thief.[112] More specifically, it requires debt collectors to stop collecting from those consumers who have filed identity theft reports to the police, or have adduced evidence to hold themselves out as victims of

---

[108] *Id.*

[109] Fight Identity Theft, *Credit Report Freeze*, *available at* http://www.fightidentitytheft.com/legislation_california_sb168.html (last visited Mar. 7, 2006). Credit bureaus are required to release the report within 3 business days of the request.

[110] *Id.*

[111] *Id.* The provisions under SB 168 that relate to credit freezes and consumer fraud alerts amended the California Credit Reporting Agencies Act (CRAA), Civil Code Section 1785.1 et seq. Thus, the remedies under the CRAA apply for credit freezes and consumer fraud alerts.

[112] California Dept. of Consumer Affairs, *Identity Theft*, *available at* http://www.privacy.ca.gov/lawenforcement/laws.htm#five (last visited Mar. 8, 2006).

identity theft.[113] Once a debt collector determines that a consumer is not responsible for the debt, it must inform the consumer of that finding. The legislation goes further to provide that a consumer may clear their name by having the debt collector, who ceases to collect debts, to dutifully inform creditors and consumer reporting agencies that their initial consumer information was erroneous, and that necessary modifications should be invoked.

Other privacy laws such as California's Penal Code Section 1524 permits law enforcement authorities to obtain search warrants from a county's magistrate for persons or property located in another county.[114] Given that identity theft can occur in multiple jurisdictions, conflict of laws rules suggest that the jurisdiction to bring a criminal action for identity theft in California is normally the county where the theft occurred or where the identity was unlawfully used.[115] On the other hand, if the identity theft occurs in several jurisdictions from various sources, any of these jurisdictions may serve as a convenient forum for initiating identity theft claims, depending on how substantial the identity theft crime is connected to the jurisdiction where the victim is located.

Given the developments in the area of privacy, current efforts to engage consumers about identity theft include California's second summit entitled *Teaming Up Against Identity Theft: A Summit on Solutions*.[116] The focus of this summit was to engage consumers, businesses, law enforcement agencies, federal and state departments, and financial institutions about identity theft. Moreover, new technologies and victim assistance relating to personal data was prominently displayed. The participation of the Federal Trade Commission at this summit clearly indicates both the degree of cooperation between federal and state authorities, and the sense of urgency in dealing with identity theft's impact on the marketplace.

---

[113] *Id.*

[114] *Id.* § 1524 (c) of California's Penal Code does not pertain to documentary evidence in the possession and control of lawyers, a physician, a psychotherapist, or a member of the clergy.

[115] Calif. Dept. of Consumer Affairs, *Identity Theft, available at* http://www.privacy.ca.gov/lawenforcement/laws.htm#five (last visited Mar. 8, 2006). California's Penal Code §786 is labeled as 'Consolidation of Identity Theft Cases'. Here, the traditional conflicts of law principle of *lex loci delecti*, where jurisdiction to hear a case is proper where the place of the harm occurred, is applied for identity theft occurrences in either a single jurisdiction or multiple jurisdictions.

[116] State of Calif., State and Consumer Services Agency, Press Release (Oct. 14, 2005), *available at* http://www.scsa.ca.gov/RecentNews/pr10.13.05idtheftsummit.htm (last visited Apr. 18, 2006). This summit was convened by Governor Arnold Schwarzenegger, the California State and Consumer Services Agency, the California Department of Consumer Affairs, and the California District Attorneys Association.

District of Columbia

The District of Columbia (D.C.) recently amended its Theft and White Collar Crimes Act of 1982 to include identity theft as a crime as part of its consumer protection legislation.[117] Known as the Identity Theft Emergency Amendment Act of 2003, determining penalties against those guilty of identity theft, the District of Columbia divides identity theft into first degree and second degree categories. In each of these categories, D.C. charges any wrongdoer with three times the value of property stolen or three times the financial injury.[118] Moreover, under the second degree penalty of identity theft, D.C.'s legislation provides enhanced penalties for persons committing identity theft against elder citizens over the age of 65, whereby a fine of 1 ½ times the fine of $1,000 or 1 ½ times the maximum term of imprisonment.[119]

The Act in D.C. provides the most modern definition of personal identifying information, including: (1) name, address, telephone number, date of birth, or mother's maiden name; (2) driver's license number; (3) savings, checking, or other financial account number; (4) Social Security Number, or tax identification number; (5) passport number; (6) citizenship status, visa, or alien registration card or number; (7) birth certificate; (8) credit or debit card; (9) credit history; (10) signature; (11) personal identification number, electronic identification number, password, access code or device, electronic address, routing information or code, digital signature, or telecommunication identifying information; (12) biometric data (such as fingerprint, voice print, retina or iris image, or other unique physical representation); (13) place of employment, employment history, or employee identification number; and (14) any other numbers of information that can access a person's financial resources, medical information, or obtain property.[120]

Using this comprehensive definition, D.C. monitors the types of identity theft crimes. At present, the most frequent identity theft crime reported in D.C. involves credit

---

[117] An Act in the Council of the District of Columbia, *available at* http://www.usdoj.gov/usao/dc/Legislation/Identity_Theft_Emergency_Amendment_Act_2003.pdf (last visited Apr. 18, 2006) [hereinafter DC Council].
[118] Identity Theft Emergency Amendment Act of 2003 at § 1260(1).
[119] National Conference Statutes, *supra* note 91. See also An Act in the Council of the District of Columbia, *available at* http://www.usdoj.gov/usao/dc/Legislation/Identity_Theft_Emergency_Amendment_Act_2003.pdf (last visited Apr. 9, 2006).
[120] DC Council, *supra* note 117.

card fraud, at 41 percent.[121] Closely behind this statistic is bank fraud (at 23 percent) and phone and utilities fraud (at 22 percent).[122] Recently, in February 2006, the District of Columbia held the National Consumer Protection Week.[123] As part of this initiative, the District of Columbia Council approved funding for establishing an Office of Consumer Protection.[124] The establishment of an office dealing exclusively with privacy issues is a common feature among jurisdictions in North America to protect consumer personal data.

Minnesota

In Minnesota, there are already well-established privacy regulations that form part of the state's consumer protection laws. For instance, under its Financial Privacy Act of 2004, Minnesota requires financial institutions such as banks and mortgage companies to obtain an *affirmative consent* from consumers prior to sharing their personal information with a third party.[125] This form of consent must be in writing and signed by the consumer.[126] Under section 5 of the Act, a consumer may file a written request to a financial institution to obtain both its nonpublic personal information and a summary of procedures to enable the consumer to correct, amend, or delete this personal

---

[121] Identity Theft District of Columbia Information, Identity Theft Types Reported by District of Columbia Victims, *available at* http://101-identitytheft.com/identity-theft-district-of-columbia.htm (last visited Apr. 9, 2006). Percentage is based on 917 victims reporting from the District of Columbia.

