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

LEGISLATIVE APPROACHES TO IDENTITY THEFT:

AN OVERVIEW

March, 2007

CIPPIC Working Paper No. 3 (ID Theft Series)

www.cippic.ca

CIPPIC Identity Theft Working Paper Series

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

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

Suggested Citation:
CIPPIC (2007), "Legislative Approaches to Identity Theft", CIPPIC Working Paper No.3 (ID Theft Series), March 2007, Ottawa: Canadian Internet Policy and Public Interest Clinic.

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

CIPPIC

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

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

EXECUTIVE SUMMARY

This Working Paper examines the legislative framework relating to identity theft in Canada, the U.S., U.K., Australia and France, as of December 2006. It provides an overview of relevant legislation in the five jurisdictions, while the three supplementary papers listed below provide an annotated inventory of existing and proposed laws in each jurisdiction, along with statutory excerpts.

Working Paper No.3A: Canadian Legislation Relevant to Identity Theft: Annotated Review
Working Paper No.3B: United States Legislation Relevant to Identity Theft: Annotated Review
Working Paper No.3C: Australian, French, and U.K. Legislation Relevant to Identity Theft: Annotated Review

The legislation examined falls into four general categories: criminal law, privacy law, consumer law, and laws relating to issuing government identity documents. The U.S. federal government and California have statutes directly focused on identity theft, and these receive particular attention.

Our analysis reveals that the focus of most non-criminal legislation is the aftermath of identity theft, as opposed to its prevention. In Canada, numerous provisions in the *Criminal Code* outlaw the fraudulent use of personal information, but mere unauthorized possession of another's personal information is not an offence. No Canadian legislation focuses on identity theft *per se* and the term "identity theft" is nowhere defined in Canadian legislation.

With the possible exception of laws directed at real estate fraud, the U.S. legal framework pertaining to identity theft is far more developed than that of Canada, with a host of laws in the former directed specifically at the problem. Although Canadian privacy laws are more comprehensive than those in the U.S., Canada notably lacks a data security breach notification law. (See CIPPIC's White Paper, *Approaches to Security Breach Notification*). There are also gaps in Canadian consumer protection law, especially relating to credit bureau security freezes and to the authentication practices of credit bureaus and credit issuers.

NOTE RE TERMINOLOGY

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

TABLE OF CONTENTS

1. INTRODUCTION

One of the keys to combating identity theft is having effective legislation for its prevention, detection and mitigation. Statutory measures alone are not, of course, a complete solution: also important are enforcement, sound policies and effective public and private sector practices. Comprehensive education and awareness programs, effective reporting mechanisms and prudent choices on the part of individuals are also part of the solution. However, a strong legal framework can also provide a foundation for tackling the problems associated with identity theft.

During the last decade, Canada, the U.S. and other countries have passed legislation that directly and indirectly pertain to identity theft. The U.S. has been especially proactive on this front. With time, legislative activity will increase as governments react to the increasingly pervasive and sophisticated nature of identity theft and respond to growing public awareness and demands for action.

Statutory measures applicable to identity theft fall into two groups: 1) prevention measures, which aim to deter identity fraud; and 2) enforcement measures, aimed at detection, prosecution and conviction of identity thieves and mitigation of the impact on victims. Some statutes specifically target identity fraud, while others have different stated objectives but in effect do address various aspects of the problem. The latter include statutes prohibiting business practices that facilitate identity theft, those instituting procedures for issuing government identification documents, and legislation related to privacy and information collection and management.

This Working Paper analyses existing and proposed statutory measures in Canada, the U.S., the U.K., Australia and France, which aim to prevent or reduce the prevalence of identity theft and deal with its aftermath. Supplementary Working Papers 3A, 3B, and 3C provide an annotated inventory of applicable legislation in each country, including proposed legislation in Canada and the U.S. Excerpts from relevant statutes are provided in appendices to these papers. Legislation and caselaw relating specifically to the disclosure of security breaches are reviewed separately in the CIPPIC White Paper, "Approaches to Security Breach Notification".[1]

These papers fill a gap in the literature on identity theft, in that they contain the first comprehensive review of Canadian legislation that can be used against identity theft, and the first comparative review of various countries' identity theft statutes of which we are aware.

[1] Canadian Internet Policy and Public Interest Clinic ("CIPPIC"), Approaches to Security Breach Notification: A White Paper (9 January 2007), online: <www.cippic.ca>.

2. CANADA

2.1. Introduction

In Canada, statutory measures applicable to identity theft are primarily found in the *Criminal Code*, and in privacy and consumer protection legislation. Privacy and consumer protection statutes may be federal or provincial. Collectively, this legislation applies to a wide range of identity theft techniques.

Criminal Code measures target the fraudulent use of personal information, while privacy legislation limits one's ability to acquire personally identifiable information by regulating its collection and disclosure. Consumer statutes generally target the aftermath of identity theft rather than its prevention. For example, they limit liability for unauthorized charges to a credit account and regulate the tactics and behaviour of debt collectors. Identity document statutes pertain to government-issued documents, such as Social Insurance Number cards, passports, birth certificates and driver's licences.

It should be noted that, at the time of writing, there is no statutory definition of identity theft in Canada. The issue of terminology is discussed in the first Working Paper in this series: "Introduction and Background". 'Personal information' is defined in the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") and in certain provincial privacy statutes.[2]

2.2. Legislative Authority in Canada

In Canada, authority to enact legislation is divided between the Parliament of Canada and the provincial legislatures, as set out in the Constitution. The federal government's sphere of authority includes unemployment insurance, banks, and criminal and privacy matters. The provincial sphere includes consumer reporting agencies, consumer protection, collection agencies, highway and transportation, personal health, vital statistics and privacy. Some provinces' private sector privacy legislation is substantially similar to and overrides federal privacy laws; this is the case in British Columbia, Quebec and Alberta.

3. ANALYSIS OF CANADIAN STATUTES

A variety of Canadian statutes relate to prevention, detection and mitigation of identity theft. In this section, we examine general trends and omissions.

3.1. Criminal Code

The *Criminal Code* does not contain a specific identity theft offence. However, it does criminalize fraud (s.380), forgery (s.366), uttering a forged document (s.368), theft, forgery

[2] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5

etc. of a credit/debit card (s. 342), unauthorized use of a computer (s. 342.1), personation (s.403), forgery of or uttering a forged passport (s. 57), theft (s. 322), possession of property obtained by crime (s. 354) and conspiracy to commit an indictable offence (s. 465(1)(c). If done with intent to defraud, the Code also criminalizes the making, executing, drawing, signing, accepting or endorsing of a document in the name or on the account of another person (s. 374).

These provisions cover most fraudulent *uses* of personal information by identity thieves, but they do not address the unauthorized *acquisition and possession* of personal information by thieves. Other than in limited circumstances, the collection and possession of personal information, the starting point for identity theft, is not criminalized. This is not surprising, as identity theft was not the issue it is today when the Code was last amended.

In its 2004 and 2006 consultation papers the Department of Justice identified and requested comment on a number of perceived gaps in the *Criminal Code* with respect to identity theft.[3] Some of these are discussed below.

