



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

**CANADIAN LEGISLATION
RELEVANT TO IDENTITY THEFT:
AN ANNOTATED REVIEW**

March, 2007

CIPPIC Working Paper No. 3A (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), "Canadian Legislation Relevant to Identity Theft: Annotated Review", CIPPIC Working Paper No.3A (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
No.3A: Canadian Legislation Relevant to Identity Theft: Annotated Review
No.3B: United States Legislation Relevant to Identity Theft: Annotated Review
No.3C: Australian, French, and U.K. Legislation Relevant to Identity Theft: Annotated Review
No.4: Caselaw on Identity Theft
No.5: Enforcement of Identity Theft Laws
No.6: Policy Approaches to Identity Theft
No.7: Identity Theft: Bibliography

CIPPIC

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

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

TABLE OF CONTENTS

	Page
1. CANADIAN STATUTES – ANNOTATED REVIEW.....	1
1.1. FEDERAL	1
1.1.1. <i>Criminal Code, R.S.C., 1985, c. C-46.....</i>	<i>1</i>
1.1.2. <i>Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5.....</i>	<i>5</i>
1.1.3. <i>Privacy Act, R.S. 1985, c. P-21.....</i>	<i>6</i>
1.1.4. <i>Employment Insurance Act, S.C. 1996, c. 23.....</i>	<i>6</i>
1.1.5. <i>Canada Post Corporation Act, R.S. 1985, c. C-10.....</i>	<i>7</i>
1.1.6. <i>Federal Legislative Proposals</i>	<i>7</i>
1.2. ONTARIO	9
1.2.1. <i>Consumer Reporting Act, R.S.O. 1990, c. C.33</i>	<i>9</i>
1.2.2. <i>Personal Health Information Protection Act, S.O. 2004, c. 3, Sch. A.....</i>	<i>10</i>
1.2.3. <i>Trespass to Property Act, R.S.O. 1990, c. T.21.....</i>	<i>10</i>
1.2.4. <i>Consumer Protection Act, S.O. 2002, c. 30, Sch. A.....</i>	<i>11</i>
1.2.5. <i>Mortgage Brokers Act, R.S.O. 1990, c. M.39.....</i>	<i>11</i>
1.2.6. <i>Vital Statistics Act, R.S.O. 1990, c. V.4.....</i>	<i>11</i>
1.2.7. <i>Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.3</i>	<i>12</i>
1.2.8. <i>Freedom of Information and Protection of Privacy Act - R.R.O. 1990, Reg. 460.....</i>	<i>12</i>
1.2.9. <i>Collection Agencies Act, R.R.O. 1990, Reg. 74.....</i>	<i>12</i>
1.2.10. <i>Highway Traffic Act, R.S.O. 1990, c. H.8.....</i>	<i>13</i>
1.2.11. <i>Bill 152 - An Act to modernize various Acts administered by or affecting the Ministry of Government Services.....</i>	<i>13</i>
1.3. BRITISH COLUMBIA	15
1.3.1. <i>Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165.....</i>	<i>15</i>
1.3.2. <i>Business Practices and Consumer Protection Act, R.S.B.C. 2004, c. 2.....</i>	<i>15</i>
1.3.3. <i>Vital Statistics Act, R.S.B.C. 1996, c. 479.....</i>	<i>16</i>
1.4. ALBERTA.....	16
1.4.1. <i>Personal Information Protection Act, S.A. 2003, c. P-6.5</i>	<i>16</i>
<i>Protection of information.....</i>	<i>17</i>
1.4.2. <i>Fair Trading Act, c. F-2.....</i>	<i>18</i>
1.4.3. <i>Debtors' Assistance Act, c. D-6.....</i>	<i>18</i>
1.4.4. <i>Freedom of Information and Protection of Privacy Act, R.S.A. 2000, c. F-25.....</i>	<i>18</i>
1.5. QUEBEC.....	19
1.5.1. <i>An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information, R.S.Q., c. A-2.1</i>	<i>19</i>
1.5.2. <i>An Act Respecting the Protection of Personal Information in the Private Sector, R.S.Q., c. P- 39.1 20</i>	<i>20</i>
1.5.3. <i>Consumer Protection Act, R.S.Q., c. P-40.</i>	<i>21</i>
1.6. MANITOBA	21
1.6.1. <i>Personal Investigations Act, C.C.S.M. c. P34.....</i>	<i>21</i>
1.6.2. <i>The Consumer Protection Act, C.C.S.M. c. C200.....</i>	<i>22</i>
1.6.3. <i>Bill 200 - The Personal Information Protection and Identity Theft Prevention Act.....</i>	<i>23</i>
1.7. SASKATCHEWAN	24
1.7.1. <i>Credit Reporting Act, S.S. 2004, c. C-43.2.....</i>	<i>24</i>
1.7.2. <i>The Consumer Protection Act, S.S. 1996, c. C-30.1.....</i>	<i>25</i>
1.8. NOVA SCOTIA.....	25
1.8.1. <i>Consumer Reporting Act, R.S.N.S. 1989, c. 93</i>	<i>25</i>
1.8.2. <i>Consumer Protection Act, R.S. 1989, c. 9.....</i>	<i>25</i>

1.8.3.	<i>Vital Statistics Act, R.S.N.S. 1989, c. 494</i>	26
1.8.4.	<i>Personal Information International Disclosure Protection Act, S.N.S. 2006, c. 3</i>	26
1.9.	NEW BRUNSWICK	26
1.9.1.	<i>Collection Agencies Act, R.S.N.B. 1973, c. C-8</i>	26
1.10.	PRINCE EDWARD ISLAND	26
1.10.1.	<i>Consumer Reporting Act, R.S.P.E.I. 1988, c. C-20</i>	26
1.10.2.	<i>Consumer Protection Act, R.S.P.E.I. 1988, c. C-19</i>	27
1.11.	NEWFOUNDLAND AND LABRADOR	27
1.11.1.	<i>Consumer Reporting Agencies Act, R.S.N.L. 1990, c. C-32</i>	27
1.11.2.	<i>Consumer Protection Act, R.S.N.L. 1990, c. C-3</i>	28
2.	STATUTE EXCERPTS	29
2.1.	FEDERAL LAWS	29
2.1.1.	<i>Criminal Code, R.S.C., 1985, c. C-46</i>	29
2.1.2.	<i>Bill C-359 - An Act to amend the Criminal Code (personal identity theft)</i>	43
2.1.3.	<i>Bill C-299 - An Act to amend the Criminal Code, the Canada Evidence Act and the Competition Act (personal information obtained by fraud)</i>	44
2.1.4.	<i>Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5</i>	45
2.1.5.	<i>Privacy Act, R.S. 1985, c. P-21</i>	47
2.1.6.	<i>Employment Insurance Act, S.C. 1996, c. 23</i>	50
2.1.7.	<i>Canada Post Corporation Act, R.S. 1985, c. C-10</i>	51
2.2.	ONTARIO	51
2.2.1.	<i>Consumer Reporting Act, R.S.O. 1990, c. C.33</i>	51
2.2.2.	<i>Bill 174 - Consumer Reporting Amendment Act, 2005</i>	55
2.2.3.	<i>Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sch. A</i>	55
2.2.4.	<i>Trespass to Property Act, R.S.O. 1990, c. T.21</i>	56
2.2.5.	<i>Consumer Protection Act, S.O. 2002, c. 30, Sch. A</i>	57
2.2.6.	<i>Mortgage Brokers Act, R.S.O. 1990, c. M.39</i>	57
2.2.7.	<i>Vital Statistics Act, R.S.O. 1990, c. V.4</i>	58
2.2.8.	<i>Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31</i>	61
2.2.9.	<i>Freedom of Information and Protection of Privacy Act - R.R.O. 1990, Reg. 460</i>	64
2.2.10.	<i>Collection Agencies Act, R.R.O. 1990, Reg. 74</i>	64
2.2.11.	<i>Highway Traffic Act, R.S.O. 1990, c. H.8</i>	65
2.2.12.	<i>Bill 152 - An Act to modernize various Acts administered by or affecting the Ministry of Government Services</i>	66
2.3.	BRITISH COLOMBIA	73
2.3.1.	<i>Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165</i>	73
2.3.2.	<i>Vital Statistics Act, R.S.B.C. 1996, c. 479</i>	73
2.3.3.	<i>Bill 43- Vital Statistics Amendment Act, 2004</i>	73
2.4.	ALBERTA	74
2.4.1.	<i>Personal Information Protection Act, S.A. 2003, c. P-6.5</i>	74
2.4.2.	<i>Fair Trading Act, Reg. 194/99 Collection and Debt Repayment Practices Regulation</i>	75
2.4.3.	<i>Freedom of Information and Protection of Privacy Act, R.S.A. 2000, c. F-25</i>	78
2.5.	QUEBEC	82
2.5.1.	<i>An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information, R.S.Q., c. A-2.1</i>	82
2.5.2.	<i>An Act Respecting the Protection of Personal Information in the Private Sector, R.S.Q., c. P-39.1</i>	85
2.5.3.	<i>Consumer Protection Act, R.S.Q., c. P-40</i>	86
2.6.	MANITOBA	86
2.6.1.	<i>Personal Investigations Act, C.C.S.M. c. P34</i>	86
2.6.2.	<i>The Consumer Protection Act, C.C.S.M. c. C200</i>	88
2.6.3.	<i>Bill 200 - The Personal Information Protection and Identity Theft Prevention Act</i>	90
2.7.	SASKATCHEWAN	93
2.7.1.	<i>Credit Reporting Act, S.S. 2004, c. C-43.2</i>	93
2.7.2.	<i>The Consumer Protection Act, S.S. 1996, c. C-30.1</i>	96

2.8.	NOVA SCOTIA.....	97
2.8.1.	<i>Consumer Reporting Act, R.S.N.S. 1989, c. 93</i>	97
2.8.2.	<i>Vital Statistics Act, R.S.N.S. 1989, c. 494</i>	100
2.8.3.	<i>Personal Information International Disclosure Protection Act, S.N.S. 2006, c. 3</i>	101
2.9.	NEW BRUNSWICK.....	103
2.9.1.	<i>Collection Agencies Act, N.B. Reg. 84-256</i>	103
2.10.	PRINCE EDWARD ISLAND.....	103
2.10.1.	<i>Consumer Reporting Act, R.S.P.E.I. 1988, c. C-20</i>	103
2.10.2.	<i>Conduct of Creditors Regulations, P.E.I. Reg. EC578/83</i>	107
2.11.	NEWFOUNDLAND AND LABRADOR	108
2.11.1.	<i>Consumer Reporting Agencies Act, R.S.N.L. 1990, c. C-32</i>	108

1. CANADIAN STATUTES – ANNOTATED REVIEW

1.1. Federal

1.1.1. Criminal Code, R.S.C., 1985, c. C-46

Although the Criminal Code addresses different aspects of both phases of identity theft, most provisions relate to the unlawful use of another person's personal information. Presented below are the main provisions of the Code that are applicable to identity theft.

Forgery of or uttering forged passport

Section 57 criminalizes the making and use of forged passports and the making of misleading statements to obtain them. This provision relates to the first stage of identity theft. In order to obtain a passport, the identity thief must have acquired without authorization the necessary personal information to apply for it. Forged passports then may be used to engage in other unlawful uses of this personal information.

Theft

Section 322 criminalizes theft, the taking or converting of anything fraudulently and without colour of right, to achieve one of four purposes. The most common stated purpose is to deprive the rightful owner of the thing or his or her property or interest in it. This provision criminalizes certain techniques used to acquire personal information and the stealing of identification documents.

However, section 322 does not criminalize stealing personal information by itself. There is no proprietary interest in personal data per se.¹ Thus, for example, this section criminalizes stealing a driver's licence card but it does not criminalize stealing the driver's licence number by making a copy or memorizing it. The driver's licence number is considered to be confidential information and confidentially cannot be stolen.²

Theft of telecommunication service

Section 326 criminalizes the theft of telecommunications services, such as the use of stolen cell phone accounts. It is also applicable to certain acquisition techniques that rely on the internet. Section 327 criminalizes the trafficking and possession of devices used to steal telecommunication services.

¹ Department of Justice, *Consultation Document on Identity Theft* (October 2004) at 14. Not publicly available.

² *R. c. Stewart*, [1998] 1 R.C.S. 963. The wording of that section restricts the meaning of "anything" in two ways: first, whether tangible or intangible, "anything" must be of a nature such that it can be the subject of a proprietary right; and second, the property must be capable of being taken or converted in a manner that results in the deprivation of the victim. Confidential information does not fall within that definition. Confidential information does not qualify as property for the purposes of s. 283 of the Code.

Criminal breach of trust

Section 336 criminalizes the conversion of anything held by an organization, by an insider of the organization. This provision has been used when employees have obtained loans in the name of clients and when some employees have ordered extra credit cards in the name of clients. Given the ruling in *R. v. Stewart*, it is not clear whether an insider could be charged with criminal breach of trust if they had only misappropriated personal information about a client, without attempting to use it.³

Theft, forgery, etc., of credit card

Section 342 criminalizes the theft, forgery or falsification of a credit card. Thus, it prohibits skimming to obtain debit, credit or calling card information and the forging, use and trafficking of forged or falsified credit cards. An offence is committed under paragraph 342.1(1)(c)(i) when an accused finds a credit card and subsequently forms the intention to convert the card to his/her own use.⁴

Subsection 342(3) criminalizes the possession, use and trafficking of credit card data. The result is that selling or buying credit card information from “carder networks” is an offence. Unfortunately, “credit card data” is not defined and it is not clear if it is limited to existing card data or if using personal information to obtain a new credit card is sufficient.

Section 342.01 criminalizes the possession and trafficking of devices used to make false credit cards.

Unauthorized use of computer

Section 342.1 criminalizes many of the identity theft techniques that rely on computers, electronic equipment or the internet to acquire or use personal information. For example, it criminalizes the use of spyware, pharming, trojan horse applications, key loggers, cracking and wardriving, all of which involve the “interception of any function of a computer system”. The use of acoustic equipment to record PIN numbers when they are entered using a phone is also criminalized.

This section also criminalizes the use, possession and trafficking of “computer passwords”. This provision is applicable to phishing and pharming if the scam is used to acquire “computer passwords” such as usernames and passwords needed to access accounts. It is not clear if phishing to acquire personal information, excluding information required to access existing accounts, is sufficient. Arguably, the personal information can be used to gain access to the password, for example, by contacting a bank and getting the password of an account reset.

³ *Ibid.*

⁴ Department of Justice, *supra* note 1 at 18.

The provision on computer passwords criminalizes the use of internet service provider (ISP) accounts via credentials that were obtained fraudulently. Identity thieves operating online use these accounts to cover their traces, send phishing e-mails and the like.

Possession of device to obtain computer service

Section 342.2 criminalizes the possession and trafficking of devices used to commit offences under section 341.1. For example, the possession of a key logger to capture passwords at a public terminal is criminalized.

Possession of property obtained by crime

Section 354 criminalizes the possession of any property or thing knowing that it was obtained by criminal means. This section offers no direct protection against either stage of identity theft and does not provide any victim assistance. However, the doctrine of recent possession permits a court to infer guilty knowledge from unexplained possession of recently stolen goods.⁵ Thus, prosecutors have used this section to charge identity thieves who had obtained property or money.

Theft from mail

Section 356 makes it an offence to steal any thing sent by post, after it is deposited at a post office and before it is delivered, or to be in possession of such things.

Forgery and uttering forged document

Section 366 criminalizes the use of personal information to make forged documents, knowing they are false and with the intent that they should be used or acted on as genuine, to the prejudice of anyone, or to induce someone to act or refrain from acting by their belief that they are genuine. The offence is committed as soon as the document is made with the required intent and knowledge. The perpetrator does not need to intend that a particular person will act on it.⁶

There are two types of false documents covered: 1) a document that in whole, or a material part of which, purports to be made by or on behalf of a person who did not make it or authorize it to be made or who did not exist⁷; 2) a document made in the name of an existing person, with a fraudulent intent that it should pass as having been made by another person.