[122] *Id.*

[123] Department of Consumer & Regulatory Affairs (District of Columbia), News Release, City Kicks Off National Consumer Protection Week in DC, *available at* http://dcra.dc.gov/dcra/cwp/view,a,11,q,635344,dcraNav_GID,1695.asp (last visited Apr. 1, 2006). This office will concentrate primarily on education, mediation, and enforcement, especially in the areas of home improvement and car repair. As part of its consumer protection program, the office will establish a web-based business license verification system to help consumers check if businesses have the requisite license to conduct business.

[124] *Id.*

[125] Office of the Attorney General, Consumer Protection Division, Legislative Efforts, Privacy/Personal Finance, *available at* http://www.ag.state.mn.us/consumer/LegislativeEfforts/LegislativeEfforts.htm#privacyfinance (last visited Apr. 2, 2006) at § 4, chapter 13E.04 [hereinafter Financial Privacy Act].

[126] Minnesota Senate, S.F. No. 810, First Engrossment – 83rd Legislative Session (2003-2004), *available at* http://www.revisor.leg.state.mn.us/bin/bldbill.php?bill=S0810.1&session=ls83 (last visited Apr. 2, 2006). Under Section 4, Subdivision 2, the affirmative consent form must be on a separate page that clearly and conspicuously discloses: (1) the time during which the consent will operate, not longer than five years; (2) each category of nonpublic personal information to be disclosed, including the consumer's social security number, account numbers, account balances, credit limits, the date of transaction, the identity of persons to whom checks are made payable, and the identity of merchants honoring the credit cards.

information.[127] In 2005, Minnesota enacted the Security Breach Disclosure Act, which requires businesses to notify Minnesota consumers when an unauthorized access of their personal data occurs electronically.[128] Here, a consumer must be notified, either through written means or by e-mail, in the event a financial institution's security system is breached.[129] This type of notice must be sent as expeditiously as possible, and without unreasonable delay.[130]

Aside from these statutes, Chapter 609.527 of Minnesota's most recent identity theft legislation provides a full range of penalties to compensate a "direct victim", which is defined as any person or entity whose identity has been transferred, used, or possessed.[131] Consumers falling under this category may pursue legal remedies on the basis of the number of adversely affected individuals and the amount of direct loss suffered. From this, remedies are calculated to provide some form of redress to victims of identity theft. Here, Minnesota emphasizes the number of victims affected by identity theft - the more victims adversely affected by identity theft, the greater the penalties imposed on identity thieves. For instance, if four or more victims lose their personal information through identity theft, the maximum penalty imposed is imprisonment of not more than 20 years, or a fine of not more than $20,000.[132]

Recent efforts are being pursued to enact identity theft legislation known as Clean Credit and Identity Theft Protection Act.[133] First, the Act allows consumers the right to place a security freeze on their credit report in order to allow their personal data to be divulged only upon their consent. Second, the Act goes further in placing limitations on using a consumer's Social Security Number, and requires more businesses to notify consumers if their personal information is utilized in suspicious circumstances. Third, consumers will be permitted to file a declaration of innocence to local police (answering

---

[127] Financial Privacy Act, *supra* note 125.
[128] Minnesota Office of the Attorney General, Protecting Your Privacy, Attorney General Mike Hatch Announces the Security Breach Disclosure Act (Feb. 18, 2005), *available at* http://www.ag.state.mn.us/consumer/PR/PR_050224SecurityBreachDisclosure.htm (last visited Apr. 2, 2006). This statute follows California's law that was enacted on July 1, 2003.
[129] *Id.*
[130] *Id.* The only exception of this notice requirement is if it would impede in a criminal investigation.
[131] Minnesota Statutes, Chapter 609.527 (Identity Theft), *available at* http://www.revisor.leg.state.mn.us/stats/609/527.html (last visited Apr. 2, 2006).
[132] National Conference Statutes, *supra* note 91.
[133] AARP, Spot ID Fraud and Stop It, AARP Works to Empower Consumers and Strengthen Laws to Fight Identity Theft, *available at* http://www.aarp.org/states/mn/mn-news/spot_id_fraud_and_stop_it.html (last visited Apr. 9, 2006).

to the criminal identity theft problem), while providing notice to future creditors on a no-fault basis. Finally, the Act would give consumers monthly access to credit reports for a minimal fee.[134] Such aggressive measures reveal a clear intent by local law-makers to respond directly to identity theft, particularly for online commercial activity.

Establishing Common Ground Between U.S. and Canadian Privacy Initiatives

In the context of consumer protection, remarkable similarities in the enforcement of identity theft measures exist between the U.S. and Canada. These similarities include: (1) the highly coordinated online complaint forums offered by federal and local jurisdictions; (2) allowing consumers to contact consumer reporting agencies and correct personal identifying information; (3) the utilization of consumer toolkits; and (4) the strong interplay between federal and local privacy laws. Designed to protect personal identifying information belonging to the average consumer, much of the U.S. initiatives find its way into Canadian privacy legislation, including an integrated approach involving federal and local authorities employing conventional methods of responding to consumer complaints of identity theft, as well as online complaint systems to initiate formal investigations by local and federal law enforcement agencies.

V. CURRENT TRENDS TO REGULATE IDENTITY THEFT IN CANADA

Canada

The Privacy Framework in Canada

Canada is beginning to play an active role in guarding against the effects of identity theft in its marketplace. This is a result of a major increase in identity theft complaints from 31,117 in 2000 to 161,819 in 2002.[135] Drawing largely from U.S. consumer protection initiatives, the federal government and various provinces have

[134] Retired Educators Association of Minnesota (REAM), The REAM News, AARP Minnesota Legislative Updates, *available at* http://www.mnream.org/pages/786440/index.htm (last visited Apr. 9, 2006).
[135] Public Safety Canada, *supra* note 4.

enacted legislation and local initiatives that specifically target identity theft. Like the Federal Trade Commission in the U.S., the Ministry of Public Safety and Emergency Preparedness Canada (PSEPC) is a federal agency that provides constructive guidance on identity theft matters in the best interests of Canadian consumers.[136] The PSEPC and the federal Royal Canadian Mounted Police (RCMP) have partnered together to provide victims of identity theft with useful online resources, while also encouraging them to contact consumer reporting companies such as *Equifax* and *TransUnion*.[137] Using these federal efforts, several Canadian provinces provide legal redress for victims of identity theft crimes.

The Commercial Crime Section of the RCMP often partners with local law enforcement agencies and privacy industry representatives in offering consumer protection.[138] In provinces like Ontario, law enforcement agencies often recommend that consumers contact *PhoneBusters*, a national agency responsible for monitoring fraudulent activity in the marketplace.[139] Recognizing the need to mobilize an integrated approach to consumer protection, federal, provincial, and territorial ministers responsible for consumer affairs in their respective jurisdictions came together in January 2004 to raise awareness about identity theft, and its impact on the consumer and economy.[140]

---

[136] *Id.*

[137] Ottawa Police Service, Organized Fraud Section, *available at* http://www.ottawapolice.ca/en/serving_ottawa/support_units/fraud_identity.cfm (last visited Mar. 7, 2006). The Royal Canadian Mounted Police (RCMP) is Canada's national police service, and an agency for the Ministry of Public Safety and Emergency Preparedness (PSEPC). The RCMP operates at the federal and provincial levels, and provides policing services for approximately 198 municipalities and 192 First Nations communities. The RCMP is equivalent to the Federal Bureau of Investigations (FBI). See generally RCMP, About the RCMP, *available at* http://www.rcmp-grc.gc.ca/about/index_e.htm (last visited Mar. 18, 2006).