3.1.1. Fraud, Forgery, Impersonation

The fraud and forgery provisions in the Code are widely used to charge and convict identity thieves, who often use these techniques. The focus of criminal prohibitions on fraud is on the consequences for the organization that is defrauded, however, and not on the damages incurred by individual victims. For example, Section 342, concerning theft and forgery of credit cards, criminalizes the thief's abuse of the credit card system rather than the abuse of the victim's identity *per se*.

The "personation" offence found at s. 403 of the *Criminal Code* makes the fraudulent impersonation of any person, living or dead, for one of three specified intents, an offence. The intents include intent to cause disadvantage, to gain advantage or to obtain property. In the 2005 case of *R. v. Boyle*, the court held that the words "gain an advantage" could scarcely be more broad in scope.[4] In this case, "gain[ing] an advantage" included obtaining a new driver's licence in another individual's name in order to hide one's past. The court found it irrelevant that the thief did not steal money or gain any other advantage: the intent to gain an advantage was enough to trigger Section 403.

However, s.403 does not currently cover impersonation of a fictitious person. It is possible that other offences, such as uttering a forged document, would capture this.[5]

[3] Department of Justice, *Consultation Document on Identity Theft* (October 2004) and *Identity Theft: Consultations on Proposals to Amend the Criminal Code* (June 2006).Not publicly available.
[4] *R v. Boyle*, [2005] B.C.J. No. 2501 (B.C.C.A.) (Q.L.) 2005 B.C.C.A. 537.
[5] *Department of Justice (2004), supra* note 3 at 19.

3.1.2. Possession of personal information

Under the *Criminal Code*, mere possession of personal information is not an offence. This is consistent with *Charter* jurisprudence and the general requirement for *mens rea* in criminal offences. The *Code* does contain two provisions that prohibit the *fraudulent* possession of two types of personal information: computer passwords (s.342.1(1)(d)), and credit card data (s.342(3)). Even in these cases, mere possession is insufficient; some kind of fraud or lack of justification for that possession must be made out. In all other cases, until the personal information misappropriated by thieves is used to commit another offence, no crime has been committed.

Several organizations, including the Canadian Bankers Association, have criticized this gap in the legislation.[6] The Department of Justice, in its consultation papers on identity theft, identified the possibility of creating an offence of possessing (and trafficking in) personally identifiable information with intent to commit fraud, possibly with a reverse onus on defendants to prove the legitimacy of their information possession.[7]

3.1.3. Computer misuse

Technology - particularly computers and the internet - is routinely used to perpetrate identity crimes. The computer misuse provisions of the *Criminal Code* are generally considered effective in this regard.[8] The main deficiency of such provisions, in the context of identity theft, is that they do not apply when users are tricked into giving away their personal information via phishing schemes or through other online social engineering tactics.

3.1.4. Sentencing

Another perceived gap in the *Criminal Code* is the lack of sentencing guidelines for identity theft crimes. The sentences for debit card fraud, for example, range from a fine to a few months in jail. Harsher sentences might deter potential perpetrators. This issue is discussed further in Working Paper No.5 on Enforcement of Identity Theft Laws.

3.1.5. Fraudulent declaration to government agencies

Many statutes, such as the Ontario *Vital Statistics Act* and *Mortgage Brokers Act*, establish offences for providing false information to government agencies.[9] Surprisingly, the *Vital Statistics Act* of British Columbia does not make it an offence to provide false information.[10]

---

[6] Canadian Bankers Association, *Identity Theft: A prevention policy is needed*, 2e ed. (January 2005) at 4, online: <http://www.cba.ca/en/content/reports/Identity%20Theft%20-%20A%20Prevention%20Policy%20is%20Needed%20ENG.pdf>.

[7] *Department of Justice*, *supra* note 3.

[8] Michael W. Kim, "How countries handle computer crime" MIT 6.805/STS085: Ethics and Law on the Electronic Frontier (Fall 1997), <http://www.swiss.ai.mit.edu/6.805/student-papers/fall97-papers/kim-crime.html>.

[9] *Vital Statistics Act*, R.S.O. 1990, c. V.4 and *Mortgage Brokers Act*, R.S.O. 1990, c. M.39.

[10] *Vital Statistics Act*, R.S.B.C., 1996, c. 479.

Sanctions can only be imposed if the fraudster refuses to return the fraudulently obtained certificate.

3.2. Privacy: Data Protection

Canada has two categories of data protection statutes: public sector and private sector. The latter are more recent and, in some respects, are more stringent than the former. Most privacy statutes in Canada require organizations to take precautions to prevent unauthorized access to personal data under their control. "Personal information" is generally defined as "any [recorded] information about an identifiable individual".

3.2.1. Collection, Retention, Use and Disclosure of Personal Information

All Canadian privacy statutes limit the collection, use and disclosure of personal information by private organizations and/or public bodies. Collection, use and disclosure must be for "reasonable purposes" and with consent of the individual, unless specific exceptions apply. Under private sector statutes, collection of personal information must be limited to that which is necessary for the purposes identified by the organization, and personal information must be retained only as long as is necessary for the fulfilment of those purposes.

These restrictions could potentially reduce the risk of identity theft. However, research has demonstrated that many businesses fail to comply with basic requirements under the law.[11] For example, some organizations do not limit their collection of personal information to what is necessary for the immediate transaction, and many organizations retain personal information longer than necessary. The result is that more personal information is vulnerable to identity theft should thieves obtain access to it, as they did in the January 2007 case of Winners/TJX.[12]

3.2.2. Security measures

Most data protection legislation includes a duty to take "reasonable security measures" to protect personal information from theft, loss and unauthorized access, use, collection, disclosure, copying, modification or disposal. The *Ontario Personal Health Information Protection Act* and *Vital Statistics Act* contain a similar provision: the latter requires that information be kept in a "safe place".[13] A notable exception is the decades-old federal *Privacy Act*, which has not been updated to deal with the challenges of new technologies.[14]

---

[11] Canadian Internet Policy and Public Interest Clinic (CIPPIC), *Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up?* (April 2006) at 3, online: <http://www.cippic.ca/en/news/documents/May1-06/PIPEDAComplianceReport.pdf>.

[12] See news reports on the Winners/TJX case, such as <http://www.theregister.co.uk/2007/03/29/tjx_credit-card_debacle/>. See also Philippa Lawson and John Lawford, *Identity Theft: The Need for Better Consumer Protection (* Public Interest Advocacy Centre, November 2003) at 30, online: <http://www.piac.ca/files/idtheft.pdf>. For CIPPIC complaint re: Winners/TJX, see http://www.cippic.ca/en/projects-cases/privacy/pipeda-complaints/.

[13] *Personal Health Information Protection Act*, S.O. 2004, c. 3, Sch. A and *Vital Statistics Act*, *supra* note 9.

[14] *Privacy Act*, R.S. 1985, c. P-21.

Under PIPEDA, security safeguards must be "appropriate to the sensitivity of the information".[15] According to the British Columbia Information and Privacy Commissioner, for security measures to be reasonable they must be objectively diligent and prudent in all of the circumstances.[16] When evaluating the reasonableness of security measures, one must consider factors such as sensitivity of the personal information, documenting security measures, use of encryption and cost.