Section 368 criminalizes the use of forged documents. Forged documents can be used in all stages of an identity theft. They are sometimes used to acquire more information; for example a fake driver's licence can be presented in order to redirect a victim's mail. They can also be presented as identification when opening new accounts. For an offence to be committed, the document must be used; its mere possession is not sufficient and actions

⁵ *Ibid.* at 15.

⁶ *Ibid.* at 19.

⁷ *Ibid.*

where no deceit is involved are not criminalized.⁸ The transfer of a forged document to a person who knows that the document is forged is not an offence⁹.

Counterfeiting stamp, etc.

Section 376(2) of the code criminalizes using a counterfeit mark to falsify driver's licences or other photo identification.

Fraud

Section 380 of the code criminalizes fraud for economic gain. Thus, it criminalizes the techniques that use personal information for economic gain. This section is applicable to most unlawful uses of personal information. For fraud to be committed there must be 1) a deceit, falsehood or "other fraudulent means" and 2) a deprivation (detriment, prejudice or risk thereof to the economic interest of the victim). A proof of the intention to cause a loss is not required.

One cannot be defrauded of his or her personal information unless it leads to a deprivation. If someone fraudulently obtains personal information and subsequently opens a new credit card account, for example, the loss will be suffered by the card issuer and not by the person whose information was stolen. Fraud in this case is not committed against the person; it is committed against the card issuer.

Personation with intent

Personation is committed by impersonating a person, living or dead, with the intent to gain a personal advantage, obtain property or cause a disadvantage to a person.

Section 403 deals directly with "identity theft" or personation. Personation criminalizes both types of unlawful uses of personal information: fraudulent uses for economic gain and uses that relate to the appropriation of someone's image. This measure is framed in language broad enough to be applicable to almost any type of unlawful use committed as part of an identity theft crime. Some identity thieves have been charged under this section and have pleaded guilty.¹⁰

Conspiracy

To obtain a conviction under subsection 465(1)(c) there must be an agreement by two or more persons to commit a criminal offence or to achieve a lawful object by committing a criminal offence, and an intention by them to agree and intention to carry out the agreement.

This provision can be used in the context of identity theft when the agreement is for one person to collect personal information and for another to use it. The collection of

⁸ *Ibid.* at 20.

⁹ *Ibid.*

¹⁰ *R. v. Thiel*, [2005] A.J. No. 698; *R. v. Bradley*, [2004] A.J. No. 1278; *R. v. Taft*, [2003] B.C.J. No. 444.

information by the first person is usually not illegal in itself, but the subsequent unlawful use is. The involvement of the first person must be more than mere knowledge or passive acquiescence.¹¹ These agreements are hard to prove in the absence of wiretaps or the testimony of a witness to the agreement.¹²

1.1.2. *Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5*

The *Personal Information Protection and Electronic Documents Act* (“PIPEDA”) is relevant to identity theft because it pertains to the security of personal information. By improving information collection, management and disclosure practices on the part of businesses, opportunities for identity theft can be lessened. PIPEDA also provides a definition for personal information: “personal information” means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.

Unfortunately, the principles are drafted in very broad terms, offering a lot of flexibility to organizations, and the statute lacks both strong enforcement powers and penalties for noncompliance. Experience has shown that its provisions are widely ignored by retailers.¹³

Also, PIPEDA does not include a requirement that individuals whose personal information might be at risk be notified in the event of a security breach. This deficiency is discussed in detail in the CIPPIC White Paper entitled “Approaches to Security Breach Notification”.¹⁴

Appropriate purposes

Section 5 imposes a duty to comply with the principles set out in Schedule 1 of the Act. It also limits the uses an organization can engage in with the information it collects. The information can only be collected, used, or disclosed for purposes that a reasonable person would consider are appropriate in the circumstances.

Principle 4 – Limiting Collection

This principle limits the collection of information to “that which is necessary for the purposes identified by the organization.” Indiscriminate collection is not permitted. It also limits methods of collection to “fair and lawful means”.

¹¹ *Department of Justice, supra* note 1 at 1.

¹² *Ibid.*

¹³ The Canadian Internet Policy and Public Interest Clinic (CIPPIC), *Compliance with Canadian Data Protection Laws* (April 2006), online: <www.cippic.ca>.

¹⁴ The Canadian Internet Policy and Public Interest Clinic (CIPPIC), *Approaches to Security Breach Notification: A White Paper* (9 January 2007), online: <www.cippic.ca>.

Principle 5 – Limiting Use, Disclosure, and Retention

This principle limits the uses and disclosures of personal information to those specified at the time of collection. It also imposes a time limit, “only as long as necessary”, on the retention of personal information.

Principle 7 – Safeguards

This principle imposes a duty to use appropriate safeguards when storing, transmitting and destroying or discarding personal information. Implicitly, this principle imposes a duty of care on organizations to prevent loss or theft, as well as unauthorized access, disclosure, copying, use, or modification of personal information they hold. However, it does not mandate the implementation of specific safeguards such as access controls based on a “need-to-know” basis. Nor does it require reporting or notification of security breaches.

1.1.3. Privacy Act, R.S. 1985, c. P-21

The *Privacy Act* governs the federal government’s collection and use of the personal information of Canadians. Limiting the use and disclosure of personal information reduces the risk of identity theft. However, this statute does not have any requirements that the information be safeguarded appropriately and does not mandate any access controls. The Privacy Commissioner has called for reforms to this older statute.¹⁵

Use of personal information

Section 7 limits how the information provided to a government institution can be used. Information cannot be used for purposes other than for the purpose of collection.

Disclosure of personal information

Section 8 limits the disclosure of personal information provided to a government institution.

*1.1.4. Employment Insurance Act, S.C. 1996, c. 23**Prohibitions*

Section 141 prohibits applying for a Social Insurance Number (SIN) more than once. It also prohibits using or lending a SIN number with the intention to defraud and making or selling copies of SIN cards.

¹⁵ Ottawa Citizen, “Outdated Privacy Act needs overhaul” (30 March 2006) at A3.

1.1.5. Canada Post Corporation Act, R.S. 1985, c. C-10

Opening mail

Section 48 makes it an offence to knowingly open, detain or delay any mail.

Abandonment of mail

Section 49 makes it an offence to unlawfully and knowingly abandon, misdirect, obstruct, delay or detain the progress of any mail or mail conveyance.

1.1.6. Federal Legislative Proposals

At the federal level, there have recently been two federal private members' bills pertaining to identity theft. There is also a private member's bill in Manitoba, which is discussed below.

The federal bills would criminalize certain aspects of identity theft. They are: 1) Bill C-359 - *An Act to amend the Criminal Code (personal identity theft)*; and 2) Bill C-299 - *An Act to amend the Criminal Code, the Canada Evidence Act and the Competition Act (personal information obtained by fraud)*.

1.1.6.1. Bill C-359 - An Act to amend the Criminal Code (personal identity theft)

This bill was tabled April 5, 2005 by M.P. Tom Lukiwski but subsequently died when the government fell in December 2005.¹⁶ Its provisions were directed toward the first phase of identity theft, the collection of personal information. The purpose of this bill was to criminalize the possession and transfer of personal information and identity documents without lawful excuse.

The bill cast a very broad net. Information was defined as "information that can be used to identify a person". Also, the mere possession of stolen information would be an offence.

With respect to this last point, the Department of Justice Canada has noted that:

"It is unlikely that an offence that criminalized the possession of misappropriated information, without more, would be held to be constitutional. At a minimum, the accused must have knowledge that the personal information was misappropriated and must not have a lawful excuse for possessing the information."¹⁷

Bill C-359 did not meet these minimal constitutional requirements.

¹⁶ Parliament of Canada, *Federal Political Experience - Lukiwski, Tom*, online:

<<http://www.parl.gc.ca/information/about/people/key/bio.asp?Language=E&query=18586&s=M>>.

¹⁷ Department of Justice, *supra* note 1 at. 8.

1.1.6.2. Bill C-299 - An Act to amend the Criminal Code, the Canada Evidence Act and the Competition Act (personal information obtained by fraud)

This bill was tabled May 17, 2006 by M.P James Rajotte. The purpose of the bill is to protect individuals against the collection of their personal information through fraud and impersonation. This practice is often known as “pretexting” and it is a widespread problem in the growing market for personal information. The bill aims to close some of the loopholes in Canada's data protection law that allow data brokers to exploit people's personal information for commercial gain.

Like Bill C-359, this bill also targets the first phase of identity theft, the collection of personal information. However, this bill approaches the problem from a different perspective. Bill C-359 would criminalize the end result of collection, i.e. the possession of personal information, whereas this bill would criminalize the collection process itself, when it is conducted by false pretences or by personation. It would also criminalize trafficking of personal information that was obtained in such a manner.

The bill would make it an offence to counsel another person to obtain, sell or otherwise disclose personal information obtained from a third party by a false pretence or by fraud. These offences would be punishable by up to two years imprisonment. The *Criminal Code* offence for personation would be amended to make it an offence to personate a person, living or dead, with intent to obtain any personal information about a third party. It would be an illegal trade practice under the *Competition Act* to seek to obtain personal information from a third party by fraud, false pretence or fraudulent personation of any person, living or dead.

The approach in this bill avoids the constitutional problems inherent in Bill C-359, since it would criminalize specific fraudulent behaviour. Its not clear however if subsection 362(1)(g) “sells or otherwise discloses personal information obtained from a third party by a false pretence or by fraud” covers the situation where someone outside Canada acquired the personal information and transferred it to a Canadian who subsequently used it.

Another shortfall is that this bill does not address the significant problem posed by insider abuse. When an insider collects personal information about a business's clients, the employee will rarely have to use false pretences or personate another individual. Information acquired in this manner could be transferred to a third party without breaking the law. A similar problem exists with personal information obtained either via mail theft or dumpster diving. Proving mail theft can be very difficult if the identity thief has simply copied the information from the mail and discarded the actual mail.

A final problem is that identity thieves will rarely be caught when they are acquiring personal information. The police are more likely to arrest someone who is already in possession of identifying information about other individuals. This bill would continue to leave them powerless in the former situation.

1.2. Ontario

1.2.1. Consumer Reporting Act, R.S.O. 1990, c. C.33

The *Consumer Reporting Act* provides some prevention and early detection mechanisms that have the potential to minimize identity theft.

Disclosure of report on request

Section 10.2 imposes a duty to give a written notice to consumers that a credit report will be requested. Section 10.5 imposes a duty on organizations to notify the consumer in writing that they intend to share information about the consumer with others, unless they obtain the consumer's consent.

Section 10 ensures that consumers are informed, but it does not give them any power to limit the disclosure of their information. Credit grantors can refuse to extend credit unless consumers consent to its disclosure.

Right of consumer to disclosure

Section 12 of the *Consumer Reporting Act* gives consumers the right to request their file from the credit bureau and lists of organizations that have accessed the file. By doing this on a regular basis, consumers can detect any unauthorized activities in their credit file.

1.2.1.1. Bill 174 - An Act to amend the Consumer Reporting Act

This bill, introduced by M.L.A. Tony Ruprecht in 2005, has passed the second reading and at the time of writing, is being studied by the Standing Committee on Finance and Economic Affairs.¹⁸ Its significance for identity theft lays in the fact that it would provide for a duty to notify consumers about unlawful disclosures, or security breaches.

Collection, storage and disclosure of information in files

Section 3 would amend section 9 to impose a duty to ensure that "information is collected, stored and disclosed in accordance with this Act and the principles of fair information practices listed in Schedule 1 to the *Personal Information Protection and Electronic Documents Act (Canada)*". Section 3 would also impose a duty to adequately secure, using encryption, personal and credit information from inadvertent disclosure.

Supplying list of names

Section 5 would amend subsection 11 (4) to impose a duty on credit agencies to obtain explicit consent from the consumer when they receive a list of names and criteria, or receive a request for names of persons, so that information may be inferred about them.

¹⁸ Legislative Assembly of Ontario, Bill 174, *Consumer Reporting Amendment Act, 2005*: online <http://www.ontla.on.ca/library/bills/381/174381.htm>.

Duty to inform consumer of unlawful disclosure

Section 7 would amend section 12 to add a duty to inform consumers of unlawful disclosure of their personal information.

1.2.2. *Personal Health Information Protection Act, S.O. 2004, c. 3, Sch. A*

The object of this act is to protect the personal health information of Ontario residents. Health information is defined as the information pertaining to physical and mental health, health history, the person's health care providers, eligibility, payments and health number. The statute contains strong provisions for information security and is the only Canadian statute that requires notification in the event of a security breach.

Security

Section 12 of this act imposes a duty of care on health providers to protect health information. They must take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

Notification

Section 12 also 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.

Identity of individual

Section 54 (9) imposes a duty to take reasonable steps to be satisfied as to the individual's identity when a request to access health information is made by an individual.

1.2.3. *Trespass to Property Act, R.S.O. 1990, c. T.21*

This statute offers some remedies against persons who a property-owner suspects of dumpster diving. It can be used to deny access to the owner's property and expel anyone who does not have express permission to be on the premises.

It thus provides individuals and organizations with a means to control who enters upon their premises. However, these provisions by themselves do not offer much protection against dumpster diving or theft of equipment containing personal information. Protection is afforded only if individuals or organizations invest in enforcing the rights granted to them under this Act.

Trespass an offence

Section 2 of this act makes it an offence to enter onto premises without the express permission of the owner, if the premises are enclosed in a manner that indicates the occupier's intention to keep persons off the premises.

Method of giving notice

Section 5 lets an owner expressly deny access to the premises by means of signs posted, such that a sign is clearly visible in daylight under normal conditions from the approach to each ordinary point of access to the premises to which it applies.

Arrest without warrant on premises

Section 9 allows the police or the owner to arrest persons who they have reasonable and probable grounds to think are on the premises in contravention of section 2.

1.2.4. Consumer Protection Act, S.O. 2002, c. 30, Sch. A*Limiting liability for unauthorized charges*

Section 69 limits the responsibility of a borrower when unauthorized charges are made on his or her account. This statute offers little or no protection against identity theft, but it does assist in minimizing its impacts. It only limits the potential financial liability of victims.

1.2.5. Mortgage Brokers Act, R.S.O. 1990, c. M.39*Offences*

Section 31 of this Act criminalizes providing false information on applications or other statements. The Act does not, however, impose a duty on mortgage brokers to verify the identity of individuals.

1.2.6. Vital Statistics Act, R.S.O. 1990, c. V.4

The duty to keep records and documents in a place of safety reduces the risk of theft and insider abuse. The duty to return found documents can help prevent some identity documents from falling in the wrong hands. However, this statute does not impose a duty on the registrars to take reasonable measures to ascertain that the information provided is accurate, or to ascertain the identity of the individual providing or requesting it.

Duties of division registrar

Section 39 imposes a duty on registrars to keep all records and documents in a safe place.

Duty to report lost documents

Section 51 imposes a duty on the registrar to report any loss or theft of certificates or certified copies of a birth registration. It also imposes a duty to return any found documents.

False information

Section 56 criminalizes making false statements in any notice, registration, statement, certificate, return or other document respecting any particulars required to be furnished under this Act.

1.2.7. *Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.3**Personal privacy*

Section 21 imposes limits on the disclosure of information about an individual. Information cannot be disclosed if the disclosure would constitute an unjustified invasion of personal privacy.

Section 21.3 provides an extensive list of situations where a disclosure is presumed to be an unjustified invasion of privacy. It is unclear if this presumption can be refuted or how or what circumstances would justify refuting it.

Regulations

Section 60 (1) gives the Lieutenant Governor in Council the power to make regulations regarding administrative, technical and physical safeguards to ensure the security and confidentiality of records and personal information under the control of government institutions.