[138] Royal Canadian Mounted Police, Financial Integrity, *available at* http://www.rcmp-grc.gc.ca/qc/pro_ser/int_finan_e.htm#Delits (last visited Mar. 11, 2006). The Commercial Crime Section investigate and control white-collar crimes on provincial, federal, and international cases. This section focuses primarily on: (1) Counterfeiting; (2) Bribery and Corruption; (3) Fraudulent Bankruptcy; and (4) General Fraud.

[139] *Id.*

[140] Consumer Measures Committee, Identity Theft, *available at* http://cmcweb.ca/epic/internet/incmc-cmc.nsf/en/fe00084e.html (last visited Mar. 10, 2006). The Consumer Measures Committee (CMC) is a consumer protection body that was created under Chapter Eight of the Agreement on Internal Trade (AIT). The CMC has a representative from the federal government and each provincial and territorial governments. The CMC's main objective is to provide a national forum on consumer protection and break down barriers between the provinces and territories by harmonizing laws, focusing on regulations and policies, and raising public awareness of key issues affecting the Canadian marketplace. See generally Consumer Measures Committee, About the CMC, *available at* http://cmcweb.ca/epic/internet/incmc-cmc.nsf/en/h_fe00013e.html (last visited Mar. 10, 2006).

The result was the formation of a multi-jurisdictional Consumer Measures Committee (CMC) task force that will monitor and educate the general public about identity theft crimes in Canada. In July 2005, consumer advocates across Canada also developed a public consultation paper called *Working Together to Prevent Identity Theft*.[141] This gathering revealed that identity theft equally impacts several areas of commerce. Below, Table 3 summarizes these key findings from this public consultation paper, reflected by the percentage in which various crimes occur.[142]

Table 3: Key Areas of Commerce Affected by Identity Theft (by percentage in occurrence)

Opening of a New Credit Card Account	Insurance or Payment Fraud	Obtaining Government Benefits	Opening of a New Telephone or Utility Account	Obtaining Fraudulent Loans
36 %	**24%**	**24%**	**23%**	**22%**

As part of this initiative, consumers and industry stakeholders provided input on proposed legislation that would aim to protect consumers from identity theft crimes. Key topics included in the public consultation paper included:

> (1) a requirement for organizations to provide *notice* to consumers who experience a security breach and credit bureaus who handle consumer credit reports;
> (2) a streamlined procedure to place *fraud alerts* on consumer's credit reports;
> (3) the ability for consumers to place a *freeze on their credit reports* prior to contacting credit reporting agencies;

---

[141] Govt. of Alberta, National Consultation Launched on Fight Against Identity Theft (July 5, 2005), *available at* http://www.gov.ab.ca/acn/200507/183924D67E2F5-12BF-4433-9F99D47077BBA8A6.html (last visited Mar. 10, 2006). In Canada, a public consultation gives the government an opportunity to receive input from the general public on substantive issues. Citizens may provide their input by e-mailing, filling in online forms and surveys, or attend town hall meetings. From here, the government will formulate policies and legislation to reflect the emerging public sentiments. See generally Govt. of Alberta, Public Consultations, *available at* http://www.gov.ab.ca/home/index.cfm?Page=617 (last visited Mar. 10, 2006). For a complete overview of the public consultation paper, see *Working Together to Prevent Identity Theft*, *available at* http://cmcweb.ca/epic/internet/incmc-cmc.nsf/vwapj/DiscussionPaper_IDTheft.rtf/$FILE/DiscussionPaper_IDTheft.rtf (last visited Mar. 10, 2006).

[142] Working Together to Prevent Identity Theft: A Discussion Paper for Public Consultation, *available at* http://cmcweb.ca/epic/internet/incmc-cmc.nsf/vwapj/DiscussionPaper_IDTheft.rtf/$FILE/DiscussionPaper_IDTheft.rtf (last visited Mar. 10, 2006) at 5.

(4) a requirement for credit bureaus to *take reasonable steps to authenticate* a person's identity before accessing credit reports [143]
(5) removing Social Insurance numbers on credit reports or preventing their use as a unique identifier for consumers[144]

Aside from these initiatives, the CMC also provides consumers and businesses with identity theft toolkits. The toolkit available for businesses is known as the *Identity Theft Kit for Business*, a resource that permits businesses to combat theft of personal data within its organization.[145] This is in response to the growing trend of identity theft occurring within businesses. Often times, businesses contracting with each other and third parties expose personal information of their employees or clients on computers, file cabinets, and other means.[146] Canadian consumers may also refer to law enforcement agencies that utilize a special online mechanism known as Reporting Economic Crime Online (RECOL).[147] The RECOL initiative is an integrated partnership between international, federal, provincial law enforcement agencies, and private industry representatives that investigate complaints of online identity theft. Here, RECOL collects consumer fraud complaints and directs these complaints to relevant law enforcement authorities.[148] The complaint procedure is well-guarded in terms of who can access the online complaint system, while carefully ensuring privacy of content.

Since adducing evidence is crucial in proving one has been a victim of identity theft (and may likely be a victim in future attempts), the RECOL program highly recommends that consumers gather and collect canceled checks, credit card receipts,

---

[143] *Id.*
[144] Govt. of Ontario, Ministry of Govt. Services, McGuinty Govt. Seeks Public Input on How to Best Prevent Identity Theft (July 6, 2005), *available at* http://www.cbs.gov.on.ca/mcbs/english/nr0705051.htm (last visited Mar. 10, 2006).
[145] Identity Theft, Protect Your Business, Protect Your Customers, Identity Theft Kit for Business, *available at* http://cmcweb.ca/epic/internet/incmc-cmc.nsf/vwapj/busidtheftkit.pdf/$FILE/busidtheftkit.pdf (last visited Mar. 18, 2006). This kit is produced by the Federal-Provincial-Territorial Consumer Measures Committee, in association with Phonebusters (The Canadian Anti-Fraud Center).
[146] *Id.* at 1.
[147] RECOL.ca, Welcome to RECOL, *available at* https://www.recol.ca/intro.aspx?lang=en (last visited Mar. 11, 2006). RECOL is a web-based tool offering Canadian consumers to file formal complaints regarding economic crimes online. These complaints may include any identity theft-related crimes, which are forwarded to law enforcement agencies and organizations dealing with white collar crime.
[148] *Id.* Essentially, RECOL recommends key law enforcement agencies or private commercial groups to consumers who need guidance on identity theft issues. RECOL also provides information on current fraud trends, and offers education, prevention and awareness of economic crimes. The RECOL website requires one to register as a person or organization, requests a username and password, and requires one's name, address, telephone number, and e-mail. RECOL can be reached at 1-888-495-8501. See generally RECOL.ca, *available at* https://www.recol.ca/howtofile.aspx (last visited Mar. 11, 2006).

stocks, bonds (or other security documents), phone bills, faxes, pamphlets or brochures, mail receipts, printed copies of websites. These forms of documentary evidence will serve as part of the prosecution for criminal investigations. The RECOL program is delivered through the National White Collar Crime Center of Canada and the Royal Canadian Mounted Police.