3.2.3. Access Controls

Security measures may be considered unreasonable if information is not protected by access controls based on the "need-to-know" principle. If employees have access to information, the potential for insider abuse is greater. Only two statutes impose a duty to implement access controls on a "need to know" basis. The first is the Ontario *Freedom of Information and Protection of Privacy Act* regulations: "[e]very head shall ensure that only those individuals who need a record for the performance of their duties shall have access to it".[17]

The second is the Quebec statute, *An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information*.[18] The wording of the provision differs significantly from the Ontario statute: "[e]very person qualified to receive nominative information within a public body has access to nominative information without the consent of the person concerned where such information is necessary for the discharge of his duties." If nominative information is not required to carry out duties, the person must get the consent of the person whose information is being sought.

PIPEDA makes reference to the need-to-know principle.[19] This is done as an example of an organizational protection measure under its requirement for security safeguards in Principle 7 of Schedule 1.

Mandating that access be limited to a need-to-know basis offers many advantages to the prevention of identity theft. First, it makes it difficult for an insider to provide information in response to a request from the outside. In order to access the information requested, the information must relate to an employee's duties. A second benefit is that it makes it harder to assemble large lists which can be sold. Although a list of information to which the employee legitimately has access could be produced, the employee could more easily be tied to that list. This increases his or her chances of getting caught and thus serves as a deterrent to insider abuse.

---

[15] *Personal Information Protection and Electronic Documents Act*, *supra* note 2.

[16] Office of the Information and Privacy Commissioner for British Columbia, *Investigation Report F06-01* (31 March 2006) at 14, online: http://www.oipcbc.org/orders/investigation_reports/InvestigationReportF06-01.pdf.

[17] *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, Reg. 460.

[18] *An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information, R.S.Q., c. A-2.1.*

[19] *Personal Information Protection and Electronic Documents Act*, *supra* note 2.

3.2.4. Notification of Security Breaches

Privacy laws seek to protect personal information by requiring organizations and public bodies to take reasonable security measures. However, security measures cannot be perfect and security breaches will inevitably occur.

As noted in the CIPPIC White Paper on Approaches to Security Breach Notification, the only Canadian statute that imposes a duty to warn affected individuals in case of unauthorized access is the *Ontario Personal Health Information Protection Act*.[20] Section 12 of this statute imposes a duty to notify the owner of personal health information at the first reasonable opportunity if the information is stolen, lost, or accessed by unauthorized persons. Otherwise, in Canadian law there is no duty to notify affected individuals of a security breach, nor is there a duty to take reasonable steps to recover the breached information and to prevent further dissemination.

A provision similar to that in the Ontario statute has been proposed in two private member's bills, which are discussed in Working Paper 3A. While they are unlikely to pass, the bills represent the beginning of an interest on the part of legislators in an important aspect of identity theft. In Ontario, Bill 174, the *Consumer Reporting Amendment Act*, would impose a duty on consumer reporting agencies, on discovering that any of a consumer's information has been unlawfully disclosed, to immediately inform the consumer of the disclosure.[21] In Manitoba, Bill 207, the *Personal Information Protection and Identity Theft Protection Act*, would impose a duty to notify the individual of any unauthorized access.[22] In addition, it would create two new causes of action for failure to notify an individual of the unauthorized access and for failure to protect personal information.

The Information and Privacy Commissioner of Ontario's security breach guidelines are worth noting, although they are not legally binding.[23] They suggest that individuals affected by a breach be notified. According to the guidelines, the two priorities following a breach are containment and notification. The notice should provide details of the extent of the breach and the specifics of the disclosed personal information. It should also provide details about the steps that have been taken to contain and address the breach, immediately and in the long term.[24]

3.2.5. Storage location

Most privacy statutes do not require organizations to store personal information within Canada (and to thus protect the information from unauthorized access by foreign states such

---

[20] *Personal Health Information Protection Act*, *supra* note 13.
[21] Bill 38 -*Consumer Reporting Amendment Act*, online: http://www.ontla.on.ca/web/bills/bills_detail.do?locale=en&BillID=438.
[22] Bill 200 – *The Personal Information Protection and Identity Theft Prevention Act*, online: http://web2.gov.mb.ca/bills/sess/b200e.php.
[23] Information and Privacy Commissioner of Ontario, *What to do if a privacy breach occurs: Guidelines for government organizations* (May 2003) at 2, online: <http://www.ipc.on.ca/docs/prbreach.pdf>.
[24] *Ibid*.

as under the USA PATRIOT Act).[25] Such a provision was adopted by the Nova Scotia legislature, however, in the *Personal Information International Disclosure Protection Act*..[26]

3.2.6. Enforcement

Governmental organizations do not always respect privacy statutes, as evidenced by the investigation of the British Columbia Information and Privacy Commissioner into the sale of backup tapes. The Commissioner found that:

> "There can be little debate about the inadequacy of existing provincial government policies and procedures respecting the secure destruction of personal information… Many provincial government ministries have not created procedures for the destruction of removable storage media, despite their obligation to do so according to central government policy."[27]

3.3. Consumer Reporting Agencies

There are numerous provincial statutes aimed at protecting the consumer from various marketplace abuses, including those involving identity fraud. By placing restrictions and imposing duties on credit agencies with respect to credit reports and the granting of credit, some of these statutes serve to protect consumers' personal information from abuse by identity thieves. However, such statutes are by no means free of deficiencies.

3.3.1. Consent clauses

Special signed clauses are frequently used by merchants to obtain consumer consent to the collection from and disclosure to credit bureaus of their personal information. Such clauses may inform consumers but do not give them any power to limit the disclosure of their information, other than on a "take it or leave it" basis; credit grantors can refuse to extend credit unless consumers consent to the disclosure.[28] This puts into question the meaningfulness of the clauses.

3.3.2. Fraud Alerts

None of the statutes that apply to consumer reporting agencies, with the exception of the new Ontario *Consumer Protection and Service Modernization Act*, impose a duty to offer fraud alerts to consumers who have been victimized by identity fraud.[29] Currently, Canadian consumer reporting agencies offer fraud alerts on a voluntary basis. However, they make no

[25] *The Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism Act of 2001*, H.R. 3162, online: <http://www.epic.org/privacy/terrorism/hr3162.html>.
[26] Bill 16, *Personal Information International Disclosure Protection Act*, S.N.S. 2006, c. 3.
[27] *Office of the Information and Privacy Commissioner for British Columbia*, *supra* note 16 at 14.
[28] *Philippa Lawson and John Lawford*, *supra* note 12 at 32.
[29] C*onsumer Protection and Service Modernization Act, 2006*, (rec. Royal Assent December 20, 2006), online: <http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/90c33_e.htm>,

guarantees that the fraud alert will be brought to the attention of credit grantors nor do they make any other guarantees as to the form, contents or legibility of the alert.