1.2.8. *Freedom of Information and Protection of Privacy Act - R.R.O. 1990, Reg. 460*

Section 4 imposes a duty to take reasonable measures to prevent unauthorized access. It also imposes a duty to implement access controls on a “need to know” basis.

The duty to take reasonable measures to prevent unauthorized access can help reduce the risk of identity theft. The duty to implement access controls on a “need to know” basis can significantly reduce the risks posed by insider abuse. An insider cannot access a specific record unless his or her duties call for it. This makes it very hard to find information based on requests that come from outside. It also makes it difficult to assemble lists that can be sold.

1.2.9. *Collection Agencies Act, R.R.O. 1990, Reg. 74*

Section 20.h prohibits collection agencies and collectors from communicating with a person when that person has informed them that they are not the debtor sought, unless the

collection agency or the collector first takes all reasonable precautions to ensure that the person is in fact the debtor.

This regulation does not offer any protection against identity theft *per se*. However, it offers protection against overzealous debt collectors, who are often a significant factor in the pain and suffering of victims. In order to invoke this provision, the consumer would need an affidavit or police report.

1.2.10. Highway Traffic Act, R.S.O. 1990, c. H.8

Displaying licence that has been suspended, altered, etc

Section 35(a) makes it an offence to display or possess a fictitious, imitation, altered or fraudulently obtained driver's licence. Another offence, 35(d), is an individual using a driver's licence issued to another individual as his or her own. Section 35(e) also makes it an offence for an individual to have more than one driver's licence in his or her possession.

For an offence to be committed under s. 35(a) the individual must have a physical copy of the fake. The mere possession of another person's driver's licence number is not an offence. The same applies to s. 35(d) and (e).

1.2.11. Bill 152 - An Act to modernize various Acts administered by or affecting the Ministry of Government Services

The Bill aimed to amend several Acts, most of which are administered by the Ministry of Government Services. It was passed by the Ontario legislature on December 12, 2006 and received Royal Assent on December 20, 2006. It is known as the *Consumer Protection and Service Modernization Act, 2006*.¹⁹

The statute deals with identity theft in two important aspects. First, the legislation permits consumers to place fraud alerts on their credit file if they believe their personal information has been compromised. Second, safeguards are introduced to protect against mortgage fraud. These safeguards will ensure that ownership of a property cannot be lost as a result of the registration of a falsified mortgage, fraudulent sale or counterfeit power of attorney.

An amendment to allow consumers to place security freezes on their credit reports was not pursued, apparently due to concerns that Canadian credit agencies lack the capacity to meet expected demands. The mortgage fraud provisions assist owners, but do nothing to help unwitting and innocent buyers of properties whose mortgages were acquired by fraud.

¹⁹ *Consumer Protection and Service Modernization Act, 2006*, online: <http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/90c33_e.htm>.

Consumer Reporting Act amendments

Alert to verify identity of consumer

Section 12.1 will require consumer reporting agencies to place an alert on a consumer's credit file when the consumer requests it. The consumer has the obligation to provide contact information. The consumer reporting agency must take reasonable steps to verify that the person requiring the inclusion, amendment or removal of an alert is the consumer. Consumer reporting agencies can charge a fee for setting, amending and removing alerts and can also determine when such an alert will expire.

Section 12.2 imposes the obligation on consumer reporting agencies to furnish the alert to every person to whom any information from the file is disclosed. Section 12.3 imposes a duty on persons who received the alert to take reasonable steps to verify that the person involved in the transaction is the consumer before proceeding with the transaction. A transaction is extension of credit or the loaning of money or other transactions prescribed by regulations.

Land Registration Reform Act amendments

Notice to registered owner

Section 23 is amended to give the Director of Land Registration the power to send a notice to the owner when an electronic document that purports to effect a transfer or charge of land is delivered to the electronic land registration database by direct electronic transmission.

Suspending access to database

Section 23.1 is added to allow the Director of Land Registration to suspend authorization of an electronic document submitter when the filing is not authorized by the owner or by law, or when it is in the public interest.

Land Titles Act amendments

Compensation from Fund

Subsections 57 (4) and (5) are amended to let victims of fraud apply for compensation when they cannot recover compensation otherwise.

Rectification of register

Subsection 57 (13) is amended to provide the Director of Titles the power to make rectifications in the registry when fraud is committed or an error would deprive a person of land of which that person is legally in possession.

Offences

Section 156 is amended to increase penalties for persons convicted of an offence to \$50,000 or imprisonment for a term of not more than two years less a day, or both, if the person is an individual and to \$250,000 if the person is a corporation.

*Freedom of Information and Protection of Privacy Act amendments**Service provider organizations*

Section 65.1 governs how organizations which provide services to government must handle personal information collected.

Regulations

Section 60 is amended to give the Lieutenant Governor in Council the power to make regulations on procedures to follow in case of disclosure of personal information in contravention of the Act and the disposal of personal information.

1.3. British Columbia1.3.1. *Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165*

This statute limits the collection of personal information to what is minimally needed to conduct the transaction. By decreasing the number of records on file and their contents, this can reduce the risk of identity theft. The less information that is compromised, the more research an identity thief would have to do in order to use the information.

Purpose for which personal information may be collected

Section 26 limits what information can be collected by public bodies.

Protection of personal information

Section 30 imposes a duty to take reasonable security arrangements against risks such as unauthorized access, collection, use, disclosure or disposal.

1.3.2. *Business Practices and Consumer Protection Act, R.S.B.C. 2004, c. 2*

The provisions in this Act are not targeted at the prevention of identity theft but rather at its consequences for victims. Section 111 helps victims of identity theft explain to future credit grantors what happened to them. However, the reaction of credit grantors to such notices in credit reports is not clear. Also, the Act does not contain any provisions to limit a consumer's liability in case of loss or theft of credit cards.

Sections 114 and 116 offer protections against aggressive debt collectors. In order to invoke this provision, the consumer needs an affidavit or police report.

Explanation

Section 111 imposes a duty on credit reporting agencies to provide, in credit reports on an individual, any explanation or additional information relating to the information in the report that was provided to the credit reporting agency by the individual.

Harassment

Sections 114 and 116 prohibit debt collectors from harassing debtors and contacting them at their workplace.

1.3.3. *Vital Statistics Act, R.S.B.C. 1996, c. 479*

This Act does not make it an offence to fraudulently obtain a registration and certificate that can be used to commit fraud, but it does provide some protections. Sanctions can be imposed under section 49 only if the fraudster refuses to return the issued certificate. The registration and certificate can be cancelled, but in the absence of any sanctions for fraudsters, this Act cannot have an effective dissuasion effect.

Registrations fraudulently or improperly obtained

Section 28 gives the executive officer the power to cancel a registration if he or she is satisfied it was fraudulently or improperly obtained.

1.4. Alberta

1.4.1. *Personal Information Protection Act, S.A. 2003, c. P-6.5*

This Act replaces the provisions relating to the collection, use and disclosure of personal information in the *Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5* (PIPEDA).

The wording in this act suffers from vagueness. There is no clear limit on collection, use or disclosure; they only need to be “reasonable”. The same problem applies to the protection of information. It does not require specific safeguards such as the use of encryption when data is in transit and stored and access controls to limit access to a “need to know” basis. The Act does not contain any provisions to address situations where information is stolen, lost, or accessed by unauthorized persons.

Most organizations that want to collect more personal information than necessary for completing the transaction will be able to rely on section 7 (3). Consumers will be unaware that they can refuse to provide unnecessary personal information. In order for consumers to enforce the right not to disclose information, they would need to lodge a complaint with the Information and Privacy Commissioner, who can investigate and make orders requesting that the organization stop the practice. In reality, the time to complete this process will be quite long and consumers may in the end opt to give out the personal information in order to get the service or product.

Purpose

This Act governs the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of an individual to have his or her personal information protected and the need of organizations to collect, use or disclose personal information for purposes that are reasonable.

Consent required

Section 7 (2) limits the collection of personal information to that which is required to provide the product or service. Section 7 (3) lets consumers waive that right if there are reasonable terms acceptable to the individual.

Limitations on collection

Section 11 limits collection to purposes that are reasonable and limits the extent of the information that can be collected to what is reasonable to meet the purpose of the collection.

Limitations on use

Section 16 limits the use to purposes that are reasonable and limits the extent of the use to what is reasonable to meet the purpose of the use.

Limitations on disclosure

Section 19 limits the disclosure to purposes that are reasonable and limits the extent of the disclosure to what is reasonable to meet the purpose of the disclosure.

Protection of information

Section 34 imposes a duty to protect personal information, by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

1.4.2. Fair Trading Act, c. F-2

The provisions in this statute are not targeted at the prevention of identity theft but rather at its consequences for victims. Section 47 helps victims of identity theft explain to future credit grantors what happened to them. However, the obligation of credit grantors to respond to such notices in credit reports is not clear.

Section 89 limits the potential financial liability of victims. However, financial losses are not the only problem faced by victims.

Explanation by individual

Section 47 imposes a duty on credit reporting agencies to provide, in credit reports on an individual, any explanation or additional information that relates to the information in the report that was provided to the credit reporting agency by the individual.

Limitation of liability

Section 89 limits the liability of the debtor in case of loss or theft of a credit card. The liability is limited to \$50 before the issuer is notified and there is no liability once the issuer has been notified.

1.4.2.1. Fair Trading Act, Reg. 194/99 Collection and Debt Repayment Practices Regulation

Prohibited practices for collection agencies

Section 12 (k) imposes a duty on debt collectors to take all reasonable precautions to ensure that the person is in fact the debtor.

1.4.3. Debtors' Assistance Act, c. D-6

This Act establishes a Debtors' Assistance Board, with powers to provide service, advice and non-financial assistance to debtors who are unable to meet their liabilities.²⁰ However, it does not explicitly grant the director the power to help a person who has incurred loss as a result of the identity theft.

1.4.4. Freedom of Information and Protection of Privacy Act, R.S.A. 2000, c. F-25

The purposes of this statute are to give a right to control the use and disclosure of personal information held by a public body; offer a right of access to personal information held by public bodies and a right to correct personal information held by public bodies.

Limiting use and disclosure of personal information decreases the risk of identity theft.

²⁰ Alberta Government Services, *Legislation*, online:
<http://governmentservices.gov.ab.ca/index.cfm?fuseaction=legislation>.

Implementing adequate security measures can also significantly decrease the risk of personal information being compromised by insider abuse or by external threats such as crackers. However, the statute does not contain any provisions to address situations where information is stolen, lost, or accessed by unauthorized persons.

Protection of personal information

Section 38 imposes a duty to make reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.

Use of personal information

Section 39 limits how personal information may be used by a public body.

Disclosure of personal information

Section 40 imposes limits on disclosure of personal information by a public body.

1.4.4.1. Bill 20: Freedom of Information and Protection of Privacy Amendment Act, 20

This bill does not propose any changes to the provisions related to identity theft.

1.5. Quebec

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

This Act imposes duties on public bodies to track information exchanges between public bodies. Limiting information collection and access on a need to know basis, and the prompt destruction of information once its purpose is fulfilled, helps reduce the risk of identity theft. However, there is no duty to implement concrete measures to ensure that information is only accessed on a need to know basis. The Act does not contain any provisions to address situations where information is stolen, lost, or accessed by unauthorized persons.

It seems that the power to mandate appropriate security standards given in section 155 was never used to create regulations. There are no standards set out in regulations.

Unnecessary information

Section 64 limits the collection of information to what is necessary for the implementation of a program under its management.

Confidentiality

Sections 53 and 54 impose a duty to keep confidential “personal information” that includes information allowing a person to be identified. Section 59 imposes a duty to obtain the consent of the person concerned before releasing “personal information”.

Qualified person

Section 62 limits the availability of information to “qualified persons” or employees on a need to know basis.

Destruction

Section 73 imposes a duty to destroy personal information once the purpose for collection has been achieved.

Powers & Regulations

Sections 124 give the Commission the power to prescribe conditions respecting security measures to ensure confidentiality. Section 155 gives the power to make regulations fixing appropriate security standards to ensure confidentiality.

1.5.2. *An Act Respecting the Protection of Personal Information in the Private Sector, R.S.Q., c. P-39.1*

The object of this Act is to establish particular rules with respect to personal information relating to other persons, which a person collects, holds, uses or communicates to third persons in the course of carrying on an enterprise.

Limiting the collection, use and disclosure of personal information reduces the risk of identity theft. Requiring that organizations take appropriate security measures also reduces the risk of identity theft. However, as with PIPEDA and other provincial privacy protection laws, the Act does not contain any provisions requiring notification to the owner of personal information if the information is stolen, lost, or accessed by unauthorized persons.

Necessary information

Section 5 limits the collection to the information necessary for the object of the file.

Safety measures

Section 10 of the Act imposes a duty to take appropriate measures to ensure the confidentiality of the information.

Use of file

Section 12 limits the use of information to the purposes for which it was collected, unless the consent of the person concerned is obtained.

Consent

Section 13 limits disclosure to situations where consent for disclosure was given by the person concerned. Section 14 defines consent as being “manifest, free, and enlightened”, and it must be given for specific purposes.

1.5.3. Consumer Protection Act, R.S.Q., c. P-40.

This Act actually seems to facilitate identity theft. The exception to the rule that contracts must be signed can make it easier to obtain credit from stolen identities or from stolen pre-approved credit card offers. The limitations on liability do not reduce the risk of identity theft but do offer good protection to victims.

Credit cards

Section 29 adds an exception, for credit cards, to the principle that contracts must be in writing and signed by both parties on all pages. It’s sufficient for the merchant to issue the card and for the consumer to use it.

Liability limited

Sections 123 and 124 limit the financial liability of the card holder in case of loss or theft. The holder is not liable once he or she has notified the issuer of the loss of the card and liability is limited to \$50 if there is a failure to notify.

1.6. Manitoba1.6.1. Personal Investigations Act, C.C.S.M. c. P34*No divulging of contents of personal report*

Section 5 of the Act limits to whom and for what reasons a credit report on a consumer can be furnished.

Disclosure of personal file information

Section 8 provides consumers with the right to request a free copy of their credit report every six months.

Verification of information

Sections 8 and 11 give consumers the right to protest information in their credit files. It also imposes a duty on consumer reporting agencies and credit file users to investigate the protest.

Agreement not to disclose information void

Section 14 prohibits consumer reporting agencies and credit report users from entering into agreements where they would refuse to disclose information to an individual to whom it pertains.

Exemption from civil liability

Section 16 limits the liability of consumer reporting agencies toward consumers for incorrect information contained in their reports.

Void agreements

Section 18 prohibits any waiver or limitation of the rights given to consumers under this Act.

1.6.2. The Consumer Protection Act, C.C.S.M. c. C200

This Act protects debtors from aggressive debt collectors and provides protection in the event a credit card is lost or stolen. Making harassment of a debtor an offence helps reduce the potential suffering of victims of identity theft.

Imposing a duty on the card holder to notify the card issuer of unauthorized card use can make it harder for victims to escape liability when new credit card accounts are opened in their name by identity thieves. Sections 114 and 117 partially mitigate this problem.

Prohibitions

Section 98 imposes limits on collection agencies. In particular, section 98 (f) makes it an offence to harass a debtor.

Onus of proof

Section 114 sets the onus on the issuer to prove that an individual did request a credit card.

Liability for unauthorized use

Section 116 removes liability from a card holder for any debt incurred once the issuer is notified. This section also imposes a duty on a card holder to notify the card issuer of any unauthorized card use, within 30 days after receiving the statement containing the

unauthorized charge. A card holder can be liable for unauthorized use if he or she fails to notify the issuer. The liability for debt incurred before the issuer is notified is limited to \$50.

Onus of proof in disputes

Section 117 imposes the onus of proof on the card issuer when a dispute arises under section 116.