Identity theft options are also provided through other national programs such as the Canadian Consumer Information Gateway.[149] This national program collectively gathers consumer tips and resources from thirty-eight departments and agencies of the Government of Canada. Like consumer-oriented organizations, this gateway provides: (1) consumers to file online complaints; (2) a showcasing of specific privacy issues; (3) a review of consumer tips; and (4) compendium of legal rights.[150]

Recent Examples of Identity Theft in Canada

Recently, Ottawa police uncovered an identity theft scam worth $500,000 that affected 120 victims across Canada for bogus credit cards.[151] Here, two suspects were arrested for carrying sixty credit cards, Social Insurance numbers, and driver's licenses issued in the names of other persons. The two suspects used online employment ads to attract consumers to send their resumes to potential employers, promising high-paid jobs. The consumer would be required to send a $20 administration fee, along with an application form that asked for personal information such as name, address, and Social Insurance numbers.[152]

From this personal information, the identity thieves managed to secure credit cards for purchasing high-end electronic products. This credit card scam was discovered when a consumer complained to Canada Post that his mail was not being delivered. Later,

---

[149] Canadian Consumer Information Gateway, *available at* http://consumerinformation.ca/app/oca/ccig/main.do?language=eng (last visited Mar. 18, 2006). The Canadian Consumer Information Gateway is a website that offers Canadian consumers an opportunity to seek trustworthy information from services offered by over 400 federal agencies, provincial and territorial ministries, and non-governmental organizations. This project is administered by Industry Canada's Office of Consumer Affairs. This gateway is helpful in displaying the latest online scams.

[150] *Id.*

[151] Canadian Broadcasting Corporation, Ottawa Police Break Up Major Identity Theft Scam, *available at* http://www.cbc.ca/ottawa/story/ot-theft20060309.html (last visited Mar. 19, 2006).

[152] *Id.* Various fake company names were used such as Microtel Media, Logistic Telecomm, Idcor, and Pastel Media.

Canada Post found that this consumer's mail was transferred, but without the consent of the consumer. When Canada Post contacted Ottawa Police, similar occurrences of mail transfer were found by investigators that affected other consumers.

Key Federal Privacy Statute in Canada – The Personal Information Protection and Electronic Documents Act (PIPEDA)

Managed by a federal agency known as Industry Canada, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) is the main federal statute that provides personal data protection for consumers.[153] The Act defines personal information as being information about an "identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization".[154] Enacted in October 1998, PIPEDA establishes rules for organizations to manage personal information of consumers within commercial activities. The Act requires businesses to put systems in place to ensure that consumer personal data is secure, accurate, gathered with consent, and not used haphazardly.[155]

Furthering these privacy initiatives, Canada Post Corporate Security actively engages in joint investigations with federal and provincial authorities.[156] The Canada Post Act empowers Canada Post Corporate Security to provide security to consumers by pursuing complaints as a federal investigative body.[157] Both *Equifax* and *TransUnion*

---

[153] Personal Information Protection and Electronic Documents Act (PIPEDA), *available at* http://laws.justice.gc.ca/en/P-8.6/text.html (last visited Mar. 15, 2006) at § 2(1). The PIPEDA statute was introduced in the House of Commons in October 1998 as Bill C-54. It was re-introduced as Bill C-6 upon the opening of Parliamentary session in October 1999. The Senate passed this bill with two amendments related to personal health information.

[154] *Id.*

[155] Identity Theft, Protect Your Business, Protect Your Customers, Identity Theft Kit for Business, Identity Theft: Recognize It, Report It, Stop It, *available at* http://cmcweb.ca/epic/internet/incmc-cmc.nsf/vwapj/busidtheftkit.pdf/$FILE/busidtheftkit.pdf (last visited Mar. 18, 2006).

[156] Canada Post, Postal Security, How to Protect Yourself from Identity Theft, *available at* http://www.canadapost.ca/business/corporate/about/security/id_theft-e.asp (last visited Mar. 13, 2006). Canada Post Corporate Security is Canada Post's principal security advisor to its employees and customers in providing security for mail, information, personnel, and assets of Canada Post. Corporate Security is divided into 11 security programs: (1) Information Security; (2) Planning for Business Continuity; (3) Security Awareness; (4) Personnel Security; (5) Physical and Technical Security; (6) Retail Services Security; (7) Products and Process Development; (8) Financial Systems Security; (9) Investigative Standards and Procedures; (10) Loss Analysis and Control; and (11) Risk Management Network.

[157] Canada Post, Postal Security, About Us, *available at* http://www.canadapost.ca/business/corporate/about/security/default-e.asp (last visited Mar. 13, 2006).

indicate that between 1400 to 1800 identity theft complaints are received from Canadian consumers every month.[158]

Identity Theft Statutes in Selected Canadian Jurisdictions

Various forms of privacy and identity theft legislation in Canada jurisdictions are intricately linked with the federal PIPEDA statute. For example, in dealing with issues of credit reporting, Alberta's Fair Trading Act (one of the province's consumer protection statutes) requires a reporting agency to maintain consumer information that is used in accordance with PIPEDA and Alberta's Personal Information Protection Act.[159] That is, provincial privacy legislation draws from federal procedures that require reporting agencies to provide accurate and complete information to consumers on credit reports, while keeping in spirit with local privacy laws. Moreover, before a provincial reporting agency discloses credit information to a consumer requesting a credit report, the reporting agency must receive reasonable identification, similar to PIPEDA's "identifiable individual" requirement.[160]

In most Canadian jurisdictions, the privacy legislation allows consumers to add, delete, or modify their personal information on credit reports in order to verify as to their true content. Below, Table 4 illustrates various identity theft provisions from selected jurisdictions. Although only Alberta, British Columbia, Québec, and Ontario are discussed, statutes from Saskatchewan and Manitoba are meant to show how similarly-worded their privacy legislation is with other Canadian jurisdictions.

---

[158] Canada Post, Corporate Security, How to Protect Yourself from Identity Theft, *available at* http://www.canadapost.ca/business/corporate/about/security/pdf/id_theft-e.pdf (last visited Mar. 13, 2006) at 1.

[159] Alberta Regulation 193/99, Fair Trading Act, Credit and Personal Reports Regulation, *available at* http://www.qp.gov.ab.ca/documents/Regs/1999_193.cfm?frm_isbn=0779720083 (last visited Mar. 18, 2006) at § 2.1(a)(2).

[160] *Id.* at § 7(a)-(b). In Alberta, if a consumer discovers incorrect information on their credit reports, they may submit a written protest with the reporting agency. See § 3.3(1) of Alberta Regulation 193/99. Thereafter, under § 3.3(2) the reporting agency must check the accuracy and completeness of the disputed information, and must provide copies of these changes to the consumer in question. Section 4(1) of Alberta Regulation 193/99 prohibits reporting agencies from reporting (or storing on file) a consumer's health and health care history, sexual orientation, and information about a consumer's family.