Since fraud alerts are only mandated by one province, creditors in other provinces may not be obliged to acknowledge them or to take appropriate precautions when a credit report contains one.[30]

3.3.3. Consumer Explanations

Some statutes impose a duty on credit reporting agencies to provide, in credit reports, any explanation or additional information about the information contained in the credit report. However, credit grantors are not obliged to take these explanations into account when granting credit. Without such a requirement, credit grantors are at liberty to deny credit to identity theft victims, thus, in effect, punishing victims.

3.3.4. Authentication

A major concern for identity theft is the lack of legal standards for authenticating the identity of a person requesting a credit report. As demonstrated by the ChoicePoint breach, failure to properly authenticate customers can be a major source of identity theft.[31]

Furthermore, credit grantors are not required to ensure that all personal information in a credit application matches the information in the credit report before extending credit.[32] Nor are they required to take any steps to make sure that the information provided on the credit form relates to the person filling in the form. This legislative gap facilitates identity theft.

3.3.5. Notification

Creditors do not have to notify consumers when credit is granted in their name. Currently, creditors are only required to notify consumers that they will review credit reports, which notification usually takes the form of a general consent clause signed by the consumer at the initiation of the contract.[33] This notification is of no use in cases of identity theft, since the notice is given to the imposter applying for credit, and not to the consumer.

3.3.6. Right of Action

Consumer statutes do not offer individuals a private right of action against consumer reporting agencies that fail to comply with legislation. Ontario caselaw, however, suggests that such a right exists at common law. In the 2003 case of *Haskett v. Equifax Canada Inc.*, the court held that consumer reporting agencies, and creditors that report information on credit transactions to these agencies, owe a duty of care to the individuals about whom credit files are kept and about whom information is reported.[34]

---

[30] *Ibid.*
[31] *Office of the Information and Privacy Commissioner for British Columbia, supra* note 16 at 8.
[32] *Philippa Lawson and John Lawford, supra* note 12 at 32
[33] *Ibid.*
[34] *Haskett v. Equifax Canada Inc.* (2003) 63 O.R. (3d) 577 (C.A.).

One of the major problems with actions in negligence is proving damages. When an individual's credit file contains errors, the usual consequences are being denied credit, having to spend time to remedy the situation and general annoyance. These can be hard to quantify as damages. Other damages can even be hidden; for example if the credit rating is adversely affected, a consumer might get a loan but only at higher interest rates.

In the 2004 case of *Clark v. Scotiabank*, however, Clark was awarded $5,000 against each defendant for the foreseeable mental distress that they caused him by not remedying an error in Clark's credit file that was repeatedly brought to their attention.[35]

3.4. Consumer Protection & Debt Collectors

With the exception of Ontario legislation relating to mortgage fraud, Canadian statutes pertaining to consumer protection and debt collection agencies do not offer any protection against identity theft *per se*: their provisions target only the consequences of identity theft.

3.4.1. Credit Card Issuance

Easy access to credit cards, through practices such as mass mailing of applications and lack of authentication procedures, facilitates identity theft. This issue is discussed further in the Working Paper on Techniques of Identity Theft.

Manitoba's consumer protection legislation, however, offers notable protection to consumers through two unique provisions.[36] The first places the onus on the credit card issuer to prove that the individual requested a card. Consumers whose identity has been stolen can invoke this provision to avoid financial liability. The second places the onus of proof on the card issuer when a dispute arises in relation to unauthorized charges.

In contrast, Quebec's consumer protection legislation has a provision that could actually make it easier for identity thieves to obtain credit cards in the name of their victim. Section 29 of the *Consumer Protection Act* creates an exception to the rule that contracts for loans must be in writing and signed by both parties on all pages.[37] For credit card contracts to take effect, it is sufficient for the card to be issued and for it to be used.

3.4.2. Liability

Most consumer protection statutes contain provisions limiting the financial liability of identity theft victims for unauthorized credit card transactions. Usually, such liability is capped at $50. Moreover, both VISA and Mastercard currently offer "zero liability" policies, shifting the burden of fraud losses to their broader consumer base (and in particular, to those customers incurring interest). However, financial losses are not the only problem faced by

[35] *Clark v. Scotiabank*, [2004] O.J. No. 2615 (Ont. Sup. Ct. (Civ. Div.)) (Q.L.).
[36] *The Consumer Protection Act*, C.C. S.M., c. C200
[37] *Consumer Protection Act*, R.S.Q., c. P-40.

victims. Re-establishing credit ratings and financial reputations are perhaps the most serious problems faced by victims of identity fraud.

3.4.3. Debt Collector Harassment

Most provinces prohibit debt collectors from adopting overzealous behaviours when collecting debts. Some statutes refer explicitly to debt collectors. They offer protection against aggressive debt collectors, who are often a significant factor in the pain and suffering of victims.[38] They generally require debt collectors to take reasonable steps to ensure that the person is in fact the debtor, and prohibit repeatedly calling debtors at work or at home. In order to invoke certain provisions, however, the consumer will need an affidavit or police report.[39]

3.4.4. Right of action

Consumer protection statutes do not provide individuals with a private right of action against collection agencies, but they may commence actions in negligence. However, as seen in *Anderson v. Excel Collection Services Ltd.*, in order to obtain an award of damages for mental distress, one must prove that the collection agency's behaviour resulted in psychiatric illness.[40]

3.5. Statutes applicable to identity documents

The federal and provincial governments provide a number of key documents to citizens. These include Social Insurance Number ("SIN") cards, passports and non-resident cards at the federal level and provincially, drivers' licenses, health cards and birth certificates. Stolen identity documents, also known as "foundation documents", are an important tool for identity thieves. With only one original, skilled thieves can make copies and can go on to obtain other identity documents. Using them can open the door to accounts containing personal and financial information, and enable thieves to obtain credit, purchase goods and services and otherwise conduct business in the name of another person.

Improper and lax procedures for issuing these documents can leave individuals vulnerable to identity theft. Some of these documents can also be readily altered or forged, often by using readily available photocopying and other tools.

[38] U.S. Department of Justice, *Identity Theft: Problem-Oriented Guides for Police Problem-Specific Guides Series*, No. 25 (June 2004) at 4, online: <http://www.cops.usdoj.gov/mime/open.pdf?Item=1271>.
[39] *Philippa Lawson and John Lawford*, *supra* note 12 at 47.
[40] *Anderson v. Excel Collection Services Ltd.* (2006) 260 D.L.R. (4th) 367 (Ont. Sup. Ct.).

3.5.1. Social Insurance Numbers

In 2002, the Auditor General of Canada noted many problems with the issuance of Social Insurance Numbers ("SINs").[41] These flaws can have serious consequences for identity theft. Fraudulent use of someone's SIN is often part of an identity theft crime and facilitates the perpetration of these crimes.[42] For example, it is possible to use photocopies of identification documents when applying for a SIN.[43] The validity of the document is verified but no one checks whether the bearer is the rightful owner of the document.[44]

3.5.2. Driver's licences

Depending on the province, driver's licenses may be readily forged or altered. The possession of a falsified licence is an offence, for example, under the Ontario *Highway Traffic Act.*[45] However, the possession of another person's driver's licence is not an offence. Thus, thieves found in possession of drivers licence numbers belonging to others, for the purpose of creating falsified licences, could not be charged as such.