1.6.3. Bill 200 - *The Personal Information Protection and Identity Theft Prevention Act*

This bill passed the first reading December 8, 2005 and was recently reintroduced. The purpose is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of an individual to have his or her personal information protected and the need of organizations to collect, use or disclose personal information for purposes that are reasonable.

This bill proposes the “standard” obligations and restrictions on collection, use and disclosure of personal information. Nonetheless, it would introduce two novel items in terms of Canadian legislation, the duty to notify in the event of a security breach and a new right of action. The duty to notify would require organizations to inform individuals whose personal information was put at risk as the result of a security breach. The notification could significantly reduce the risk of identity theft following insider abuse or acquisition of information through cracking or other means.

A right of action would let victims recoup costs associated with re-establishing their identity, good name and credit rating and for other losses which result from the loss or theft of their identity following the failure of an organization to protect their information or warn them about a breach.

The benefit of this bill is that it would give individuals the opportunity to take action and mitigate the risk of identity theft. Without this crucial information, individuals might be faced with many identity theft threats without even realizing or ever learning about them. However, the bill does not define the “prescribed manner” in which organizations would give notice. Prompt notification is of paramount importance in order for individuals to be able to either close the window of opportunity available to the identity thief or limit damages by quickly discovering any abuse of their identity.

Consent required

Section 7 would limit collection of personal information to situations where the person has consented. Section 8 would limit consent to the uses for which the information was collected.

Limitations

Sections 11, 16 and 19 would limit the use, collection and disclosure to purposes that are reasonable.

Protection of information

Section 34 would impose a duty on organizations to make reasonable security arrangements against risks such as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

Notice if control of information lost

Section 34 would also impose a duty to notify the individual if his or her information is stolen, lost or accessed in an unauthorized manner. Furthermore, this section would introduce a cause of action in case of damages arising from the failure to protect information or failure to give a notice about the theft, loss or unauthorized access.

1.7. Saskatchewan**1.7.1. Credit Reporting Act, S.S. 2004, c. C-43.2**

This Act provides similar protections to consumers concerning their credit reports as are found in other provinces.

To whom credit reports may be provided

Section 17 of the Act limits to whom and for what reasons a credit report on a consumer can be furnished.

Disclosure to consumer by credit reporting agency

Section 21 provides consumers with the right to request a copy of their credit report from a consumer reporting agency.

Investigation by credit reporting agency

Section 24 gives consumers the right to dispute any information in their credit reports. It imposes an obligation on consumer reporting agencies to investigate any disputed information. This section also gives consumers the right to include an explanation of any disputed information in their credit reports. Consumer reporting agencies are required to transmit the explanations when providing the consumer's credit file.

Waiver of benefits ineffective; inclusion of certain clauses forbidden

Section 29 prohibits any waiver or limitation of the rights given to consumers under this Act.

1.7.2. The Consumer Protection Act, S.S. 1996, c. C-30.1

This Act does not contribute to the prevention of identity theft but, as with its counterparts in other provinces, it offers some protection from financial liability when identity thieves use the victim's personal information to obtain credit cards or take over accounts.

Limitation of liability for unauthorized use of credit card

Section 75.2 limits the liability of card holders for debt to \$50 before they notify the issuer of unauthorized use, loss or theft of the card. The liability is completely removed if the card issuer is notified within 30 days of receiving the first statement containing the unauthorized charges.

1.8. Nova Scotia

1.8.1. Consumer Reporting Act, R.S.N.S. 1989, c. 93

Confidentiality

Section 9 limits to whom and for what purposes credit reports may be furnished.

Consent and notice

Section 11 requires organizations to obtain the consent of the consumer before getting his or her credit report.

Disclosure

Section 12 imposes a duty on consumer reporting agencies to provide a free copy of an individual's credit file when the individual requests it in writing.

Protests

Section 13 gives consumers the right to protest information in their credit file. It also requires the consumer reporting agency to record the protest in the consumer's file and gives consumers the right to complain to the Director.

1.8.2. Consumer Protection Act, R.S. 1989, c. 9

Unlike its counterparts in other provinces, this statute does not contain any provisions related to identity theft.

1.8.3. Vital Statistics Act, R.S.N.S. 1989, c. 494

Similar to its federal counterpart, this statute criminalizes the obtaining of a birth certificate for fraudulent purposes. As such, it has the potential to dissuade identity thieves.

Penalty for obtaining certificate for improper purpose

Section 49A criminalizes the obtaining of a birth certificate, or a certified copy thereof, for a fraudulent or other improper purpose.

1.8.4. Personal Information International Disclosure Protection Act, S.N.S. 2006, c. 3

This Act received Royal Assent on July 14, 2006. Section 5 imposes a duty to store personal information in the custody of a public body only in Canada and to make it accessible only from Canada. Section 9 imposes a duty on public bodies to obtain consent, in writing, to disclose personal information in Canada or outside Canada.

1.9. New Brunswick

1.9.1. Collection Agencies Act, R.S.N.B. 1973, c. C-8

1.9.1.1. Collection Agencies Act, N.B. Reg. 84-256

While this Act does not contain any provisions that relate directly to identity theft, limiting the behaviour of debt collectors can reduce the impact of identity theft on victims.

Section 14 makes it an offence for debt collectors to use threatening, intimidating or coercive language and other intimidation or harassment techniques.

1.10. Prince Edward Island

1.10.1. Consumer Reporting Act, R.S.P.E.I. 1988, c. C-20

Providing information, conditions where permissible

Section 8 limits to whom and for what purposes credit reports may be furnished by consumer reporting agencies.

Consumer may request whether report made

Section 10 requires credit report users to obtain consent from the individual before obtaining his or her credit report.

Disclosure by consumer reporting agency

Section 11 requires consumer reporting agencies to furnish, free of cost, a copy of an individual's credit report upon receiving a request by the individual.

Disputing accuracy of information

Section 12 gives consumers the right to dispute information contained in their credit file. It also imposes an obligation on consumer reporting agencies to use their best endeavours to confirm or complete the information and gives consumers the right to complain to the Registrar.

1.10.2. Consumer Protection Act, R.S.P.E.I. 1988, c. C-19

Like its counterparts in other provinces, this Act does not contain any provisions that directly combat identity theft, though limiting the behaviour of debt collectors can reduce the impact of identity theft on victims. By contrast, however, the provision requiring that debt collectors be satisfied that the money is owed is weak. Most professional debt collectors will be satisfied with very little information and this statute does not require them to validate the information.

*Conduct of Creditors Regulations, P.E.I. Reg. EC578/83**Creditor conduct*

Section 2 imposes a duty on collectors to be satisfied that the money is owed by the borrower to the creditor. It also imposes limits on the techniques that can be used while collecting debts.

1.11. Newfoundland and Labrador1.11.1. Consumer Reporting Agencies Act, R.S.N.L. 1990, c. C-32*Disclosure of consumer report*

Section 19 limits to whom and for what purposes credit files can be disclosed by credit reporting agencies.

Personal information

Section 23 requires credit grantors to give notice in writing of their intention to obtain a credit report on an individual.

Disclosure of file to consumer

Section 24 requires consumer reporting agencies, upon request by the individual, to provide to the individual a copy of his or her credit report, free of charge.

1.11.2. Consumer Protection Act, R.S.N.L. 1990, c. C-3

Unlike most of its provincial counterparts, this Act does not contain any provisions related to identity theft.

2. STATUTE EXCERPTS

2.1. Federal Laws

2.1.1. Criminal Code, R.S.C., 1985, c. C-46

<p>Forgery of or uttering forged passport</p>	<p>57. (1) Every one who, while in or out of Canada,</p> <ul style="list-style-type: none"> (a) forges a passport, or (b) knowing that a passport is forged <ul style="list-style-type: none"> (i) uses, deals with or acts on it, or (ii) causes or attempts to cause any person to use, deal with or act on it, as if the passport were genuine, <p>is guilty of an indictable offence and liable to imprisonment for a term not exceeding fourteen years.</p>
<p>False statement in relation to passport</p>	<p>(2) Every one who, while in or out of Canada, for the purpose of procuring a passport for himself or any other person or for the purpose of procuring any material alteration or addition to any such passport, makes a written or an oral statement that he knows is false or misleading</p> <ul style="list-style-type: none"> (a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or (b) is guilty of an offence punishable on summary conviction.
<p>Possession of forged, etc., passport</p>	<p>(3) Every one who without lawful excuse, the proof of which lies on him, has in his possession a forged passport or a passport in respect of which an offence under subsection (2) has been committed is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.</p>
<p>Special provisions applicable</p>	<p>(4) For the purposes of proceedings under this section,</p> <ul style="list-style-type: none"> (a) the place where a passport was forged is not material; and (b) the definition “false document” in section 321, and section 366, apply with such modifications as the circumstances require.
<p>Definition of “passport”</p>	<p>(5) In this section, “passport” means a document issued by or under the authority of the Minister of Foreign Affairs for the purpose of identifying the holder thereof.</p>
<p>Jurisdiction</p>	<p>(6) Where a person is alleged to have committed, while out of Canada, an offence under this section, proceedings in respect of that</p>

offence may, whether or not that person is in Canada, be commenced in any territorial division in Canada and the accused may be tried and punished in respect of that offence in the same manner as if the offence had been committed in that territorial division.

Appearance of
accused at
trial

- (7) For greater certainty, the provisions of this Act relating to
- (a) requirements that an accused appear at and be present during proceedings, and
 - (b) the exceptions to those requirements,

apply to proceedings commenced in any territorial division pursuant to subsection (6).

R.S., 1985, c. C-46, s. 57; R.S., 1985, c. 27 (1st Supp.), s. 9; 1992, c. 1, s. 60(F); 1994, c. 44, s. 4; 1995, c. 5, s. 25.

Fraudulent use
of certificate
of citizenship

- 58.** (1) Every one who, while in or out of Canada,
- (a) uses a certificate of citizenship or a certificate of naturalization for a fraudulent purpose, or
 - (b) being a person to whom a certificate of citizenship or a certificate of naturalization has been granted, knowingly parts with the possession of that certificate with intent that it should be used for a fraudulent purpose,

is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years.

Definition of
“certificate of
citizenship”
and
“certificate of
naturalization”
Theft

- (2) In this section, “certificate of citizenship” and “certificate of naturalization”, respectively, mean a certificate of citizenship and a certificate of naturalization as defined by the *Citizenship Act*.

R.S., c. C-34, s. 59; 1974-75-76, c. 108, s. 41.

322. (1) Every one commits theft who fraudulently and without colour of right takes, or fraudulently and without colour of right converts to his use or to the use of another person, anything, whether animate or inanimate, with intent

- (a) to deprive, temporarily or absolutely, the owner of it, or a person who has a special property or interest in it, of the thing or of his property or interest in it;
- (b) to pledge it or deposit it as security;
- (c) to part with it under a condition with respect to its return that the person who parts with it may be unable to perform; or

(d) to deal with it in such a manner that it cannot be restored in the condition in which it was at the time it was taken or converted.

Time when theft completed

(2) A person commits theft when, with intent to steal anything, he moves it or causes it to move or to be moved, or begins to cause it to become movable.

Secrecy

(3) A taking or conversion of anything may be fraudulent notwithstanding that it is effected without secrecy or attempt at concealment.

Purpose of taking

(4) For the purposes of this Act, the question whether anything that is converted is taken for the purpose of conversion, or whether it is, at the time it is converted, in the lawful possession of the person who converts it is not material.

Wild living creature

(5) For the purposes of this section, a person who has a wild living creature in captivity shall be deemed to have a special property or interest in it while it is in captivity and after it has escaped from captivity.

R.S., c. C-34, s. 283.

Theft of telecommunication service

326. (1) Every one commits theft who fraudulently, maliciously, or without colour of right,

(a) abstracts, consumes or uses electricity or gas or causes it to be wasted or diverted; or

(b) uses any telecommunication facility or obtains any telecommunication service.

Definition of “telecommunication”

2) In this section and section 327, “telecommunication” means any transmission, emission or reception of signs, signals, writing, images or sounds or intelligence of any nature by wire, radio, visual or other electromagnetic system.

R.S., c. C-34, s. 287; 1974-75-76, c. 93, s. 23.

Possession of device to obtain telecommunication facility

327. (1) Every one who, without lawful excuse, the proof of which lies on him, manufactures, possesses, sells or offers for sale or distributes any instrument or device or any component thereof, the design of which renders it primarily useful for obtaining the use of any telecommunication facility or service, under circumstances that give rise

or service to a reasonable inference that the device has been used or is or was intended to be used to obtain the use of any telecommunication facility or service without payment of a lawful charge therefor, is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years.

Forfeiture (2) Where a person is convicted of an offence under subsection (1) or paragraph 326(1)(b), any instrument or device in relation to which the offence was committed or the possession of which constituted the offence, on such conviction, in addition to any punishment that is imposed, may be ordered forfeited to Her Majesty, whereupon it may be disposed of as the Attorney General directs.

Limitation (3) No order for forfeiture shall be made under subsection (2) in respect of telephone, telegraph or other communication facilities or equipment owned by a person engaged in providing telephone, telegraph or other communication service to the public or forming part of the telephone, telegraph or other communication service or system of such a person by means of which an offence under subsection (1) has been committed if such person was not a party to the offence.

1974-75-76, c. 93, s. 24.

Criminal breach of trust **336.** Every one who, being a trustee of anything for the use or benefit, whether in whole or in part, of another person, or for a public or charitable purpose, converts, with intent to defraud and in contravention of his trust, that thing or any part of it to a use that is not authorized by the trust is guilty of an indictable offence and liable to imprisonment for a term not exceeding fourteen years.

R.S., c. C-34, s. 296.

Theft, forgery, etc., of credit card **342.** (1) Every person who

- (a) steals a credit card,
- (b) forges or falsifies a credit card,
- (c) possesses, uses or traffics in a credit card or a forged or falsified credit card, knowing that it was obtained, made or altered
 - (i) by the commission in Canada of an offence, or
 - (ii) by an act or omission anywhere that, if it had occurred in Canada, would have constituted an offence, or
- (d) uses a credit card knowing that it has been revoked or cancelled, is

guilty of

(e) an indictable offence and is liable to imprisonment for a term not exceeding ten years, or

(f) an offence punishable on summary conviction.

Jurisdiction

(2) An accused who is charged with an offence under subsection (1) may be tried and punished by any court having jurisdiction to try that offence in the place where the offence is alleged to have been committed or in the place where the accused is found, is arrested or is in custody, but where the place where the accused is found, is arrested or is in custody is outside the province in which the offence is alleged to have been committed, no proceedings in respect of that offence shall be commenced in that place without the consent of the Attorney General of that province.

Unauthorized use of credit card data

(3) Every person who, fraudulently and without colour of right, possesses, uses, traffics in or permits another person to use credit card data, whether or not authentic, that would enable a person to use a credit card or to obtain the services that are provided by the issuer of a credit card to credit card holders is guilty of an indictable offence and is liable to imprisonment for a term not exceeding ten years; or

(a) an offence punishable on summary conviction.

Definition of “traffic”

(4) In this section, “traffic” means, in relation to a credit card or credit card data, to sell, export from or import into Canada, distribute or deal with in any other way.

R.S., 1985, c. C-46, s. 342; R.S., 1985, c. 27 (1st Supp.), ss. 44, 185(F); 1997, c. 18, s. 16.