Table 4: Identity Theft Statutes in Selected Canadian Jurisdictions and Pertinent Provisions

Province	Privacy Statutes with pertinent provisions
British Columbia	**Personal Information Protection Act – Section 23(1)** ". . . an organization must provide the individual with the following: (a) the individual's personal information under the control of the organization; (b) information about the ways in which the personal information referred to in paragraph (a) has been and is being used by the organization; (c) the names of the individuals and organizations to whom the personal information referred to in paragraph (a) has been disclosed by the organization." [161]
Alberta	**Personal Information Protection Act – Section 25** **Right to request correction** 25**(1)** An individual may request an organization to correct an error or omission in the personal information about the individual that is under the control of the organization. **(2)** If there is an error or omission in personal information in respect of which a request for a correction is received by an organization under subsection (1), the organization must, subject to subsection (3), (a) correct the information as soon as reasonably possible, and (b) where the organization has disclosed the incorrect information to other organizations, send a notification containing the corrected information to each organization to which the incorrect information has been disclosed, if it is reasonable to do so. **(3)** If an organization makes a determination not to make the correction under subsection (2)(a), the organization must annotate the personal information under its control with the correction that was requested but not made. **(4)** On receiving a notification under subsection (2)(b) containing corrected personal information, an organization must correct the personal information in its custody or under its control.

[161] Personal Information Protection Act, SBC 2003, c. 63, at § 23(1)(a)-(c). This rule is similarly applied under s. 23(2) toward credit reporting agencies who must provide the individual with the name of the sources from which it received the personal information.

Saskatchewan	**Privacy Act – Section 3(c)** ". . . proof that there has been: use of the name or likeness or voice of a person for the purposes of *advertising* or *promoting the sale* of, or any other *trading* in, any property or services, or for any other *purposes of gain* to the user if, in the course of the use, the person is identified or identifiable and the user *intended to exploit* the name or likeness or voice of that person . . without the consent, express or implied, of the person or some other person who has the lawful authority to give consent is prima facie evidence of a violation of the privacy of the person first mentioned." [162]
Manitoba	**The Privacy Act – Section 3(c)** " . . . privacy of a person may be violated . . . by the unauthorized use of the name or likeness or voice of that person for the purposes of *advertising* or *promoting the sale* of, or any other *trading* in, any property or services, or for any other *purposes of gain* to the user if, in the course of the use, that person is identified or identifiable and the user intended to exploit the name or likeness or voice of that person. . ." [163]
Ontario * this is Canada's most recent identity theft statute	**Victims of Identity Theft Act (Not Yet Enacted - Private Member's Bill – 1st Reading Only)** **Application for certificate** 2 (1) Every person who is the victim of identity theft may apply to the Deputy Attorney General for the issuance of a certificate confirming their identity and the fact that they have been the victim of identity theft. **Certificate proof of facts** (2) For all purposes, a certificate issued under subsection (1) is proof of the facts stated in it and may be filed with any institution, financial institution or similar body. **Certificate enforceable** (3) Any institution, financial institution or similar body with which a certificate has been filed under subsection (2) shall act upon the directions set out in the certificate *as if the certificate were an order of a court*.[164]

[162] Privacy Act, P-24, § 3(c).
[163] Privacy Act, C.C.S.M, c.P125 (Manitoba) *available at* http://web2.gov.mb.ca/laws/statutes/ccsm/p125e.php (last visited Mar. 19, 2006) at § 3(c).
[164] Legislative Assembly of Ontario, *available at* http://www.ontla.on.ca/documents/Bills/37_Parliament/Session3/b026_e.htm (last visited Mar. 21, 2006). This is also known as An Act to Provide Civil Remedies for the Victims of Identity Theft [hereinafter Bill 26].

Québec	**An Act Respecting The Protection of Personal Information in the Private Sector** "A person who collects personal information from the person concerned must, when establishing a file on that person, inform him (1) of the object of the file; (2) of the use which will be made of the information and the categories of persons who will have access to it within the enterprise; (3) of the place where the file will be kept and of the rights of access and rectification." [165]
Newfoundland and Labrador	**Privacy Act - Section 4(c)** "Proof that there has been . . . use of the name or likeness or voice of an individual for the purposes of *advertising* or *promoting the sale* of, or other *trading* in, property or services, or for other *purposes of advantage* to the user where, in the course of the use, the individual is identified or identifiable and the user *intended to exploit* the name or likeness or voice of that individual…without the consent , express or implied, of the individual or some other person who has the lawful authority to give the consent is, in the absence of evidence to the contrary , proof of a violation of the privacy of the individual first mentioned." [166]

Among the selected jurisdictions, Canadian courts generally provide remedies to victimized consumers by: (1) awarding damages; (2) granting injunctions where it is just and reasonable; (3) ordering the defendant to account to the plaintiff for any profits that have accrued; and (4) ordering the defendant to deliver to the plaintiff all articles or documents that are in identity thief's possession by reason of the violation.[167]

British Columbia (B.C.)

British Columbia's legislation creates an affirmative duty on an organization to designate individuals to ensure it complies with its Personal Information Protection

[165] An Act Respecting The Protection of Personal Information in the Private Sector, available at http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/P_39_1/P39_1_A.html (last visited Mar. 26, 2006) at § 8 [hereinafter Private Sector Act].
[166] RSNL 1990, c. P-22, § 4(c).
[167] *Id.* Under § 4(2) of the Manitoba legislation, considerations in awarding damages include: (1) nature, incidence, and occasion of the act, conduct or publication constituting the violation of privacy of that person; (2) the effect of the violation of privacy on the health, welfare, social, business, or financial position of that person or his family; (3) any relationship, domestic or otherwise, between the parties to the action; and (4) any distress, annoyance, or embarrassment suffered by that person or his family arising from the violation of privacy.

Act.[168] The Act provides that these organizations must make available to the public the "position name or title" and "contact information" of the privacy compliance officer to lodge complaints.[169] Moreover, the Act requires organizations to disclose to the consumer how their personal data was used.[170] B.C.'s legislation requires all organizations handling personal data to provide reasonable security arrangements.[171] This standard of care is found in most other Canadian jurisdictions.

British Columbia's legislation serves as a necessary tool to counteract the growing problem of identity theft in the province. For instance, an example of identity theft in B.C. occurred in the city of Coquitlam, where police recovered thousands of stolen credit cards, bank statements and identification cards.[172] These identification cards included birth certificates, Social Insurance Numbers (SIN), and health care provincial cards. Among the items found in this police raid were manuals that described how to reprogram machines, equipment to reset locks, and Canada Post uniforms and keys to residents' postal mail boxes. To safeguard against these occurrences, the *Office of the Information and Privacy Commissioner* works closely with police, government agencies, and private industry to strengthen the protections for consumers who fall victim to identity theft.[173] The OIPC is the main investigatory body responsible for monitoring consumer identity theft, but also educates organizations and consumers about their legal rights and tips to reduce the risk of identity theft.