3.5.3. Birth certificates

Most vital statistics statutes criminalize making false statements in any notice, registration, statement, certificate, return or other document. They also usually contain provisions imposing a duty to return found identity documents and to report the loss or theft of identity documents issued under these statutes.

3.6. Real Estate Fraud

One of the newer types of identity theft involves real estate fraud. This form of identity theft has become a growing concern to homeowners and to the real estate and financial sectors. Unsuspecting homeowners can lose their home as a result of a falsified mortgage, fraudulent sale or counterfeit power of attorney. The identity thief impersonates the registered owner of the real property or the director, officer or shareholder of the corporation that owns the property. The thief then fraudulently transfers ownership of the property from the rightful owner to themselves. The property, generally a principal residence, is then mortgaged or sold by the thief, who absconds with the funds. The value of the property may be artificially increased in the interim through a series of sales and resales. This problem is discussed in the Working Paper entitled Techniques of Identity Theft.

---

[41] Office of the Auditor General of Canada, *Report of the Auditor General of Canada - 2002 Status Report*, c. 1 Human Resources (8 October 2002), at 11, online: <http://www.oag-bvg.gc.ca/domino/reports.nsf/html/20020901ce.html/$file/20020901ce.pdf>.

[42] *Ibid*. at 10.

[43] *Ibid*. at 16.

[44] *Ibid*. at 12.

[45] Section 35 (1) (a) of the Ontario *Highway Traffic Act*, R.S.O. 1990, c. H8 states that "No person shall display or cause or permit to be displayed or have in his or her possession a fictitious, imitation, altered or fraudulently obtained driver's licence".

Ontario has led the way in passing legislation to protect and compensate property owners who are victims of real estate fraud.[46] This is a positive step, though similar protections seem not to be available to those who unknowingly purchase, and then lose, a property acquired by fraudulent means.

4. UNITED STATES

4.1. Introduction

In contrast to Canada, many U.S. jurisdictions have passed legislation specifically aimed at preventing identity theft, assisting its victims, improving prosecution and conviction rates, and otherwise addressing its consequences. Both federal and state identity theft statutes exist and most were passed in recent years. With many bills awaiting approval, additional U.S. legislation in this area can be expected.

In addition to specific identity theft legislation, the U.S. has federal statutes dealing with false identification, data protection, and credit, as well as "general" statutes applicable to identity theft. At the state level, Arizona was the first state to pass legislation recognizing identity theft as an independent crime.[47] All 50 states have now enacted legislation making identity theft a misdemeanour or a felony offence. State legislation is especially important because most prosecutions take place at the state level. Anecdotal evidence suggests that state laws have been effective in increasing awareness of identity theft if not deterring the crime.[48]

Our inventory of state legislation focuses on California, whose various codes contain a number of identity theft provisions. This state is a leader in legislating to combat identity theft and to assist victims of identity theft. While statutes do vary by state, those of California have provided a model framework for much of the other state legislation and are generally representative of the U.S. approach.[49]

---

[46] *Consumer Protection and Service Modernization Act, 2006, supra* note 29.

[47] Graeme R. Newman & Megan M. McNally, *Identity Theft Literature Review*, report to the U.S. Department of Justice (July 2005) at 63, online: National Criminal Justice Reference Service <http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf >. Ariz. Rev. Stat. § 13-2008 defines "identity theft" as follows: "A person commits taking the identity of another person or entity if the person knowingly takes, purchases, manufactures, records, possesses or uses any personal identifying information or entity identifying information of another person or entity, including a real or fictitious person or entity, without the consent of that other person or entity, with the intent to obtain or use the other person's or entity's identity for any unlawful purpose or to cause loss to a person or entity whether or not the person or entity actually suffers any economic loss as a result of the offense", online: <http://www.azleg.stste.az.us/ars/13/02008.htm>.

[48] *Graeme R. Newman & Megan M. McNally, supra* note 47 at 65.

[49] *Graeme R. Newman & Megan M. McNally, supra* note 47at 64. The British Columbia Freedom of Information and Privacy Association (BCFIPA) study provides a useful, selective inventory of U.S. state laws. See British Columbia Freedom of Information and Privacy Association (BCFIPA), *PIPEDA and Identity Theft: Solutions for Protecting Canadians* (30 April 2005) at 25, online: <www.fipa.bc.ca>.

It is important to note that U.S. federal provisions sometimes pre-empt states from enacting legislation that is contrary to or stronger than federal legislation. The federal government, for example, established a permanent pre-emption for credit law legislation. The main goal of pre-emption is to create a standard set of requirements and obligations applicable to all states. As a result, on issues addressed by federal legislation, pre-emption may limit what individual states can do to combat identity theft and some state statutes may be weakened.[50] This happened with the federal *Fair and Accurate Credit Transactions Act* ("FACTA"), This statute, which requires that one free credit report per year be provided, pre-empts Californian legislation requiring credit bureaus to provide identity theft victims with one free credit report per month while they are correcting their records.[51]

4.2. Federal statutes

This section explores U.S. federal identity theft statutes as well as some bills addressing identity theft. Underlying the analysis is consideration of how the U.S. experience can prove useful to Canada.

4.2.1. Identity theft-specific legislation

As noted, U.S. legislation at both federal and state levels makes identity theft a criminal offence. The federal *Identity Theft and Assumption Deterrence Act of 1998* is a landmark in the evolution of U.S. identity theft legislation.[52] It was the first statute to define identity theft, as an act involving one who "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".[53] Because the definition is broad, the statute makes it easier to prosecute identity thieves.[54]

This statute also defines personal information (referred to as "means of identification") broadly, to include government-issued identifiers, such as Social Security and passport numbers, biometric information, and telecommunication and electronic identifiers.

4.2.1.1. Possession of personal information

In contrast to Canada, U.S. legislation criminalizes the possession of personal information under certain circumstances. At the federal level, the *Identity Theft and Assumption Deterrence Act of 1998* criminalizes the possession of a means of identification of another

[50] Gail Hillebrand, "After the FACT Act: What States Can Still Do to Prevent Identity Thef t" Consumers Union, online: <http://www.consumersunion.org/pdf/FACT-0104.pdf>.
[51] *Fair and Accurate Credit Transactions Act* (FACTA), U.S.C. § 1681: online <http://www.ftc.gov/os/statutes/031224fcra.pdf>.
[52] *Identity Theft and Assumption Deterrence Act*, 18 U.S.C § 1028: online <http://www.ftc.gov/os/statutes/itada/itadact.htm>.
[53] See http://www.ftc.gov/os/statutes/itada/itadact.htm.
[54] Federal Trade Commission, *Cybersecurity and Consumer Data: What's at Risk for the Consumer?*, (19 November 2003) at ix, online: <http://www.ftc.gov/os/2003/11/031119swindletest.htm>.

person, with intent to use the personal information in an unlawful manner.[55] Thus, unlike in Canada, the possession of personal information may be criminal even if no further offence is committed.