Making, having or dealing in instruments for forging or falsifying credit cards

342.01 (1) Every person who, without lawful justification or excuse,

(a) makes or repairs,

(b) buys or sells,

(c) exports from or imports into Canada, or

(d) possesses

any instrument, device, apparatus, material or thing that the person knows has been used or knows is adapted or intended for use in forging or falsifying credit cards is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

Forfeiture	(2) Where a person is convicted of an offence under subsection (1), any instrument, device, apparatus, material or thing in relation to which the offence was committed or the possession of which constituted the offence may, in addition to any other punishment that may be imposed, be ordered forfeited to Her Majesty, whereupon it may be disposed of as the Attorney General directs.
Limitation	(3) No order of forfeiture may be made under subsection (2) in respect of any thing that is the property of a person who was not a party to the offence under subsection (1). 1997, c. 18, s. 17.
Unauthorized use of computer	<p>342.1 (1) Every one who, fraudulently and without colour of right, obtains, directly or indirectly, any computer service,</p> <p>(a) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system,</p> <p>(b) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or</p> <p>(c) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c)</p> <p>is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.</p>
Definitions	(2) In this section,
“computer password”	“computer password” means any data by which a computer service or computer system is capable of being obtained or used;
“computer program”	“computer program” means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;
“computer service”	“computer service” includes data processing and the storage or retrieval of data;

“computer system”	<p>“computer system” means a device that, or a group of interconnected or related devices one or more of which,</p> <ul style="list-style-type: none"> (a) contains computer programs or other data, and (b) pursuant to computer programs, <ul style="list-style-type: none"> (i) performs logic and control, and (ii) may perform any other function;
“data”	<p>“data” means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system;</p>
“electro-magnetic, acoustic, mechanical or other device”	<p>“electro-magnetic, acoustic, mechanical or other device” means any device or apparatus that is used or is capable of being used to intercept any function of a computer system, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing;</p>
“function”	<p>“function” includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer system;</p>
“intercept”	<p>“intercept” includes listen to or record a function of a computer system, or acquire the substance, meaning or purport thereof;</p>
“traffic”	<p>“traffic” means, in respect of a computer password, to sell, export from or import into Canada, distribute or deal with in any other way.</p> <p>R.S., 1985, c. 27 (1st Supp.), s. 45; 1997, c. 18, s. 18.</p>
Possession of device to obtain computer service	<p>342.2 (1) Every person who, without lawful justification or excuse, makes, possesses, sells, offers for sale or distributes any instrument or device or any component thereof, the design of which renders it primarily useful for committing an offence under section 342.1, under circumstances that give rise to a reasonable inference that the instrument, device or component has been used or is or was intended to be used to commit an offence contrary to that section,</p> <ul style="list-style-type: none"> (a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or (b) is guilty of an offence punishable on summary conviction.

Forfeiture

(2) Where a person is convicted of an offence under subsection (1), any instrument or device, in relation to which the offence was committed or the possession of which constituted the offence, may, in addition to any other punishment that may be imposed, be ordered forfeited to Her Majesty, whereupon it may be disposed of as the Attorney General directs.

Limitation

(3) No order of forfeiture may be made under subsection (2) in respect of any thing that is the property of a person who was not a party to the offence under subsection (1).

1997, c. 18, s. 19.

Possession of property obtained by crime

354. (1) Every one commits an offence who has in his possession any property or thing or any proceeds of any property or thing knowing that all or part of the property or thing or of the proceeds was obtained by or derived directly or indirectly from

(a) the commission in Canada of an offence punishable by indictment; or

(b) an act or omission anywhere that, if it had occurred in Canada, would have constituted an offence punishable by indictment.

Obliterated vehicle identification number

(2) In proceedings in respect of an offence under subsection (1), evidence that a person has in his possession a motor vehicle the vehicle identification number of which has been wholly or partially removed or obliterated or a part of a motor vehicle being a part bearing a vehicle identification number that has been wholly or partially removed or obliterated is, in the absence of any evidence to the contrary, proof that the motor vehicle or part, as the case may be, was obtained, and that such person had the motor vehicle or part, as the case may be, in his possession knowing that it was obtained,

(a) by the commission in Canada of an offence punishable by indictment; or

(b) by an act or omission anywhere that, if it had occurred in Canada, would have constituted an offence punishable by indictment.

Definition of “vehicle identification number”

(3) For the purposes of subsection (2), “vehicle identification number” means any number or other mark placed on a motor vehicle for the purpose of distinguishing the motor vehicle from other similar motor vehicles.

Exception

(4) A peace officer or a person acting under the direction of a peace officer is not guilty of an offence under this section by reason only that the

peace officer or person possesses property or a thing or the proceeds of property or a thing mentioned in subsection (1) for the purposes of an investigation or otherwise in the execution of the peace officer's duties.

R.S., 1985, c. C-46, s. 354; 1997, c. 18, s. 23.

Theft from
mail

356. (1) Every one who

(a) steals

(i) any thing sent by post, after it is deposited at a post office and before it is delivered,

(ii) a bag, sack or other container or covering in which mail is conveyed, whether or not it contains mail, or

(iii) a key suited to a lock adopted for use in the Canada Post Corporation, or

(b) has in his possession anything in respect of which he knows that an offence has been committed under paragraph (a),

is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years.

Allegation of
value not
necessary

(2) In proceedings for an offence under this section it is not necessary to allege in the indictment or to prove on the trial that anything in respect of which the offence was committed had any value.

R.S., c. C-34, s. 314; 1980-81-82-83, c. 54, s. 56.

False
pretence or
false
statement

362. (1) Every one commits an offence who

(a) by a false pretence, whether directly or through the medium of a contract obtained by a false pretence, obtains anything in respect of which the offence of theft may be committed or causes it to be delivered to another person;

(b) obtains credit by a false pretence or by fraud;

(c) knowingly makes or causes to be made, directly or indirectly, a false statement in writing with intent that it should be relied on, with respect to the financial condition or means or ability to pay of himself or herself or any person or organization that he or she is interested in or that he or she acts for, for the purpose of procuring, in any form whatever, whether for his or her benefit or the benefit of that person or organization

(i) the delivery of personal property,

(ii) the payment of money,

- (iii) the making of a loan,
- (iv) the grant or extension of credit,
- (v) the discount of an account receivable, or
- (vi) the making, accepting, discounting or endorsing of a bill of exchange, cheque, draft or promissory note; or

(d) knowing that a false statement in writing has been made with respect to the financial condition or means or ability to pay of himself or herself or another person or organization that he or she is interested in or that he or she acts for, procures on the faith of that statement, whether for his or her benefit or for the benefit of that person or organization, anything mentioned in subparagraphs (c)(i) to (vi).

Punishment

- (2) Every one who commits an offence under paragraph (1)(a)
- (a) is guilty of an indictable offence and liable to a term of imprisonment not exceeding ten years, where the property obtained is a testamentary instrument or the value of what is obtained exceeds five thousand dollars; or
 - (b) is guilty
 - (i) of an indictable offence and is liable to imprisonment for a term not exceeding two years, or
 - (ii) of an offence punishable on summary conviction, where the value of what is obtained does not exceed five thousand dollars.

Idem

(3) Every one who commits an offence under paragraph (1)(b), (c) or (d) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years.

Presumption from cheque issued without funds

(4) Where, in proceedings under paragraph (1)(a), it is shown that anything was obtained by the accused by means of a cheque that, when presented for payment within a reasonable time, was dishonoured on the ground that no funds or insufficient funds were on deposit to the credit of the accused in the bank or other institution on which the cheque was drawn, it shall be presumed to have been obtained by a false pretence, unless the court is satisfied by evidence that when the accused issued the cheque he believed on reasonable grounds that it would be honoured if presented for payment within a reasonable time after it was issued.

Definition of “cheque”	<p>(5) In this section, “cheque” includes, in addition to its ordinary meaning, a bill of exchange drawn on any institution that makes it a business practice to honour bills of exchange or any particular kind thereof drawn on it by depositors.</p> <p>R.S., 1985, c. C-46, s. 362; R.S., 1985, c. 27 (1st Supp.), s. 52; 1994, c. 44, s. 22; 2003, c. 21, s. 5.</p>
Forgery	<p>366. (1) Every one commits forgery who makes a false document, knowing it to be false, with intent</p> <p style="padding-left: 40px;">(a) that it should in any way be used or acted on as genuine, to the prejudice of any one whether within Canada or not; or</p> <p style="padding-left: 40px;">(b) that a person should be induced, by the belief that it is genuine, to do or to refrain from doing anything, whether within Canada or not.</p>
Making false document	<p>(2) Making a false document includes</p> <p style="padding-left: 40px;">(a) altering a genuine document in any material part;</p> <p style="padding-left: 40px;">(b) making a material addition to a genuine document or adding to it a false date, attestation, seal or other thing that is material; or</p> <p style="padding-left: 40px;">(c) making a material alteration in a genuine document by erasure, obliteration, removal or in any other way.</p>
When forgery complete	<p>(3) Forgery is complete as soon as a document is made with the knowledge and intent referred to in subsection (1), notwithstanding that the person who makes it does not intend that any particular person should use or act on it as genuine or be induced, by the belief that it is genuine, to do or refrain from doing anything.</p>
Forgery complete though document incomplete	<p>(4) Forgery is complete notwithstanding that the false document is incomplete or does not purport to be a document that is binding in law, if it is such as to indicate that it was intended to be acted on as genuine.</p> <p>R.S., c. C-34, s. 324.</p>
Uttering forged document	<p>368. (1) Every one who, knowing that a document is forged,</p> <p style="padding-left: 40px;">(a) uses, deals with or acts on it, or</p> <p style="padding-left: 40px;">(b) causes or attempts to cause any person to use, deal with or act on it, as if the document were genuine,</p>

- (c) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or
- (d) is guilty of an offence punishable on summary conviction.

Wherever forged

(2) For the purposes of proceedings under this section, the place where a document was forged is not material.

R.S., 1985, c. C-46, s. 368; 1992, c. 1, s. 60(F); 1997, c. 18, s. 25.

Counterfeiting stamp, etc.

376. (1) Every one who

- (a) fraudulently uses, mutilates, affixes, removes or counterfeits a stamp or part thereof,
- (b) knowingly and without lawful excuse, the proof of which lies on him, has in his possession
 - (i) a counterfeit stamp or a stamp that has been fraudulently mutilated, or
 - (ii) anything bearing a stamp of which a part has been fraudulently erased, removed or concealed, or
- (c) without lawful excuse, the proof of which lies on him, makes or knowingly has in his possession a die or instrument that is capable of making the impression of a stamp or part thereof, is guilty of an indictable offence and liable to imprisonment for a term not exceeding fourteen years.

Counterfeiting mark

(2) Every one who, without lawful authority,

- (a) makes a mark,
 - (b) sells, or exposes for sale, or has in his possession a counterfeit mark,
 - (c) affixes a mark to anything that is required by law to be marked, branded, sealed or wrapped other than the thing to which the mark was originally affixed or was intended to be affixed, or
 - (d) affixes a counterfeit mark to anything that is required by law to be marked, branded, sealed or wrapped,
- is guilty of an indictable offence and liable to imprisonment for a term not exceeding fourteen years.

Definitions

3) In this section,

“mark”
« marque »

“mark” means a mark, brand, seal, wrapper or design used by or on behalf of

(a) the government of Canada or a province,

(b) the government of a state other than Canada, or

(c) any department, board, commission or agent established by a government mentioned in paragraph (a) or (b) in connection with the service or business of that government;

“stamp”
« timbre »

“stamp” means an impressed or adhesive stamp used for the purpose of revenue by the government of Canada or a province or by the government of a state other than Canada.

R.S., c. C-34, s. 334.

Fraud

380. (1) Every one who, by deceit, falsehood or other fraudulent means, whether or not it is a false pretence within the meaning of this Act, defrauds the public or any person, whether ascertained or not, of any property, money or valuable security or any service,

(a) is guilty of an indictable offence and liable to a term of imprisonment not exceeding fourteen years, where the subject-matter of the offence is a testamentary instrument or the value of the subject-matter of the offence exceeds five thousand dollars; or

(b) is guilty

(i) of an indictable offence and is liable to imprisonment for a term not exceeding two years, or

(ii) of an offence punishable on summary conviction,

where the value of the subject-matter of the offence does not exceed five thousand dollars.

Affecting
public
market

(2) Every one who, by deceit, falsehood or other fraudulent means, whether or not it is a false pretence within the meaning of this Act, with intent to defraud, affects the public market price of stocks, shares, merchandise or anything that is offered for sale to the public is guilty of an indictable offence and liable to imprisonment for a term not exceeding fourteen years.

R.S., 1985, c. C-46, s. 380; R.S., 1985, c. 27 (1st Supp.), s. 54; 1994, c. 44, s. 25; 1997, c. 18, s. 26; 2004, c. 3, s. 2.

Personation
with intent

- 403.** Every one who fraudulently personates any person, living or dead,
- (a) with intent to gain advantage for himself or another person,
 - (b) with intent to obtain any property or an interest in any property, or
 - (c) with intent to cause disadvantage to the person whom he personates or another person,

is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years or an offence punishable on summary conviction.

R.S., 1985, c. C-46, s. 403; 1994, c. 44, s. 27.

Conspiracy

465. (1) Except where otherwise expressly provided by law, the following provisions apply in respect of conspiracy:

- (a) every one who conspires with any one to commit murder or to cause another person to be murdered, whether in Canada or not, is guilty of an indictable offence and liable to a maximum term of imprisonment for life;
- (b) every one who conspires with any one to prosecute a person for an alleged offence, knowing that he did not commit that offence, is guilty of an indictable offence and liable
 - (i) to imprisonment for a term not exceeding ten years, if the alleged offence is one for which, on conviction, that person would be liable to be sentenced to imprisonment for life or for a term not exceeding fourteen years, or
 - (ii) to imprisonment for a term not exceeding five years, if the alleged offence is one for which, on conviction, that person would be liable to imprisonment for less than fourteen years;
- (c) every one who conspires with any one to commit an indictable offence not provided for in paragraph (a) or (b) is guilty of an indictable offence and liable to the same punishment as that to which an accused who is guilty of that offence would, on conviction, be liable; and
- (d) every one who conspires with any one to commit an offence punishable on summary conviction is guilty of an offence punishable on summary conviction.

(2) [Repealed, 1985, c. 27 (1st Supp.), s. 61]

Conspiracy to commit offences	(3) Every one who, while in Canada, conspires with any one to do anything referred to in subsection (1) in a place outside Canada that is an offence under the laws of that place shall be deemed to have conspired to do that thing in Canada.
Idem	(4) Every one who, while in a place outside Canada, conspires with any one to do anything referred to in subsection (1) in Canada shall be deemed to have conspired in Canada to do that thing.
Jurisdiction	(5) Where a person is alleged to have conspired to do anything that is an offence by virtue of subsection (3) or (4), proceedings in respect of that offence may, whether or not that person is in Canada, be commenced in any territorial division in Canada, and the accused may be tried and punished in respect of that offence in the same manner as if the offence had been committed in that territorial division.
Appearance of accused at trial	(6) For greater certainty, the provisions of this Act relating to <ul style="list-style-type: none"> (a) requirements that an accused appear at and be present during proceedings, and (b) the exceptions to those requirements, apply to proceedings commenced in any territorial division pursuant to subsection (5).
Where previously tried outside Canada	(7) Where a person is alleged to have conspired to do anything that is an offence by virtue of subsection (3) or (4) and that person has been tried and dealt with outside Canada in respect of the offence in such a manner that, if the person had been tried and dealt with in Canada, he would be able to plead <i>autrefois acquit</i> , <i>autrefois convict</i> or pardon, the person shall be deemed to have been so tried and dealt with in Canada. R.S., 1985, c. C-46, s. 465; R.S., 1985, c. 27 (1st Supp.), s. 61; 1998, c. 35, s. 121.

2.1.2. Bill C-359 - An Act to amend the Criminal Code (personal identity theft)

Possession or transfer of identifying information	355.1 (1) Every one commits an offence who, without lawful excuse, has in his or her possession or transfers any information that can be used to identify a person other than him or her.
Possession and transfer of identity	(2) Every one commits an offence who, without lawful excuse, has in his or her possession or transfers a document appearing to be issued for the

documents purpose of identifying a person other than him or her, including a credit card, a birth certificate, a passport, a driver's licence or a health insurance card.