Alberta

Alberta's Personal Information Protection Act (PIPA) is the main privacy protection statute that outlines the responsibilities of organizations that handle consumer personal data.[174] Under section 5, an organization is responsible for personal information

[168] Personal Information Protection Act, SBC 2003, c. 63, at § 4(3). Under section 5(b) of B.C's Act, organizations must develop a process to respond to complaints arising from consumers.
[169] *Id.*
[170] *Id.* at § 23(1).
[171] *Id. at* § 34.
[172] CBC.ca, British Columbia, Identity Theft Broken Up (Mar. 17, 2006), *available at* http://www.cbc.ca/bc/story/bc_identity-theft20060317.html (last visited Apr. 4, 2006).
[173] Office of the Information and Privacy Commissioner, Identity Theft Resources, *available at* http://www.oipcbc.org/sector_private/public_info/IDtheftresources(updatedDec8-05).pdf (last visited Apr. 4, 2006).
[174] *Personal Information Protection Act*, c. P-6.5 (2003), *available at* http://www.qp.gov.ab.ca/documents/Acts/P06P5.cfm?frm_isbn=0779737415 (last visited Mar. 26, 2006).

that is in its custody or under its control.[175] An organization must also designate individuals to assist consumers, develop policies and practices to help comply with the Act in a reasonable manner, and make information about the policies and practice available upon request.[176] Notification to a consumer about personal data handling practices is important in that an organization must notify a consumer in writing or orally as to the purpose for which the information is collected, and the name of a person who will act on behalf of the organization to answer the consumer's questions about the collection process.[177] Under section 25 of PIPA, several rights exist for a consumer to correct its personal information.[178] This right to correct personal information is a common feature in the Canadian privacy regime.

Another common feature in the Canadian privacy sector involves a local privacy commissioner. The role of this provincial Privacy Commissioner (Commissioner) is crucial in the investigation and resolution of privacy complaints launched by consumers.[179] In Alberta, the Commissioner is generally responsible for: (1) conducting investigations; (2) informing the public about the Act; (3) receiving public input; (4) engaging in research to comply with the Act; (5) bringing to the attention of an organization failing to assist consumers under section 27 (duty to assist); and (6) giving advice and making recommendations to organizations on their rights.[180]

The Commissioner has the power to investigate formal complaints filed by consumers relating to the handling of personal data by organizations. An organization must produce these records within 10 days of the Commissioner's request.[181] These powers of investigation also include the right to receive and examine any record the Commissioner demands.[182] The Commissioner, or any agent acting on behalf of the Commissioner, has immunity against legal proceedings, as long as its duties are exercised in good faith.[183] Simply put, the Commissioner acts as a conduit between administrative enforcement of privacy laws and consumer rights.

---

[175] *Id.* at § 5(1).
[176] *Id.* at §§ 5(3), 5(5), and 6.
[177] *Id.* at § 13(1)(a)-(b).
[178] *Id.* at § 25.
[179] *Id.* at § 36(1).
[180] *Id.*
[181] *Id.* at § 38(3).
[182] *Id.* at § 38(1)-(2).
[183] *Id.* at § 42.

Québec

Québec's privacy legislation is geared towards the private sector. Known as An Act Respecting the Protection of Personal Information in the Private Sector, the nature of personal data protection is given special emphasis.[184] Here, personal information is defined as "any information which relates to a natural person and allows that person to be identified".[185] No organization may disclose the personal data of a consumer to a third party without the express consent of the consumer in question.[186] Under section 10 of the Act, every enterprise handling personal information must establish "safety measures" to ensure confidentiality of that information, a rule found in other Canadian jurisdictions requiring "reasonable security arrangements" for the same purpose.[187]

Under Québec's legislation, there are *personal information agents* who must be registered with the province's Commission in order to apply a method of operation that serves to keep a consumer's file up to date and accurate.[188] The Commission is a provincial administrative body that enforces Québec's privacy legislation by regulating organizations handling consumer data, and investigating any matter relating to protecting personal information.[189] The Commission may enter facilities of organizations holding personal data (and passing this information to third parties), as well as examine and make copies of the personal information in any form.[190] After every five year period, the Commission must submit a report on the scope of application of the legislation.[191]

Ontario

Canada's most recent statute dealing with identity theft is Ontario's Bill 26 (2002), known as Victims of Identity Theft Act.[192] Under this legislation, consumers may apply to Ontario's Deputy Attorney General for a certificate verifying both their

---

[184] Private Sector Act, *supra* note 165. Under § 1, the Act applies to such information in various forms of media, including written, graphic, taped, filmed, computerized, or other. The Act does not apply to public bodies.
[185] *Id.* at § 2.
[186] *Id.* at § 13.
[187] *Id.* at § 10.
[188] *Id.* at § 70.
[189] *Id.* at § 81.
[190] *Id.* at § 81(1)-(2).
[191] *Id.* at § 88.
[192] Bill 26, *supra* note 164.

identity and that they have been victims of identity theft.[193] Known as *certificate proof of facts*, the certificates may be filed with any public sector organization, financial institution, or consumer reporting agency to conduct a credit check on the consumer's account.[194] As confirmation of how serious Ontario considers identity theft, these certificates must be treated by the financial institution as a court order.[195] Like other Canadian jurisdictions, the issuance of the B.C. certificates allows both financial institutions and credit reporting agencies to correct the consumer's personal information if found to be incorrect.

The Ontario consumer may seek damages against financial institutions and consumer reporting agencies for failing to adequately protect personal information, as well as failing to correct the personal information.[196] However, if the financial institution or consumer reporting agency is found to act in good faith, no action for damages will be permitted against them.[197] Overall, for the consumer, Bill 26 provides a right of action for damages against the person committing the identity theft, without proving special damages.[198] Bill 26 thus represents a contemporary approach in addressing identity theft.

Contemporary Views and Recommendations on Identity Theft: The Need to Incorporate Identity Theft into the Criminal Code

In Canada, criminal law is under federal jurisdiction, and the Criminal Code is the main source of reference in the classification and enforcement of crimes.[199] With respect to privacy protection, Canada's criminal law remains silent on the statutory definition of identity theft. Despite the Criminal Code including privacy as a listed crime, identity theft and the misuse of personal data are not specifically mentioned. Other crimes such as

[193] *Id.* at § 2(1). This certificate is known as a "certificate proof of facts" under s. 2(2).
[194] *Id.*
[195] *Id.* at § 2(3). Under § 4(2)(a)-(b), the certificate proof of facts must set out the full legal name of the victim of identity theft and the time period during which the identity theft occurred. The certificate may be issued even if no person is convicted of identity theft. See Explanatory Note.
[196] *Id.*
[197] *Id.* at § 6.
[198] *Id.* at § 5(1).
[199] Canadian Legal Information Institute, Criminal Code of Canada, R.S. 1985, c. C-46, *available at* http://www.canlii.org/ca/sta/c-46/ (last visited Apr. 2, 2006).

personation,[200] forgery,[201] and fraud[202] are clearly delineated, but were established for dealing with conventional white-collar crimes involving traditional commercial transactions, rather than more high-tech online commercial activity. Thus, the Criminal Code, by implication, may be used to protect victims of identity theft.[203] As such, in the context of identity theft and other cyber crimes, there are serious calls to substantially modify Canada's Criminal Code in dealing with more modern white-collar crimes like identity theft.