As well, U.S. legislation criminalizes the act of fraudulently acquiring another's personal information from a financial institution, and the act of asking someone else to fraudulently acquire the information.[56] Furthermore, wilfully acquiring personal information from a consumer reporting agency under false pretences is criminalized.[57]

4.2.1.2. Insider Abuse

U.S. legislation addresses the risk posed by insider abuse by requiring a review of sentencing guidelines for individuals who abuse their position to obtain personal information unlawfully.[58] In addition, credit laws prohibit employees or agents of consumer reporting agencies from providing information about a consumer to a person not authorized to receive it.[59]

4.2.1.3. Unlawful uses

The various unlawful uses of identity information are covered by pre-existing criminal offences in the U.S. In addition, the *Health Insurance Portability and Accountability Act of 1996* ("HIPAA") criminalizes using personal information to defraud health care benefit programs of money, property, health care benefits, items or services.[60]

4.2.1.4. Risk reduction

U.S. federal legislation contains provisions that seek to reduce the risk of identity theft by protecting personal information.[61] These include requirements that credit card information be truncated on receipts, that consumer reporting agencies notify credit grantors of discrepancies in addresses and that consumer reporting agencies make reasonable efforts to verify the identity of credit report users. They also include requirements pertaining to the disposal of records compiled from credit reports.

In order to mitigate the damage of identity fraud, some U.S. statutes, such as the *Fair and Accurate Credit Transactions Act* ("FACTA"), require credit bureaus to issue fraud alerts in certain circumstances.[62] This statute provides for both standard fraud alerts and extended

---

[55] *Identity Theft and Assumption Deterrence Act, supra* note 52.
[56] *Gramm-Leach-Bliley Act*, 12 U.S.C § 1811: online <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ102.106.pdf>.
[57] *Fair and Accurate Credit Transactions Act, supra* note 51.
[58] *Identity Theft Penalty Enhancement Act*, 18 U.S.C § 1001,online: <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ275.108.pdf>.
[59] *Fair and Accurate Credit Transactions Act, supra* note 51.
[60] *Health Insurance Portability and Accountability Act of 1996* (HIPAA), 42 U.S.C § 201, online: U.S. Government Printing Office Home Page <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid= f:publ191.104.pdf>.
[61] *Fair and Accurate Credit Transactions Act, supra* note 51.
[62] *Ibid.*

fraud alerts. A standard fraud alert must be issued if the consumer asserts a good faith suspicion that identity theft has occurred. However, it remains on file for only 90 days. Extended fraud alerts, on the other hand, can remain active for up to seven years. However, they are available only where the consumer provides an identity theft police report to the consumer reporting agency.

Another problem with the standard fraud alert is that it does not require a potential credit grantor to respect a pre-established procedure to confirm that the transaction is properly authorized. Consumers can provide a telephone number so that they may be contacted for authorization, but credit grantors are not obligated to use this procedure. The current provisions only mandate that credit grantors use a reasonable procedure to form a reasonable belief that the person making the request is in fact the individual. Under extended fraud alerts, however, credit grantors must contact the consumer personally for authorization in each case of a credit request. Moreover, there are restrictions on how the consumer reporting agency can use the consumer's file. For example, for five years the consumer's information cannot be included in lists used to send pre-approved credit offers.

The requirements for fraud alerts apply only to credit transactions, such as granting new credit and issuing a new card, and not to credit checks involving employment, utilities, and insurance and property rentals. When a credit report is requested for these uses, the user is not obligated to contact the individual or use a reasonable procedure to form a reasonable belief that the person making the request is in fact the individual.

Notably, U.S. consumers repeatedly report that credit grantors have failed to honour fraud alerts on their credit files.[63]

4.2.1.5. Aftermath

U.S. statutes are not just concerned with prosecuting and convicting criminals. They also contain provisions which aim to help the victims of identity theft deal with aftermath of the crime. For example, the *Fair and Accurate Credit Transactions Act* ("FACTA") requires consumer reporting agencies to notify other consumer reporting agencies when they receive a request to place a fraud alert on a consumer file.[64] Another provision prohibits consumer reporting agencies from including transactions that result from identity theft in credit reports and prohibits businesses from re-transmitting this information to consumer reporting agencies after they have been notified. This provision allows victims to re-establish their credit history. However, no identity theft-specific provisions address other consequences of identity theft, such as fake bankruptcies or criminal records.

U.S. federal statutes requiring businesses to provide victims and police with information about identity theft transactions are potentially useful in two ways. They provide information on how the victim's identity was compromised and can speed up investigations

[63] Bob Sullivan, *Your Evil Twin: Behind the Identity Theft Epidemic* (Hoboken, New Jersey: John Wiley & Sons, 2004) at 84.
[64] *Fair and Accurate Credit Transactions Act, supra* note 51

by law enforcement agencies. However, consumers have no right of action if businesses fail to provide the information.[65]

4.2.1.6. Sentencing

Sentencing is discussed in the CIPPIC Working Paper on No. 5 on Enforcement of Identity Theft Laws. When handing down a sentence for identity theft under Section 1028 of the U.S. Code, the following factors must be taken into account: the number of victims; the number of means of identification and, the type of identification documents involved in the offence.[66]

In practice, sentences for identity theft have tended to be low compared with other economic crimes. This, along with the potentially high rewards and relatively low risk of being caught, has helped to make identity theft a crime of choice. Harsher sentences have been introduced for aggravated identity theft, which occurs when the personal information of another person is possessed, used or transferred, without lawful authority, while another felony is being committed.[67] A sentence for aggravated identity theft must be consecutive to that for the other offence.

4.2.2. False Identification Statutes

Under U.S. law it is a criminal offence to create, transfer or use stolen or counterfeited identification documents.[68] However, mere possession is criminal only if an individual has five or more such documents, the individual has the intention of defrauding the United States, or the individual knows that the document is stolen or was produced without lawful authority and that the document is from the United States.

The production, use and trafficking of counterfeited "access devices" (i.e. credit, debit and calling cards and account numbers) is also criminalized. “Access devices” is defined broadly and includes identification documents used by private businesses such as gym or video stores. The *Internet False Identification Act of 2000* closed a loophole that allowed counterfeiters to legally sell counterfeit social security cards by maintaining the fiction that such cards were “novelties” rather than counterfeit documents.[69] However, the possession, transfer and use of “novelty” counterfeited documents are not criminal if the documents do

---

[65] Electronic Privacy Information Center (EPIC), “The Fair Credit Reporting Act (FCRA) and the Privacy of Your Credit Report” (7 October 2005), online: <http://www.epic.org/privacy/fcra>.

[66] Michael J. Elston & Scott A. Stein, “International Cooperation in On-Line Identity Theft Investigations: A Hopeful Future but a Frustrating Present”, online: <http://www.isrcl.org/Papers/Elston%20and%20Stein.pdf>.

[67] *Identity Theft Penalty Enhancement Act*, 18 U.S.C § 1001: online <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ275.108.pdf>.

[68] *Fraud and related activity in connection with identification documents Act*, 18 U.S.C. § 1028: online http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001028----000-.html and *Internet False Identification Act of 2000*, 18 U.S.C § 1021: online <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ578.106.pdf>..