Punishment (3) Every one who commits an offence under subsection (1) or (2) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years.

2.1.3. Bill C-299 - An Act to amend the Criminal Code, the Canada Evidence Act and the Competition Act (personal information obtained by fraud)

Criminal Code

“personal information”

1. Section 2 of the Criminal Code is amended by adding the following in alphabetical order:

“personal information” has the same meaning as in subsection 2(1) of the Personal Information Protection and Electronic Documents Act;

2. (1) Subsection 362(1) of the Act is amended by striking out the word “or” at the end of paragraph (c) and by adding the following after paragraph (d):

(e) obtains personal information from a third party by a false pretence or by fraud;

(f) counsels another person to obtain personal information from a third party by a false pretence or by fraud; or

(g) sells or otherwise discloses personal information obtained from a third party by a false pretence or by fraud.

(2) Section 362 of the Act is amended by adding the following after subsection (3):

(3.1) Every one who commits an offence under paragraph (1)(e), (f) or (g)

(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or

(b) is guilty of an offence punishable on summary conviction.

3. Section 403 of the Act is amended by adding the following after paragraph (a):

(a.1) with intent to obtain any personal information about a third party,

Competition Act

“personal information”

5. Subsection 2(1) of the Competition Act is amended by adding the following in alphabetical order:

“personal information” has the same meaning as in subsection 2(1) of the *Personal Information Protection and Electronic Documents Act*;

7. Subsection 50(1) of the Act is amended by striking out the word “or” at the end of the paragraph (b), by adding the word “or” at the end of paragraph (c) and by adding the following after paragraph (c):

(d) seeks to obtain personal information from a third party by fraud, false pretence or fraudulent personation of any person, living or dead,(a.1) with intent to obtain any personal information about a third party,

2.1.4. *Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5*

Compliance with obligations

5. (1) Subject to sections 6 to 9, every organization shall comply with the obligations set out in Schedule 1.

Meaning of “should”

(2) The word “should”, when used in Schedule 1, indicates a recommendation and does not impose an obligation.

Appropriate purposes

(3) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

PIPEDA, Schedule 1:

Principle 4 — Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

4.4.1

Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Clause 4.8).

4.4.2

The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

4.4.3

This principle is linked closely to the Identifying Purposes principle (Clause 4.2) and the Consent principle (Clause 4.3).

Principle 5 — Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

4.5.1

Organizations using personal information for a new purpose shall document this purpose (see Clause 4.2.1).

4.5.2

Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

4.5.3

Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

4.5.4

This principle is closely linked to the Consent principle (Clause 4.3), the Identifying Purposes principle (Clause 4.2), and the Individual Access principle (Clause 4.9).

Principle 7 — Safeguards

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

4.7.1

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

4.7.2

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

4.7.3

The methods of protection should include

- (a) physical measures, for example, locked filing cabinets and restricted access to offices;
- (b) organizational measures, for example, security clearances and limiting access on a “need-to-know” basis; and
- (c) technological measures, for example, the use of passwords and encryption.

4.7.4

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

4.7.5

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

2.1.5. Privacy Act, R.S. 1985, c. P-21

Use of
personal
information

7. Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except

- (a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or
- (b) for a purpose for which the information may be disclosed to the institution under subsection 8(2).

1980-81-82-83, c. 111, Sch. II “7”.

Disclosure
of personal
information

8. (1) Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with this section.

Where
personal
information
may be
disclosed

(2) Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed

(a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose;

(b) for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure;

(c) for the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information;

(d) to the Attorney General of Canada for use in legal proceedings involving the Crown in right of Canada or the Government of Canada;

(e) to an investigative body specified in the regulations, on the written request of the body, for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation, if the request specifies the purpose and describes the information to be disclosed;

(f) under an agreement or arrangement between the Government of Canada or an institution thereof and the government of a province, the council of the Westbank First Nation, the government of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, for the purpose of administering or enforcing any law or carrying out a lawful investigation;

(g) to a member of Parliament for the purpose of assisting the individual to whom the information relates in resolving a problem;

(h) to officers or employees of the institution for internal audit purposes, or to the office of the Comptroller General or any other person or body specified in the regulations for audit purposes;

(i) to the Library and Archives of Canada for archival purposes;

(j) to any person or body for research or statistical purposes if the head of the government institution

(i) is satisfied that the purpose for which the information is

disclosed cannot reasonably be accomplished unless the information is provided in a form that would identify the individual to whom it relates, and

(ii) obtains from the person or body a written undertaking that no subsequent disclosure of the information will be made in a form that could reasonably be expected to identify the individual to whom it relates;

(k) to any aboriginal government, association of aboriginal people, Indian band, government institution or part thereof, or to any person acting on behalf of such government, association, band, institution or part thereof, for the purpose of researching or validating the claims, disputes or grievances of any of the aboriginal peoples of Canada;

(l) to any government institution for the purpose of locating an individual in order to collect a debt owing to Her Majesty in right of Canada by that individual or make a payment owing to that individual by Her Majesty in right of Canada; and

(m) for any purpose where, in the opinion of the head of the institution,

(i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or

(ii) disclosure would clearly benefit the individual to whom the information relates.

Personal information disclosed by Library and Archives of Canada

(3) Subject to any other Act of Parliament, personal information under the custody or control of the Library and Archives of Canada that has been transferred there by a government institution for historical or archival purposes may be disclosed in accordance with the regulations to any person or body for research or statistical purposes.

Copies of requests under paragraph (2)(e) to be retained

(4) The head of a government institution shall retain a copy of every request received by the government institution under paragraph (2)(e) for such period of time as may be prescribed by regulation, shall keep a record of any information disclosed pursuant to the request for such period of time as may be prescribed by regulation and shall, on the request of the Privacy Commissioner, make those copies and records available to the Privacy Commissioner.

Notice of disclosure under paragraph (2)(m)

(5) The head of a government institution shall notify the Privacy Commissioner in writing of any disclosure of personal information under paragraph (2)(m) prior to the disclosure where reasonably practicable or in any other case forthwith on the disclosure, and the Privacy Commissioner may, if the Commissioner deems it appropriate, notify the individual to

whom the information relates of the disclosure.

Definition of
“Indian
band”

- (6) In paragraph (2)(k), “Indian band” means
- (a) a band, as defined in the Indian Act;
 - (b) a band, as defined in the Cree-Naskapi (of Quebec) Act, chapter 18 of the Statutes of Canada, 1984;
 - (c) the Band, as defined in the Sechelt Indian Band Self-Government Act, chapter 27 of the Statutes of Canada, 1986; or
 - (d) a first nation named in Schedule II to the Yukon First Nations Self-Government Act.

Definition of
“aboriginal
government”

- (7) The expression “aboriginal government” in paragraph (2)(k) means
- (a) Nisga’a Government, as defined in the Nisga’a Final Agreement given effect by the Nisga’a Final Agreement Act;
 - (b) the council of the Westbank First Nation;
 - (c) the Tlicho Government, as defined in section 2 of the Tlicho Land Claims and Self-Government Act; or
 - (d) the Nunatsiavut Government, as defined in section 2 of the Labrador Inuit Land Claims Agreement Act.

Definition of
“council of
the
Westbank
First
Nation”

(8) The expression “council of the Westbank First Nation” in paragraphs (2)(f) and (7)(b) means the council, as defined in the Westbank First Nation Self-Government Agreement given effect by the Westbank First Nation Self-Government Act.

R.S., 1985, c. P-21, s. 8; R.S., 1985, c. 20 (2nd Supp.), s. 13, c. 1 (3rd Supp.), s. 12; 1994, c. 35, s. 39; 2000, c. 7, s. 26; 2004, c. 11, s. 37, c. 17, s. 18; 2005, c. 1, ss. 106, 109, c. 27, ss. 21, 25.

2.1.6. Employment Insurance Act, S.C. 1996, c. 23

Prohibitions

141. (1) No person

- (a) who has been assigned a Social Insurance Number shall knowingly make an application to be again assigned a Social Insurance Number, whether the person gives information that is the same as or different from that contained in their previous application on which the Social Insurance Number had been assigned;
- (b) shall, with intent to defraud or deceive any person, present, loan or use a Social Insurance Number or Social Insurance Number card;
- (c) shall, without the authority of the Commission, manufacture a

Social Insurance Number card or a substantially similar card, or duplicate a Social Insurance Number card, except by making a paper photocopy for record purposes only; or

(d) shall, without the authority of the Commission, sell a Social Insurance Number, a Social Insurance Number card or a substantially similar card.

Offence and punishment

(2) Every person who contravenes subsection (1) is guilty of an offence and liable on summary conviction to a fine of not more than \$1,000 or to imprisonment for a term of not more than one year, or to both.

2.1.7. Canada Post Corporation Act, R.S. 1985, c. C-10

Opening mail

48. Every person commits an offence who, except where expressly authorized by or under this Act, the Customs Act or the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, knowingly opens, keeps, secretes, delays or detains, or permits to be opened, kept, secreted, delayed or detained, any mail bag or mail or any receptacle or device authorized by the Corporation for the posting of mail.

R.S., 1985, c. C-10, s. 48; R.S., 1985, c. 1 (2nd Supp.), s. 172; 2000, c. 17, s. 88; 2001, c. 41, s. 79.

Abandonment of mail

49. Every person commits an offence who unlawfully and knowingly abandons, misdirects, obstructs, delays or detains the progress of any mail or mail conveyance.

1980-81-82-83, c. 54, s. 43.

2.2. Ontario

2.2.1. Consumer Reporting Act, R.S.O. 1990, c. C.33

Disclosure of report on request

10. (1) Every person shall, where requested by a consumer in writing or personally, inform the consumer whether or not a consumer report respecting him or her has been or is to be referred to in connection with any specified transaction or matter in which such person is engaged, and, if so, of the name and address of the consumer reporting agency supplying the report. R.S.O. 1990, c. C.33, s. 10 (1).

- Notice of intention to get consumer report
- (2) No person shall request or obtain a consumer report,
- (a) containing personal information about a consumer; or
- (b) on the basis that the person is considering extending credit to a consumer who has not, at the time of the request, made application for credit,
- unless that person first gives written notice of the fact to the consumer and, where the consumer so requests, informs the consumer of the name and address of the consumer reporting agency supplying the report. R.S.O. 1990, c. C.33, s. 10 (2).
- Idem
- (3) Where a person proposes to extend credit to a consumer and a consumer report containing credit information only is being or may be referred to in connection with the transaction, the person shall give notice of the fact to the consumer in writing at the time of the application for credit, or if the application is made orally, orally at the time of the application for credit. R.S.O. 1990, c. C.33, s. 10 (3).
- Assignee as creditor
- (4) Where, before extending credit, the proposed creditor obtains the acceptance or refusal of an assignment or proposed assignment of the credit transaction by an assignee or proposed assignee, subsection (3) applies to the assignee or proposed assignee in the same manner as to the person proposing to extend credit, but the giving of a notice under subsection (3) by a person proposing to extend credit or under this subsection by the person's assignee or proposed assignee shall be deemed to be sufficient notice by both. R.S.O. 1990, c. C.33, s. 10 (4).
- Limitation on divulgence of information
- (5) No person extending credit to a consumer shall divulge to other credit grantors or to a consumer reporting agency any personal information respecting the consumer except with the consent of the consumer or on the consumer's referral unless the person notifies the consumer in writing at the time of the application for credit that the person intends to do so. R.S.O. 1990, c. C.33, s. 10 (5).
- Form of notice
- (6) Any notice referred to in this section shall be clearly set forth in bold type or underlined and in letters not less than ten point in size. R.S.O. 1990, c. C.33, s. 10 (6).
- Adverse action
- (7) Where a benefit is denied to a consumer or a charge to a consumer is increased either wholly or partly because of information received from a consumer reporting agency or a person other than a consumer reporting agency, the user of such information shall deliver to the consumer at the time such action is communicated to the consumer notice of the fact and, upon the request of the consumer made within sixty days after such notice,

shall inform the consumer,

(a) of the nature and source of the information where the information is furnished by a person other than a consumer reporting agency; or

(b) of the name and address of the consumer reporting agency, where the information is furnished by a consumer reporting agency,

and the notice required to be given by the user under this subsection shall contain notice of the consumer's right to request the information referred to in clauses (a) and (b) and the time limited therefor. R.S.O. 1990, c. C.33, s. 10 (7).

Right of
consumer to
disclosure

12. (1) Every consumer reporting agency shall, at the written request of a consumer and during normal business hours, clearly and accurately disclose to the consumer, without charge,

(a) the nature and substance of all information in its files pertaining to the consumer at the time of the request;

(b) the sources of credit information;

(c) the name and, at the option of the consumer reporting agency, either the address or telephone number of every person on whose behalf the file has been accessed within the three-year period preceding the request;

(d) the names of the recipients of any consumer report pertaining to the consumer that it has furnished,

(i) containing personal information, within the one year period preceding the request, and

(ii) containing credit information, within the six month period preceding the request;

(e) copies of any written consumer report pertaining to the consumer made to any other person or, where the report was oral, particulars of the content of such oral report, furnished,

(i) where the report contains personal information, within the one year period preceding the request, and

(ii) where the report contains credit information, within the six month period preceding the request,

and shall inform the consumer of his or her right to protest any information contained in the file under sections 13 and 14 and the manner in which a protest may be made. R.S.O. 1990, c. C.33, s. 12 (1); 2000, c. 26, Sched. B, s. 8 (2).

Exception for certain medical information	(2) A consumer reporting agency shall withhold from the disclosures required by subsection (1) any medical information obtained with the written consent of the consumer which the consumer's own physician has specifically requested in writing be withheld from the consumer in his or her own best interest. R.S.O. 1990, c. C.33, s. 12 (2).
Method of disclosure	(3) The disclosures required under this section shall be made to the consumer, <ul style="list-style-type: none"> (a) in person if he or she appears in person and furnishes proper identification; (b) by telephone if he or she has made a written request, with sufficient identification, for telephone disclosure and the toll charge, if any, for the telephone call is prepaid by or charged directly to the consumer. R.S.O. 1990, c. C.33, s. 12 (3).
Idem	(4) Every consumer reporting agency shall provide trained personnel to explain to the consumer any information furnished to him or her under this section. R.S.O. 1990, c. C.33, s. 12 (4).
Consumer's adviser	(5) The consumer shall be permitted to be accompanied by one other person of his or her choosing to whom the consumer reporting agency may be required by the consumer to disclose his or her file. R.S.O. 1990, c. C.33, s. 12 (5); 1993, c. 27, Sched.
Abstract	(6) At the request of the consumer, the consumer reporting agency shall give the consumer a copy of the information required to be disclosed under this section. 1994, c. 27, s. 77.
Plain language	(6.1) The copy of the information given to the consumer must be in writing and easily readable and the information must be in understandable language. 1994, c. 27, s. 77.
Identification	(7) A consumer reporting agency shall require reasonable identification of the consumer and a person accompanying him or her before making disclosures under this section. R.S.O. 1990, c. C.33, s. 12 (7).
No conditions	(8) A consumer reporting agency shall not require a consumer to give any undertaking or waive or release any right as a condition precedent to access to his or her file under this section. R.S.O. 1990, c. C.33, s. 12 (8).

2.2.2. Bill 174 - Consumer Reporting Amendment Act, 2005

Collection,
storage and
disclosure
of
information
in files

(5) For the purpose of ensuring accuracy and fairness as described in subsection (1) and, in addition, for the purpose of ensuring privacy, integrity and confidentiality with respect to the information in its reports, every consumer reporting agency shall adopt all procedures that are reasonable, including,

[...]

c) ensuring that electronic signature certificates originate from a certification authority approved by the federal Communications Security Establishment with a registered object identifier number issued by Public Works and Government Services Canada and that,

(i) all personal or credit information is adequately secured with encryption mechanisms to prevent inadvertent disclosure,

[...]