In fact, several organizations such as the Canadian Bankers Association (CBA) recommend that the Criminal Code be amended to include such terms as "identity theft".[204] The CBA echoes the sentiments of many commentators calling for the modernization of Canada's criminal laws on identity theft:

> There are approximately 30 Criminal Code offences and one offence under the National Defence Act that provide some help in addressing identity theft. Yet, the approach to dealing with identity theft in the criminal law has been on a piecemeal basis and many provisions are overlapping or are outdated. For example, it is illegal in Canada to issue a telegram in a false name, yet there are no provisions for e-mail or online communications. We are using 20th, even 19th century tools to fight 21st century problems.[205]

Recent court opinions in Ontario also signal the need for change in Canada's legislative treatment of identity theft. For instance, Justice David Stinson of the Ontario Superior Court summarized the relationship between law and technology in relation to society's goal to protect consumer personal data:

---

[200] Criminal Code at §§ 403-405. Under this provision, "personation" is defined as fraudulently impersonating any person, living or dead, with (a) an intent to gain advantage for himself or another person; (b) an intent to obtain any property or an interest in any property; or (c) an intent to cause disadvantage to the person whom he impersonates or another person. If guilty, the individual faces imprisonment of not more than ten years.

[201] *Id.* at §§ 406-414.

[202] *Id.* at § 380. Under this provision, "fraud" is defined as deceit, falsehood or other fraudulent means, and the defrauding of any property, money or valuable security or any service. If found guilty, an individual is liable to a term of imprisonment of not more than fourteen years, where the subject-matter of the offence is a testamentary instrument or the value of the subject-matter exceeds $5,000 Cdn. What is noteworthy is that the Criminal Code includes fraudulent manipulation for stock exchange information (section 382) and prohibits insider trading (section 382.1), occurrences where large amounts of personal and public information is exchanged. Yet, the Criminal Code does not cover online exchange of personal data. Thus, one needs to refer to local jurisdictional privacy statutes that cover online commercial information exchanges.

[203] Canadian Bankers Association, Identity Theft: A Prevention Policy is Needed, *available at* http://www.cba.ca/en/content/reports/Identity%20Theft%20-%20A%20Prevention%20Policy%20is%20Needed%20ENG.pdf (last visited Mar. 12, 2006) at 2.

[204] *Id.* at 1.

[205] *Id.* at 2.

> With advancements in technology, personal data of an individual can now be collected, accessed (properly and improperly), and disseminated more easily than ever before. There is a resulting increased concern in our society about the risk of unauthorized access to an individual's personal information. The traditional torts such as nuisance, trespass, and harassment may not provide adequate protection against infringement of an individual's privacy interests. Protection of those privacy interests by providing a common law remedy for their violation would be consistent with Charter values and an 'incremental revision' and logical extension of the existing jurisprudence. . . It's time to recognize the tort of invasion of privacy here.[206]

Hence, Canadian courts are indirectly calling for reforms in treating identity theft with more alacrity and precision. Recognizing that several consumer protection statutes are being modified to meet the advances in technology, it is expected that legislatures would modify the definition and scope of identity theft crimes in order to streamline consumer protection with technological innovation. How identity theft is resolved depends on the political will of jurisdictions to seek more innovative approaches to improve consumer protection. This is precisely where the crossroads between technology and law meet, thus making public policy formulation for consumerism that much more challenging.

VI. COMMON SAFEGUARDS TO PROTECT AGAINST IDENTITY THEFT IN THE UNITED STATES AND CANADA

Every jurisdiction with privacy legislation offers a number of safeguards to protect consumers from becoming victims of identity theft. These safeguards are normally offered as online complaint forums on consumer advocate websites that are affiliated with federal and state/provincial government consumer protection programs. As part of these online mechanisms, three steps are generally followed by a consumer when they discover that they have been a victim of identity theft:

---

[206] *Somwar v. McDonald's Restaurants of Canada Limited* [2006] O.J. This tort case involved a manager, Jainarine Somwar, who discovered that McDonald's had searched for his credit without his consent. Later, Mr. Somwar sued for general and punitive damages totaling $50,000 Cdn. Mr. Somwar alleged that the claim for punitive damages was "to stop the defendant from invading the privacy of other persons." (quoted from The Lawyers Weekly, Mar. 10, 2006, Vol. 25, No. 41, by John Jaffey, *Tort of Invasion of Privacy Recognized*), at 15, *available at* www.thelawyersweekly.ca (last visited Mar. 15, 2006). The Charter refers to the *Charter of Rights and Freedoms*, which represents the first thirty-four sections of Canada's constitution.

- ✓ Regularly check your credit information by requesting credit reports from any of the three consumer reporting bureaus of *Equifax, Experian,* or *TransUnion*
    - when anyone applies for credit under your name, you will be able to track this on your credit report
    - consider placing a consumer fraud alert or credit freeze
    - inform the credit bureau to remove your name from marketing lists
    - have the credit bureau call you before any new accounts are open or changed
- ✓ Contact each financial institution, credit card company, or other company that provided the identity thief with your personal data such as credit, money, goods, or services[207]
- ✓ Plan for Identity Restoration[208]

Aside from these introductory steps, consumers are also given valuable suggestions to avoid falling victim to identity theft crimes. This is because many consumers are not aware of their personal identifying information being used by identity thieves until weeks, months, or years have passed. Therefore, a list of key indicators and protective measures drawn from initiatives in the U.S. and Canada serve as common safeguards for consumers.

Key Indicators of Identity Theft

- ➢ Purchases not made by you appear on monthly bills
    - Unauthorized charges on your credit, telephone, bank accounts
- ➢ Creditor or collection agency calls about an unknown debt
- ➢ Credit card bills and bank statements do not appear in the mail, or arrive late
- ➢ You are refused when applying for credit cards, loans, mortgage, or other forms of credit

Protective Measures for Paper and Electronic Identity

Generally

- ➢ Never divulge information over the phone or Internet unless you initiate the call or e-mail (and verify the representative you are communicating with)
    - ▪ Avoid telephone solicitations that offer instant prizes or awards[209]

---

[207] Govt. of Ontario, Ministry of Govt. Services, 09-05 What if I am a Victim of Identity Theft?, *available at* http://www.cbs.gov.on.ca/mcbs/english/victim_IDtheft.htm (last visited Mar. 8, 2006).

[208] Fight Identity Theft, Are You a Victim of Identity Theft?, *available at* http://www.fightidentitytheft.com/identity_theft_learn.html (last visited Mar. 7, 2006). Fight Identity Theft is a website that raises awareness about identity theft, and provides essential tips to protect consumers. The website is a product of Dave Nielsen, who was part of an executive team for QSpace (http://www.qspace.com), the first company to offer credit reports over the Internet. QSpace normally sells products through companies like Yahoo!, e-Loan, and InfoSpace.