[69] *Internet False Identification Act of 2000*, *supra* note 68. See *also* Federal Deposit Insurance Corporation Division of Supervision and Consumer Protection, *Putting an End to Account-Hijacking Identity Theft* (14 December 2004), online: <http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf>.

not appear to be issued by the government. Such acts are criminal only if the identification document falls under the definition of an "access device".

4.2.3. Privacy and Personal Data Statutes

4.2.3.1. Collection, use and disclosure

In response to information abuses, a patchwork of data protection laws has emerged in the U.S., providing spotty protection to individuals in various specific situations. State departments of motor vehicles, for example, may not disclose personal information and "highly restricted personal information" (individual's photograph or image, Social Security Number, medical or disability information) other than in certain predefined situations.

Under U.S. federal law, financial institutions may only disclose personal information if they have notified the consumer and have provided the option to opt-out of disclosure. The reliance on opt-out mechanisms puts the burden on consumers to know their rights and request that their information not be shared. Another problem with the *Gramm-Leach-Bliley Act* is that consumers have no right to stop their information from being shared with affiliates.[70] Financial institutions can also avoid opt-outs by offering co-branded services which require the sharing of information with non-affiliated organizations. These services fall under the provider/joint marketing exemption. Furthermore, the legislation does not require the privacy policies of financial institutions to provide details of how information is shared.[71] Finally, consumers have no private right of action against financial institutions.

In contrast to Canada, there are only a few provisions in U.S. laws limiting the collection, use and disclosure of personal information by organizations other than financial ones. Consumer reporting agencies can sell personal information, even if it is obtained from financial institutions, as long as the financial institution gave the consumer notice and the ability to opt-out. The only information they are prohibited from selling is the consumer's age.[72]

4.2.3.2. Personal identifiers

Health care providers are required to use a unique health identifier for each patient.[73] As a result, Social Security Numbers ("SSNs") are not used as identifiers in the context of health care. In other sectors, however, SSNs are commonly used as personal identifiers.

U.S. businesses can require that a consumer provide his or her SSN, even when it is not essential to the transaction at hand. In most transactions, another identifier such as a driver's licence will suffice. Yet, consumers may be pressured into providing their SSN in order to

[70] *Gramm-Leach-Bliley Act, supra* note 56. See also: Electronic Privacy Information Center (EPIC), "*Gramm-Leach-Bliley Act* (GLBA)", online: <http://www.epic.org/privacy/glba>.
[71] *Gramm-Leach-Bliley Act, supra* note 56..
[72] *Ibid.*.
[73] *Health Insurance Portability and Accountability Act of 1996 (HIPAA), supra* note 60.

get goods and services. Furthermore, businesses are not required to keep SSNs confidential; in fact, they can even be sold to data brokers for profit.

Recent U.S. law has addressed the widespread use of these numbers as personal identifiers. The *Social Security Confidentiality Act of 2000* reduces the risk of identity theft posed by mail "tampering" by mandating that SSNs not be visible on unopened mail containing government issued cheques or drafts.[74] This requirement does not reduce the risk posed by mail theft, and the SSN can still be printed on the cheque. But it does mean that this important number is not visible on the envelope.

4.2.3.3. Security

The U.S. *Privacy Act* requires that agencies implement appropriate security measures to protect the confidentiality of records.[75] This statute is generally similar to PIPEDA.

Under the *Health Insurance Portability and Accountability Act of 1996* (HIPAA), health care providers must follow standards to protect electronic health information.[76] Persons who maintain or transmit health information are also required to implement administrative, technical and physical safeguards, to ensure the confidentiality of information and protect against unauthorized uses or disclosures. However, it seems that there is widespread non-compliance with these requirements. There have been 19,420 complaints, mostly about unauthorized access or improper disclosure. About 14,000 of these have been closed with a ruling that there was no violation or with a promise to correct things, which suggests that about one-quarter of the complaints were valid.[77]

Financial institutions are subject to the same requirement, except that they must implement measures to protect against unauthorized access that could result in substantial harm or inconvenience to any customer.[78] To meet this requirement, financial institutions must follow the Federal Trade Commission's Safeguards Rules. These rules do not mandate any specific technical requirements.[79] Instead, they require companies to conduct risk analysis studies and take appropriate steps to counter identified threats. Institutions must also periodically review their data security policies and update them as necessary.[80]

---

[74] *Social Security Number Confidentiality Act of 2000*, 31 U.S.C § 3301. s. 2, online: <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ433.106.pdf>.

[75] *Privacy Act of 1971*, 5 U.S.C. § 552a: online <http://www.uscg.mil/ccs/cit/cim/foia/PRIVACY_ACT_OF_1974.pdf>.

[76] *Health Insurance Portability and Accountability Act of 1996 (HIPAA), supra* note 60.

[77] Washington Post, "Medical Privacy Law Nets No Fines" (5 June 2006), online: <http://www.washingtonpost.com/wp-dyn/content/article/2006/06/04/AR2006060400672.html>.

[78] *Gramm-Leach-Bliley Act, supra* note 56.

[79] Federal Trade Commission, *Data Breaches and Identity Theft* (16 June 2005) at 9, online: <http://www.consumer.gov/idtheft/pdf/ftc_06.16.05.pdf>.

[80] *Ibid*.

4.2.4. Credit Legislation

The U.S. has several statutes regulating the activities of consumer reporting agencies and credit issuers. At the federal level these include the *Fair and Accurate Credit Transactions Act, Fair Credit Reporting Act, Consumer Credit Protection Act, Electronic Funds Transfer Act, Fair Credit Billing Act and Fair Debt Collection Practices Act.* Relevant California statutes are the *Civil Code* and the *Business and Professions Code.*[81]

4.2.4.1.Disclosure

These U.S. credit statutes restrict to whom and for what uses consumer reporting agencies may provide credit reports. Consumer reporting agencies are also required to make a reasonable effort to verify the identity of a prospective credit report user. Permissible uses of credit reports include, but are not limited to, evaluating applications for credit, insurance, rentals, or employment, issuing court orders and law enforcement access.[82]

Credit providers may issue a means of access to a consumer account, such as a credit card, only when consumers request it. However, as in Canada, there is no requirement that the card issuer take reasonable steps to verify the identity of the requestor, which could leave consumer accounts exposed to identity theft.

4.2.4.2. Aftermath

Many of the provisions in U.S. consumer and credit statutes deal with the aftermath of identity crimes, and can assist victims. They include limits on consumer liability for unauthorized electronic fund transfers. Other provisions permit consumers to correct billing errors or otherwise dispute information on credit card accounts when unauthorized activity occurs and the consumer notifies the card issuer.

The *Fair and Accurate Credit Transactions Act* (FACTA) requires business entities to provide a copy of application and business transaction records concerned where identity theft has occurred.[83] This information must be made available to the victim or to a law enforcement agency specified by the victim. Law enforcement agencies and victims need information from affected organizations to investigate claims and redress their situation after identity theft occurred.