Supplying
list of
names

(1) No person shall supply a list of names and criteria to a consumer reporting agency in order to obtain an indication of the names of the persons named in the list who meet the criteria unless,

(a) the person first notifies in writing each person named on the list or about whom information is being obtained that such a list is being submitted or that information is being requested; and

(b) the person provides the name and address of the consumer reporting agency involved.

Duty to
inform
consumer
of unlawful
disclosure

12.1 Every consumer reporting agency shall, immediately on discovering that any of a consumer's information has been unlawfully disclosed, inform the consumer of the disclosure.

2.2.3. Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sch. A

Security

12. (1) A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal. 2004, c. 3, Sched. A, s. 12 (1).

Notice of
loss, etc.

(2) Subject to subsection (3) and subject to the exceptions and additional requirements, if any, that are prescribed, a health information custodian

that has custody or control of personal health information about an individual shall notify the individual at the first reasonable opportunity if the information is stolen, lost, or accessed by unauthorized persons. 2004, c. 3, Sched. A, s. 12 (2).

Exception

(3) If the health information custodian is a researcher who has received the personal health information from another health information custodian under subsection 44 (1), the researcher shall not notify the individual that the information is stolen, lost or accessed by unauthorized persons unless the health information custodian under that subsection first obtains the individual's consent to having the researcher contact the individual and informs the researcher that the individual has given the consent. 2004, c. 3, Sched. A, s. 12 (3).

Identity of individual

54. (9) A health information custodian shall not make a record of personal health information or a part of it available to an individual under this Part or provide a copy of it to an individual under clause (1) (a) without first taking reasonable steps to be satisfied as to the individual's identity. 2004, c. 3, Sched. A, s. 54 (9).

2.2.4. Trespass to Property Act, R.S.O. 1990, c. T.21

Trespass an offence

2. (1) Every person who is not acting under a right or authority conferred by law and who,

(a) without the express permission of the occupier, the proof of which rests on the defendant,

(i) enters on premises when entry is prohibited under this Act, or

(ii) engages in an activity on premises when the activity is prohibited under this Act; or

(b) does not leave the premises immediately after he or she is directed to do so by the occupier of the premises or a person authorized by the occupier,

is guilty of an offence and on conviction is liable to a fine of not more than \$2,000. R.S.O. 1990, c. T.21, s. 2 (1).

Colour of right as a defence

(2) It is a defence to a charge under subsection (1) in respect of premises that is land that the person charged reasonably believed that he or she had title to or an interest in the land that entitled him or her to do the act complained of. R.S.O. 1990, c. T.21, s. 2 (2).

Method of giving notice	<p>5. (1) A notice under this Act may be given,</p> <p>(a) orally or in writing;</p> <p>(b) by means of signs posted so that a sign is clearly visible in daylight under normal conditions from the approach to each ordinary point of access to the premises to which it applies; or</p> <p>(c) by means of the marking system set out in section 7. R.S.O. 1990, c. T.21, s. 5 (1).</p>
Substantial compliance	<p>(2) Substantial compliance with clause (1) (b) or (c) is sufficient notice. R.S.O. 1990, c. T.21, s. 5 (2).</p>
Arrest without warrant on premises	<p>9. (1) A police officer, or the occupier of premises, or a person authorized by the occupier may arrest without warrant any person he or she believes on reasonable and probable grounds to be on the premises in contravention of section 2. R.S.O. 1990, c. T.21, s. 9 (1).</p>
Delivery to police officer	<p>(2) Where the person who makes an arrest under subsection (1) is not a police officer, he or she shall promptly call for the assistance of a police officer and give the person arrested into the custody of the police officer. R.S.O. 1990, c. T.21, s. 9 (2).</p>
Deemed arrest	<p>(3) A police officer to whom the custody of a person is given under subsection (2) shall be deemed to have arrested the person for the purposes of the provisions of the Provincial Offences Act applying to his or her release or continued detention and bail. R.S.O. 1990, c. T.21, s. 9 (3).</p>

2.2.5. Consumer Protection Act, S.O. 2002, c. 30, Sch. A

Limiting liability for unauthorized charges	<p>69. A borrower is not liable for any amount that is greater than the prescribed maximum for unauthorized charges under a credit agreement for open credit. 2004, c. 19, s. 7 (18).</p>
---	--

2.2.6. Mortgage Brokers Act, R.S.O. 1990, c. M.39

Offences	<p>31. (1) Every person who, knowingly,</p> <p>(a) furnishes false information in any application under this Act or in any statement or return required to be furnished under this Act or the regulations;</p> <p>(b) fails to comply with any order, direction or other requirement</p>
----------	---

made under this Act; or

(c) contravenes any provision of this Act or the regulations,

and every director or officer of a corporation who knowingly concurs in such furnishing, failure or contravention is guilty of an offence and on conviction is liable to a fine of not more than \$100,000 or to imprisonment for a term of not more than one year, or to both.

Corporations

(2) Where a corporation is convicted of an offence under subsection (1), the maximum penalty that may be imposed upon the corporation is \$200,000 and not as provided therein. R.S.O. 1990, c. M.39, s. 31 (1, 2).

(3) Repealed: 1997, c. 28, s. 184.

Limitation

(4) No proceeding under clause (1) (a) shall be commenced more than one year after the facts upon which the proceeding is based first came to the knowledge of the Superintendent. R.S.O. 1990, c. M.39, s. 31 (4); 1997, c. 28, s. 172 (1).

Limitation

(5) No proceeding under clause (1) (b) or (c) shall be commenced more than two years after the facts upon which the proceeding is based first came to the knowledge of the Superintendent. 1997, c. 19, s. 15 (5); 1997, c. 28, s. 172 (1).

2.2.7. Vital Statistics Act, R.S.O. 1990, c. V.4

Duties of division registrar

39. The division registrar shall,

(a) receive and sign statements and registrations and issue burial permits;

(b) supply, free of charge, any prescribed form required by any person in order to comply with this Act;

(c) keep all registrations, records, notices and documents received by him or her in a place of safety;

(d) use all available means to obtain the necessary information for the purpose of completing the registrations required to be made by him or her;

(e) inform the proper person of the duty to furnish him or her with particulars for the registration of a birth, death or still-birth if the division registrar has reason to believe that any has taken place within his or her division and has not been registered, and, on the failure of the person to make the registration within seven days, supply to the Registrar General such information as the division registrar possesses

regarding the failure of any person to furnish the required particulars;

- (f) examine every statement of birth, death or still-birth in order to ascertain whether or not it has been completed in the prescribed form;
- (g) ensure that every registration of birth, death or still-birth has been written legibly in durable ink;
- (h) refuse to accept any statement that does not contain all the items of information required therein unless he or she has received a satisfactory explanation for the omission;
- (i) call attention to any errors in a statement of personal particulars or medical certificate of death that is incomplete or unsatisfactory, and withhold the issuance of the acknowledgment of registration of death and the burial permit until the errors have been corrected;
- (j) sign every registration as division registrar in attestation of the date of registration in his or her office;
- (k) number consecutively the registrations of births, deaths and still-births in separate series, beginning with the number “1” for the first registration of a birth, death or still-birth in each calendar year;
- (l) transmit to the Registrar General as required by the regulations the registration of every birth, death or still-birth made by him or her;
- (m) report the fact to the Registrar General, in the prescribed form, if no birth, death or still-birth has been registered;
- (n) keep such records as may be prescribed by the regulations;
- (o) transmit to the proper division registrar within forty-eight hours every statement of birth received by the division registrar that did not occur within his or her registration division; and
- (p) transmit to the proper division registrar within forty-eight hours notice of every registration of death or still-birth made by him or her that did not occur within his or her registration division. R.S.O. 1990, c. V.4, s. 39; 1993, c. 27, Sched.

Duty to
report lost
documents

51.1 (1) A person who has lost or had stolen or destroyed a certificate or certified copy of a birth registration or such other registrations as may be prescribed shall notify the Registrar General of the loss, theft or destruction, as the case may be, immediately upon becoming aware of it. 2001, c. 21, s. 9.

Duty to
return
found
documents

(2) A person who finds a certificate or certified copy of a birth registration or such other registrations as may be prescribed shall notify the Registrar General of the find within 24 hours of finding it and shall forthwith forward the certificate or certified copy to the Registrar General.

2001, c. 21, s. 9.

Exception

(3) Subsection (2) does not apply to a person who forthwith delivers the found certificate or certified copy to the police or to a lost and found service. 2001, c. 21, s. 9.

Duty of police or lost and found

(4) If the police or a lost and found service receives a certificate or certified copy of a registration that is believed to have been lost and that is not claimed within 24 hours of receiving it, the police or the operator of a lost and found service, as the case may be, shall notify the Registrar General of the receipt. 2001, c. 21, s. 9.

Return of documents

(5) If a certificate or certified copy of a registration that has been lost is claimed from the police or a lost and found service within 24 hours of their having received it, they may return it. 2001, c. 21, s. 9.

Duty to return document

(6) In returning a document as authorized by subsection (5), the police or lost and found service shall take reasonable precautions to ensure that it is returned only to the person entitled to have it and if it is not claimed by such a person, they shall forward it to the Registrar General not later than 90 days after receiving it. 2001, c. 21, s. 9.

False information

56. (1) Every person who wilfully makes or causes to be made a false statement in any notice, registration, statement, certificate, return or other document respecting any particulars required to be furnished under this Act is guilty of an offence and on conviction is liable, in the case of an individual, to a fine of not more than \$50,000 or to imprisonment for a term of not more than two years less a day, or to both, and, in the case of a corporation, to a fine of not more than \$250,000. 2001, c. 21, s. 14.

Same

(2) Every legally qualified medical practitioner who wilfully makes a false statement as to the cause of the death of any person, or represents himself or herself as having been in attendance during the last illness of any person when in fact he or she was not called in attendance until after the death, is, in addition to any penalty imposed by this Act, subject to discipline by the Council of the College of Physicians and Surgeons of Ontario. 2001, c. 21, s. 14.

Same

(3) Every person who wilfully makes or causes to be made a registration of a birth, marriage, death or still-birth as having occurred in Ontario in respect of any person whose birth, marriage, death or still-birth did not occur in Ontario is guilty of an offence and on conviction is liable, in the case of an individual, to a fine of not more than \$50,000 or to imprisonment for a term of not more than two years less a day, or to both, and, in the case of a corporation, to a fine of not more than \$250,000. 2001, c. 21, s. 14.

2.2.8. Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31Personal
privacy

- 21.** (1) A head shall refuse to disclose personal information to any person other than the individual to whom the information relates except,
- (a) upon the prior written request or consent of the individual, if the record is one to which the individual is entitled to have access;
 - (b) in compelling circumstances affecting the health or safety of an individual, if upon disclosure notification thereof is mailed to the last known address of the individual to whom the information relates;
 - (c) personal information collected and maintained specifically for the purpose of creating a record available to the general public;
 - (d) under an Act of Ontario or Canada that expressly authorizes the disclosure;
 - (e) for a research purpose if,
 - (i) the disclosure is consistent with the conditions or reasonable expectations of disclosure under which the personal information was provided, collected or obtained,
 - (ii) the research purpose for which the disclosure is to be made cannot be reasonably accomplished unless the information is provided in individually identifiable form, and
 - (iii) the person who is to receive the record has agreed to comply with the conditions relating to security and confidentiality prescribed by the regulations; or
 - (f) if the disclosure does not constitute an unjustified invasion of personal privacy. R.S.O. 1990, c. F.31, s. 21 (1).

and every director or officer of a corporation who knowingly concurs in such furnishing, failure or contravention is guilty of an offence and on conviction is liable to a fine of not more than \$100,000 or to imprisonment for a term of not more than one year, or to both.

Criteria re
invasion of
privacy

- (2) A head, in determining whether a disclosure of personal information constitutes an unjustified invasion of personal privacy, shall consider all the relevant circumstances, including whether,
- (a) upon the prior written request or consent of the individual, if the record is one to which the individual is entitled to have access;
 - (b) access to the personal information may promote public health and safety;
 - (c) access to the personal information will promote informed choice in the purchase of goods and services;

- (d) the personal information is relevant to a fair determination of rights affecting the person who made the request;
- (e) the individual to whom the information relates will be exposed unfairly to pecuniary or other harm;
- (f) the personal information is highly sensitive;
- (g) the personal information is unlikely to be accurate or reliable;
- (h) the personal information has been supplied by the individual to whom the information relates in confidence; and
- (i) the disclosure may unfairly damage the reputation of any person referred to in the record. R.S.O. 1990, c. F.31, s. 21 (2).

Presumed
invasion of
privacy

- (3) A disclosure of personal information is presumed to constitute an unjustified invasion of personal privacy where the personal information,
 - (a) relates to a medical, psychiatric or psychological history, diagnosis, condition, treatment or evaluation;
 - (b) was compiled and is identifiable as part of an investigation into a possible violation of law, except to the extent that disclosure is necessary to prosecute the violation or to continue the investigation;
 - (c) relates to eligibility for social service or welfare benefits or to the determination of benefit levels;
 - (d) relates to employment or educational history;
 - (e) was obtained on a tax return or gathered for the purpose of collecting a tax;
 - (f) describes an individual's finances, income, assets, liabilities, net worth, bank balances, financial history or activities, or creditworthiness;
 - (g) consists of personal recommendations or evaluations, character references or personnel evaluations; or
 - (h) indicates the individual's racial or ethnic origin, sexual orientation or religious or political beliefs or associations. R.S.O. 1990, c. F.31, s. 21 (3).

Limitation

- (4) Despite subsection (3), a disclosure does not constitute an unjustified invasion of personal privacy if it,
 - (a) discloses the classification, salary range and benefits, or employment responsibilities of an individual who is or was an officer or employee of an institution or a member of the staff of a minister;
 - (b) discloses financial or other details of a contract for personal

services between an individual and an institution; or

(c) discloses details of a licence or permit or a similar discretionary financial benefit conferred on an individual by an institution or a head under circumstances where,

(i) the individual represents 1 per cent or more of all persons and organizations in Ontario receiving a similar benefit, and

(ii) the value of the benefit to the individual represents 1 per cent or more of the total value of similar benefits provided to other persons and organizations in Ontario. R.S.O. 1990, c. F.31, s. 21 (4).

Refusal to
confirm or
deny
existence of
record

(5) A head may refuse to confirm or deny the existence of a record if disclosure of the record would constitute an unjustified invasion of personal privacy. R.S.O. 1990, c. F.31, s. 21 (5).

Regulations

- 60.** (1) The Lieutenant Governor in Council may make regulations,
- (0.a) prescribing standards for determining what constitutes reasonable grounds for a head to conclude that a request for access to a record is frivolous or vexatious;
 - (a) respecting the procedures for access to original records under section 30;
 - (b) respecting the procedures for access to personal information under subsection 48 (3);
 - (c) prescribing the circumstances under which records capable of being produced from machine readable records are not included in the definition of “record” for the purposes of this Act;
 - (d) setting standards for and requiring administrative, technical and physical safeguards to ensure the security and confidentiality of records and personal information under the control of institutions;
 - (e) setting standards for the accuracy and completeness of personal information that is under the control of an institution;
 - (f) prescribing time periods for the purposes of subsection 40 (1);
 - (g) prescribing the amount, the manner of payment and the manner of allocation of fees described in clause 24 (1) (c) or 48 (1) (c), subsection 50 (1.1) or section 57 and the times at which they are required to be paid;
 - (h) prescribing matters to be considered in determining whether to

waive all or part of the costs required under section 57;

- (i) designating any agency, board, commission, corporation or other body as an institution and designating a head for each such institution;
- (j) prescribing conditions relating to the security and confidentiality of records used for a research purpose;
- (k) prescribing forms and providing for their use;
- (l) respecting any matter the Lieutenant Governor in Council considers necessary to carry out effectively the purposes of this Act. R.S.O. 1990, c. F.31, s. 60; 1996, c. 1, Sched. K, s. 12 (1, 2).