[209] Royal Canadian Mounted Police, Identity Theft, Tips, *available at* http://www.rcmp-grc.gc.ca/scams/identity_e.htm (last visited Mar. 7, 2006).

- If someone offers an advertisement that requires input of personal data over the phone, ask for a written application[210]
- Pay attention to your billing cycles, and communicate with your creditor if suspicious transactions appear on your statement [211]
- Cancel your credit cards and have new ones issued to you – verify with creditors whether or not your account has been fraudulently misused
- Cut up expired credit cards
- Don't divulge personal information more than necessary for contests, rebates, or draws[212]
- Carry only personal information you need – leave other pertinent items like your Social Security/Insurance at home in a safe place [213]

Bank Accounts

- Close your bank account and open a new account with updated passwords
- For fraudulent checks, immediately issue a stop payment, close your bank account, and ask the bank to contact Chex Systems, Inc. or any other check verification service it deals with[214]
- Destroy any paperwork you no longer need (such as bills, credit card statements, receipts from electronic purchases, and pre-approved credit cards) – this will prevent dumpster-diving[215]
- Keep adequate records of expenses you incur, and document the steps you took when clearing your name to restore your credit and identity

Online

- Shield your computer from viruses and spies – use unique passwords, firewalls, and anti-virus spyware protection software (and don't click on links in pop-up windows or spam e-mail)[216]
- Be suspicious of e-mails from financial institutions and Internet service providers asking for personal information. Reputable companies generally do not ask for this information (call the company's hotline to verify their website)[217]
- After completing a transaction online, make sure to sign out of the website and clear your Internet/cache file[218]

---

[210] DOJ Recommendation *supra* note 46.
[211] *Id.*
[212] Govt. of Alberta, Consumer Tipsheet (Jan. 2006), *available at* http://governmentservices.gov.ab.ca/pdf/tipsheets/identity%20theft.pdf (last visited Apr. 4, 2006),
[213] Public Safety Canada, *supra* note 4.
[214] FTC Consumer, *supra* note 35. In this way, the retailers can be notified not to accept these checks. Several check verification companies can be contacted: (1) TeleCheck at 1-800-710-9898; (2) Certegy, Inc. (formerly Equifax) at 1-800-437-5120; and (3) SCAN at 1-800-262-7771.
[215] *Id.*
[216] California Dept. of Consumer Affairs, Top 10 Tips for Identity Theft Protection, *available at* http://www.privacy.ca.gov/sheets/cis1english.pdf (last visited Mar. 8, 2006).
[217] Office of the Privacy Commissioner of Canada, About Us, *available at* http://www.privcom.gc.ca/aboutUs/message_02_e.asp (last visited Mar. 12, 2006).
[218] Govt. of Ontario, Ministry of Govt. Services, Protecting Yourself Online, *available at* http://www.cbs.gov.on.ca/mcbs/english/risk_IDtheft.htm (last visited Mar 8, 2006).

- When making charitable donations online, refer to the organization's official website instead of clicking on unofficial websites containing the organization's website link (eg. Red Cross or Salvation Army)
- Choose complex sets of passwords, including letters, numbers, and symbols that are unique to you.[219]

Reporting the Crime

- Report the identity theft to local law enforcement agencies and/or consumer reporting company immediately
- File a formal complaint with a federal agency:
  - Federal Trade Commission (U.S.), or
  - Public Safety and Emergency Preparedness (Canada)
- File a formal complaint with a private organization
  - Internet Crime Complaint Center (IC3)
  - Call PhoneBusters national call center at 1-888-495-8501 (Canada) – it gathers information about identity theft and offers advice to victims[220]
  - Reporting Economic Crime Online (RECOL)
  - Canadian Consumer Information Gateway

CONCLUSION

Losing your personal information and identity to a stranger is indeed a harrowing experience. Technological advances that improve the flow of commercial activity by way of online commercial transactions, as well as the relative ease by which financial institutions distribute credit and other services, have produced some unintended consequences for consumers. These consequences involve the theft of personal identifying information of ordinary consumers from strangers who employ creative techniques to achieve personal gain at the expense of one's identity. At a minimum, there is a reasonable expectation by consumers who divulge their personal identifying information for commercial purposes that such information will not be used by others through illegal means.

When a stranger acquires possession and control of an innocent consumer's personal data, the identity thief can profit enormously at the consumer's expense. Thus, the stealing of personal information impacts the degree of financial independence and affects the sense of security among consumers in a marketplace continually being influenced by technological change. Simply put, consumers lose confidence in the

[219] Consumer Measures Committee, Consumer Identity Theft Checklist, *available at* http://cmcweb.ca/epic/internet/incmc-cmc.nsf/en/fe00088e.html (last visited Mar. 10, 2006).
[220] *Id.*

marketplace when they discover that their personal data is not protected, or that organizations are not doing enough to protect their personal data, whether for online commercial activity or conventional forms of buying and selling. Despite this sense of apprehension impacting the stream of commerce, consumers are increasingly becoming aware of the inadvertent means of exposing personal information to their detriment.

Generally, identity theft impacts the consumer in three ways: (1) creating money losses for consumers; (2) leaving consumers with poor credit rating; and (3) ruining the reputation of the consumer. Identity theft may also affect the flow of commercial activity among financial institutions, government, public sector organizations, and other organizations handling sensitive personal data. With the growing recognition for more practical public policy measures towards online commercial transactions, jurisdictions in the U.S. and Canada are making great advances. For example, consumer protection programs encourage consumers to utilize web-based initiatives such as online complaint forms, usually in association with federal and local authorities that use identity theft databases. As a means to prevent identity theft, both governments in the U.S. and Canada encourage consumers to use consumer kits, and provide the opportunity to correct, amend, or delete personal information that is inconsistent with past credit history.

Generally, the availability of these online complaint procedures triggers formal investigations of consumer credit, and may provide legal redress through damages and the correction of personal data. Thus, technological tools serve as a vehicle to protect consumers from unwanted invasion of their personal data. Other forms of consumer protection against identity theft include the recognition that organizations must handle personal data in a responsible manner. Many jurisdictions have enacted privacy legislation that imposes an affirmative duty on organizations to protect the personal data protection of clients, while informing consumers if their personal data is ever compromised. Several jurisdictions are reforming identity theft legislation as a response to calls for greater vigilance against the unlawful use of consumers' personal data.

Facilitating identity theft protections with a view to empower consumers in administering their rights is certainly practical in the context of public policy planning. However, while it may be possible to utilize the growing number of protective measures, a consumer must bear the responsibility of monitoring their own transactions with great care and attention. Even the strong interplay between technology and the law will not

always suffice to defend against identity theft. In many instances, technology tends to stay ahead of the law, and may contribute to alternative forms of identity theft not anticipated by existing legislation. Regardless, a healthy combination of legal remedies by way of legislation, online complaint procedures used by administrative agencies, and consumer education options will serve to increase vigilance and restore consumer confidence in the marketplace. Such measures, as adopted in both the United States and Canada, enhances protections that consumers have traditionally not had, and may prevent strangers from having unfettered access to sensitive personal information.