---

[81] *Fair and Accurate Credit Transactions Act, supra* note 51; *Fair Credit Reporting Act*, 15 U.S.C. § 1681, online: <http://www.ftc.gov/os/statutes/031224fcra.pdf>; *Consumer Credit Protection Act*, 15 U.S.C. § 1601, online: <http://www.yourcredit.com/assets/pdf/laws/federal/pubLaw/pl-tila.PDF>; *Electronic Funds Transfer Act*, 15 U.S.C. § 1693, online: http://www4.law.cornell.edu/uscode/html/uscode15/usc_sup_01_15_10_41_20_VI.html; *Fair Credit Billing Act*, 15 U.S.C § 1601, online: http://www.ftc.gov/os/statutes/fcb/fcb.pdf; *Fair Debt Collections Practices Act*, 15 U.S.C § 1601, online: <http://www.yourcredit.com/assets/pdf/laws/federal/pubLaw/pl-fdcpa.PDF>; *California Civil Code*, online: http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=civ&codebody=&hits=20 and *Business and Professions Code*, online: <http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=bpc&codebody=&hits=20>.

[82] *Fair and Accurate Credit Transactions Act, supra* note 51 and *California Civil Code, supra* note 81.

[83] *Fair and Accurate Credit Transactions Act, supra* note 51

Other statutes limit the permissible behaviour of debt collectors, restricting when and how often they can communicate with alleged debtors and prohibiting them from engaging in harassing conduct.

4.2.4.3. Rights of Action

U.S. consumer and credit laws provide consumers with a private right of action against consumer reporting agencies, users of credit reports and furnishers of information. Furthermore, although many types of violation involve limited liability, this limitation does not apply when false information was furnished with malice or wilful intent to injure the consumer.

4.2.5. General Legislation

Section 5 of the *Federal Trade Commission Act* prohibits organizations from making deceptive claims about the confidentiality and/or security of the personal information in their control.[84] However, organizations are not required to appropriately secure the information as long as they do not make erroneous claims about the quality of their safeguards.

The Federal Trade Commission seems especially concerned about the attractiveness of "data brokered" consumer information to identity thieves.[85] As a result, Bill S. 1789 would impose a duty on business entities that own, use or license personally identifiable information to adopt reasonable procedures to ensure the security and privacy of personal information.[86] However, this bill only applies to business entities possessing electronic personally identifiable information concerning more than 10,000 individuals.

4.2.6. Bills

A wide range of bills have been proposed over the past years to address the risk posed by identity theft and its aftermath. As noted in Working Paper 3B, some of these bills have become law. The keen interest of some U.S. legislators in strengthening identity theft laws stands in contrast to the Canada, where no government bills and only a few private member's bills have been introduced.

U.S. jurisdictions have proposed bills that would implement the following measures:

- mandating that public agencies and business entities notify individuals of security breaches or unauthorized access to personally identifiable information;
- requiring consumer reporting agencies to implement security freezes;

---

[84] *Federal Trade Commission Act*, 15 U.S.C. §§ 41-58, online: <http://www.law.cornell.edu/uscode/html/uscode15/usc_sec_15_00000041----000-.html>.

[85] *Federal Trade Commission, supra* note 79 at 2-3.

[86] Bill S. 1789 - *Personal Data Privacy and Security Act of 2005*, online: GovTrack.us <http://www.govtrack.us/data/us/bills.text/109/s1789.pdf>.

- restricting the use, sale and display of SSNs and prohibiting requiring consumers to divulge their SSN to obtain goods or services;
- creating new identity theft offences under certain circumstances, such as when a parent steals a dependent's identity;
- imposing limits on the issuance of credit cards;
- creating changes to duties when an individual requests a change of address with banks or the postal service;
- prohibiting debt collectors from collecting debts once they have been notified that the debt results from identity theft or fraud;
- prohibiting phishing;
- prohibiting the distribution of spyware and hard-to-uninstall software;
- requiring the collection of data and statistics on different identity crimes;
- regulating the business practices of "data brokers" that are not consumer reporting agencies;
- requiring businesses that own, use or license personal information to implement appropriate security measures;
- providing funds to law enforcement agencies;
- creating new rights of action against those who violate legal requirements;
- providing funds to promote research on identity theft and fraud; and
- requiring that businesses obtain consumer consent before selling personal information to non-affiliated third parties.

Other bills that are not directly related to identity theft also recognize the risk of this crime by providing that certain information can be redacted from some records.

4.3. California

Our inventory of California identity theft laws includes a number of statutes that provide a higher degree of protection against identity theft than do federal statutes. This confirms that California is a leader in developing an innovative legal framework to combat this crime. Highlights of California identity theft laws include the following:

4.3.1. Identity theft offence

The California *Penal Code* contains an identity theft-specific provision.[87] This offence also covers corporate identity theft, by defining a "person" as "a natural person, firm, association, organization, partnership, business trust, company, corporation, limited liability company, or public entity". As with the federal law, possession of the personal information of another person, with intent to defraud, is criminalized.

[87] *California Penal Code*, s. 530.5, online: http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=pen&codebody=&hits=20

4.3.2. Notification of security breaches

California was the first state to enact provisions requiring public agencies and businesses to notify California residents of any unauthorized access to their computerized personal information held by the agency or business.[88] The California legislation is discussed in the CIPPIC White Paper on Approaches to Security Breach Notification.[89]

The provisions require notification only when an individual's first name or first initial and last name are stored in combination with other data such as a SSN, driver's license number or bank account information. This ensures that notification is required only when there is a serious and immediate threat of identity theft.

4.3.3. Security freeze

Californians have a right to place a security freeze on their credit file.[90] This right can provide a strong defence against identity theft. The security freeze prohibits consumer reporting agencies from releasing an individual's credit report to a third party without prior express authorization by the consumer. When a consumer requests this protection, he or she is protected against one of the most common identity theft scenarios, in which a thief uses a victim's identity to obtain new credit. This protection is only effective, however, if credit grantors require a credit check before granting new credit.

4.3.4. Right to investigation

California was also the first state to give its citizens the right to obtain a copy of the police report on their identity theft case.[91] Obtaining a police report is an important first step in dealing with the aftermath of identity theft. The police report can be provided to creditors to substantiate that an individual is a victim of identity theft and not liable for certain transactions. The police report can also be used to obtain records from businesses that the identity thief defrauded.

4.3.5. Right to business records

The California Penal Code gives identity theft victims the right to obtain information about any account opened in their name by an identity thief, upon presentation of a police report.[92] This information must include the personal information used to open the account and records of all business transactions conducted with identity thieves.

---

[88] *California Civil Code*, ss. 1798.29, 1798.82-1798.84, online: <http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html>.
[89] *CIPPIC, supra* note 1.
[90] *California Civil Code, supra* note 88 at s. 1785.11.2
[91] *California Penal Code, supra* note 87 at s. 530.6.
[92] *Ibid.* at s. 530.8.

5. THE U.K, AUSTRALIA AND FRANCE

Neither the United Kingdom, Australia nor France has yet developed a comprehensive set of identity theft statutes similar to those in the U.S. However, as discussed in Working paper 3C, each has legislation dealing with various aspects of identity theft.

The U.K., for example, has legislation requiring businesses to protect personal information they collect and criminalizing the possession of false identity documents. Australia has legislation relating to fraud, deception and forgery which relate to the use of personal information for identity theft. France has similar legislation, and also criminalizes the unauthorized collection and fraudulent use of personal information.