2.2.9. Freedom of Information and Protection of Privacy Act - R.R.O. 1990, Reg. 460

4. (1) Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected. R.R.O. 1990, Reg. 460, s. 4 (1).

(2) Every head shall ensure that only those individuals who need a record for the performance of their duties shall have access to it. R.R.O. 1990, Reg. 460, s. 4 (2).

(3) Every head shall ensure that reasonable measures to protect the records in his or her institution from inadvertent destruction or damage are defined, documented and put in place, taking into account the nature of the records to be protected. R.R.O. 1990, Reg. 460, s. 4 (3).

2.2.10. Collection Agencies Act, R.R.O. 1990, Reg. 74

20. No collection agency or collector shall,

- (a) attempt to collect payment of a debt from a debtor unless the collection agency or the collector has notified or has attempted to notify the debtor in writing by letter addressed to the debtor's last known address that the collection agency or collector has been engaged by the creditor to act in respect of the collection of the debt;
- (b) commence a legal proceeding with respect to the collection of a debt, or recommend to a creditor that a legal proceeding be commenced with respect to the collection of a debt, unless the collection agency or collector first gives notice to the debtor that the collection agency or the collector intends to commence the proceeding or recommend that a proceeding be commenced, as the case may be;
- (c) directly or indirectly threaten or state an intention to proceed with any action for which the collection agency or the collector does not

have lawful authority;

(d) make telephone calls or personal calls of such nature or with such frequency as to constitute harassment of the debtor, his or her spouse or any member of the debtor's family or household;

(e) make a telephone call or personal call for the purpose of demanding payment of a debt,

(i) on a Sunday, or

(ii) on a statutory holiday,

or on any other day except between the hours of 7 o'clock in the forenoon and 9 o'clock in the afternoon;

(f) give any person, directly or indirectly, by implication or otherwise, any false or misleading information that may be detrimental to a debtor, his or her spouse or any member of the debtor's family;

(g) make a demand by telephone, by personal call or by writing for payment of a debt without indicating the name of the creditor, the balance of the moneys owing and the identity and authority of the person making the demand;

(h) where a person has informed the collection agency or the collector that the person is not in fact the debtor, continue to communicate with that person in respect of the collection of the debt unless the collection agency or the collector first takes all reasonable precautions to ensure that the person is in fact the debtor;

(i) commence or continue a court action in the name of the collection agency or collector for the recovery of the debt of a client unless the debt has been assigned to the collection agency or collector, as the case may be, in good faith by instrument in writing for valuable consideration and notice of such assignment has been given to the debtor; or

(j) commence a court action for the collection of the debt of a client in the name of the client unless the collection agency or collector has received express written authority from the client to commence such action. R.R.O. 1990, Reg. 74, s. 20; O. Reg. 42/00, s. 2; O. Reg. 299/05, s. 3.

2.2.11. Highway Traffic Act, R.S.O. 1990, c. H.8

Displaying
licence that
has been
suspended,
altered, etc

35. (1) No person shall,

(a) 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;

(b) display or cause or permit to be displayed or have in his or her possession a cancelled, revoked or suspended driver's licence other than a Photo Card portion thereof;

(c) lend his or her driver's licence or any portion thereof or permit the use of it by another person;

(d) display or represent as his or her own a driver's licence not issued to him or her;

(e) apply for, secure or retain in his or her possession more than one driver's licence; or

(f) fail to surrender to the Ministry upon its demand a driver's licence that has been suspended, revoked or cancelled. R.S.O. 1990, c. H.8, s. 35 (1); 2005, c. 26, Sched. A, s. 3 (1).

2.2.12. Bill 152 - An Act to modernize various Acts administered by or affecting the Ministry of Government Services

CONSUMER REPORTING ACT

(5) The Act is amended by adding the following section:

Alert to verify identity of consumer

12.1 (1) A consumer may require a consumer reporting agency to include, in the consumer's file, an alert warning persons to verify the identity of any person purporting to be the consumer.

Consumer must provide contact information

(2) A consumer who requires a consumer reporting agency to include an alert in the consumer's file shall provide, for inclusion in the alert, a telephone number or other method, prescribed by the regulations, of contacting the consumer to verify the identity of any person purporting to be the consumer.

Time limit for including alert in file

(3) The consumer reporting agency shall include the alert in the consumer's file as soon as practicable after being required to do so under subsection (1).

No obligation if contact information not provided	(4) The consumer reporting agency is not required to include an alert if the consumer has not complied with subsection (2).
Amendment or removal	(5) The consumer may require the consumer reporting agency to amend the alert or remove it from the consumer's file.
Time limit for amendment or removal	(6) The consumer reporting agency shall amend the alert or remove it from the consumer's file as soon as practicable after being required to do so under subsection (5).
Verification of identity by agency	(7) Before including an alert in a consumer's file or amending or removing such an alert, the consumer reporting agency shall take reasonable steps to verify that the person requiring the inclusion, amendment or removal is the consumer.
Expiry	(8) An alert expires at the end of the prescribed period, if any.
Information about expiry	(9) When a consumer reporting agency includes an alert in a consumer's file, the agency shall inform the consumer of the date, if any, that the alert will expire under subsection (8).
Fees	(10) Subject to the regulations, a consumer reporting agency may require a fee to be paid before including an alert in a consumer's file, or amending or removing an alert.
	(6) The Act is amended by adding the following section:
When alert to be given	12.2 If a consumer's file includes an alert under section 12.1 that has not expired, the consumer reporting agency shall give the alert to every person to whom any information from the file is disclosed.
	(7) The Act is amended by adding the following section:
If person receives an alert	12.3 (1) This section applies if a person receives an alert from a consumer's file under section 12.2 in connection with a transaction, described in subsection (3), involving a person purporting to be the consumer.
Duty to verify identity	(2) The person who received the alert shall not proceed with the transaction without taking reasonable steps to verify that the person involved in the transaction is the consumer.

Transactions covered	<p>(3) A transaction referred to in subsection (1) is,</p> <p>(a) the extension of credit or the loaning of money, as defined in the regulations; or</p> <p>(b) any other transaction prescribed by the regulations.</p>
Exception for transactions covered	<p>(4) Clause (3) (a) does not include an advance under a credit agreement for open credit unless the credit agreement is amended to provide for the advance.</p>
Definitions	<p>(5) In subsection (4),</p> <p>“credit agreement” means a credit agreement as defined in section 66 of the <i>Consumer Protection Act, 2002</i>; (“convention de crédit”)</p> <p>“open credit” means open credit as defined in section 1 of the <i>Consumer Protection Act, 2002</i>. (“crédit en blanc”)</p>

LAND REGISTRATION REFORM ACT

(3) Section 23 of the Act is amended by adding the following subsection:

Notice to registered owner	<p>(4) When an electronic document that purports to effect a transfer or charge of land is delivered to the electronic land registration database by direct electronic transmission, the Director of Land Registration may have a notice of the delivery issued to the registered owner of the land by the means that Director specifies.</p>
----------------------------	---

(4) The Act is amended by adding the following sections:

Suspending access to database	<p>23.1 (1) The Director of Land Registration may, by order, immediately suspend the authorization of an electronic document submitter if he or she,</p> <p>(a) has reasonable grounds to believe that the submitter has submitted an electronic document that,</p> <p style="padding-left: 40px;">(i) is not authorized by the registered owner of the land affected by the document or the holder of a registered interest in the land, or</p> <p style="padding-left: 40px;">(ii) is not otherwise authorized at law; or</p> <p>(b) considers it in the public interest to do so.</p>
-------------------------------	--

LAND TITLES ACT

15. (1) Section 1 of the Land Titles Act is amended by adding the following definitions:

“fraudulent instrument” means an instrument,

- (a) under which a fraudulent person purports to receive or grant transfer an estate or interest in land,
- (b) that is given under the purported authority of a power of attorney that is forged,
- (c) that is a transfer of a charge where the charge is given by a fraudulent person, or
- (d) that perpetrates a fraud as prescribed with respect to the estate or interest in land affected by the instrument; (“acte frauduleux”)

“fraudulent person” means a person who executes or purports to execute an instrument if,

- (a) the person forged the instrument,
- (b) the person is a fictitious person, or
- (c) the person holds oneself out in the instrument to be, but knows that the person is not, the registered owner of the estate or interest in land affected by the instrument; (“fraudeur”)

(1.1) Subsections 57 (4) and (5) of the Act are repealed and the following substituted:

Compensation
from Fund

- (4) A person is entitled to compensation from the Assurance Fund if,
 - (a) the person is wrongfully deprived of land or of some estate or interest in land by reason of,
 - (i) the land being brought under this Act,
 - (ii) some other person being registered as owner through fraud, or
 - (iii) any misdescription, omission or other error in a certificate of ownership or charge or in an entry on the register;
 - (b) the person has demonstrated the requisite due diligence as specified by the Director if the person is wrongfully deprived of land or of some estate or interest in land by reason of some other person being registered as owner through fraud;
 - (c) the person is unable under subsection (1) or otherwise to recover just compensation for the person’s loss; and

(d) the person makes an application for compensation within the time period specified in subsection (5.1).

(2) Subsection 57 (13) of the Act is repealed and the following substituted:

Rectification of register

(13) Subject to subsection (13.1), The Director of Titles may, in the first instance or after a reference to a court, or a court may direct the rectification of the register if,

- (a) a registered instrument would be absolutely void if unregistered;
- (b) the Director of Titles or a court, as the case may be, is satisfied, on the basis of evidence that the Director of Titles specifies or the court orders, that a fraudulent instrument has been registered on or after October 19, 2006; or
- (c) the effect of the error, if not rectified, would be to deprive a person of land of which the person is legally in possession or legally in receipt of the rents and profits.

(5) Sections 155 and 156 of the Act are repealed and the following substituted:

Offences

156. (1) A person is guilty of an offence if the person fraudulently procures or attempts to fraudulently procure a fraudulent entry on the register, an erasure or deletion from the register or an alteration of the register.

Penalty

- (2) A person who is convicted of an offence under this section is liable to,
 - (a) a fine of not more than \$50,000 or imprisonment for a term of not more than two years less a day, or both, if the person is an individual; and
 - (b) a fine of not more than \$250,000, if the person is a corporation.

Order for compensation or restitution

(3) If a person is convicted of an offence under this section, the court making the conviction may, in addition to any other penalty, order the person convicted to pay compensation or to make restitution.

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

1. (1) The definition of “institution” in subsection 2 (1) of the Freedom of Information and Protection of Privacy Act is amended by striking out “and” at the end of clause (a) and by adding the following clause:

(a.1) a service provider organization within the meaning of section 17.1 of the Ministry of Government Services Act, and

(2) The Act is amended by adding the following sections:

Service
provider
organizations

65.1 (1) This section applies with respect to a service provider organization as defined in section 17.1 of the Ministry of Government Services Act.

Definitions

(2) In this section,

“customer service information” means, in relation to a service,

(a) the name, address and telephone number or other contact information of the individual to whom the service is to be provided and, if applicable, the person acting on behalf of that individual,

(b) the transaction or receipt number provided by the service provider organization in relation to the request for the service,

(c) information relating to the payment of any fee, and

(d) such other information as may be prescribed; (“renseignements liés au service à la clientèle”)

“designated service” means a service designated by regulations made under subsection 17.1 (3) of the *Ministry of Government Services Act* as a service that the service provider organization may provide on behalf of the Government or a public body; (“service désigné”)

“Government” means the Government as defined in the *Ministry of Government Services Act*; (“gouvernement”)

“public body” means a public body as defined in section 17.1 of the *Ministry of Government Services Act*. (“organisme”)

public”)

Authorization
to collect
personal
information

(3) A service provider organization is authorized to collect personal information for the purposes of providing a designated service.

Collection of customer service information	(4) Without limiting the generality of subsection (3), a service provider organization is authorized to collect customer service information, with the consent of the individual to whom the information relates, for the purposes of providing a designated service.
Conveying information to the Government, etc.	(5) If required by the regulations, a service provider organization that collects personal information on behalf of the Government or a public body in the course of providing a designated service shall convey the personal information to that Government or public body in accordance with the regulations.
Limitation after information conveyed	(6) After the service provider organization has conveyed personal information under subsection (5), the service provider organization shall not use or further disclose the personal information except as allowed by the regulations.
Collection of personal information under arrangements	(7) A person who provides services on behalf of a service provider organization pursuant to an arrangement under subsection 17.1 (7) of the Ministry of Government Services Act may not collect personal information in connection with providing those services unless the service provider organization and the person have entered into an agreement that governs the collection, use and disclosure of such personal information and the agreement meets the prescribed requirements, if any.
Audits by Commissioner	(8) The Commissioner may audit a service provider organization to check that there has been no unauthorized access to or modification of personal information in the custody of the organization and the organization shall cooperate with and assist the Commissioner in the conduct of the audit.

9. Subsection 60 (1) of the Act is amended by adding the following clauses:

(d.1) providing for procedures to be followed by an institution if personal information is disclosed in contravention of this Act;

(f.1) respecting the disposal of personal information under subsection 40 (4), including providing for different procedures for the disposal of personal information based on the sensitivity of the personal information;

2.3. British Columbia

2.3.1. Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165

Purpose for which personal information may be collected

26 No personal information may be collected by or for a public body unless

- (a) the collection of that information is expressly authorized by or under an Act,
- (b) that information is collected for the purposes of law enforcement, or
- (c) that information relates directly to and is necessary for an operating program or activity of the public body.

Protection of personal information

30 A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

2.3.2. Vital Statistics Act, R.S.B.C. 1996, c. 479

Registrations fraudulently or improperly obtained

28 If, after the notice to and hearing of those interested parties as the chief executive officer considers proper, the chief executive officer is satisfied that a registration under this Act was fraudulently or improperly obtained, the chief executive officer may order that it be cancelled, and after that a certificate must not be issued in respect of the registration.

Failure to carry out duties

49 (1) A person who fails to give a notice or to furnish any statement, certificate or particulars required under this Act, within the time limited by this Act, commits an offence and is liable on conviction to a fine of not more than \$50 000.

(2) If more than one person is required to give a notice or to register or to furnish any statement, certificate or particulars required under this Act and the duty is carried out by any of those persons, the other or others are absolved from the performance of the duty.

2.3.3. Bill 43- Vital Statistics Amendment Act, 2004

20 *Section 49 (1) is amended by striking out "offence." and substituting "offence and is liable on conviction to a fine of not more than \$50 000."*

2.4. Alberta

2.4.1. Personal Information Protection Act, S.A. 2003, c. P-6.5

Consent required	<p>7(1) Except where this Act provides otherwise, an organization shall not, with respect to personal information about an individual,</p> <ul style="list-style-type: none"> (a) collect that information unless the individual consents to the collection of that information, (b) collect that information from a source other than the individual unless the individual consents to the collection of that information from the other source, (c) use that information unless the individual consents to the use of that information, or (d) disclose that information unless the individual consents to the disclosure of that information. <p>(2) An organization shall not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal information about an individual beyond what is necessary to provide the product or service.</p> <p>(3) An individual may give a consent subject to any reasonable terms, conditions or qualifications established, set, approved by or otherwise acceptable to the individual.</p>
Limitations on collection	<p>11(1) An organization may collect personal information only for purposes that are reasonable.</p> <p>(2) Where an organization collects personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is collected.</p>
Limitations on use	<p>16(1) An organization may use personal information only for purposes that are reasonable.</p> <p>(2) Where an organization uses personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is used.</p>

Limitations on disclosure	<p>19(1) An organization may disclose personal information only for purposes that are reasonable.</p> <p>(2) Where an organization discloses personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is disclosed.</p>
Protection of information	<p>34. An organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.</p>

2.4.2. Fair Trading Act, Reg. 194/99 Collection and Debt Repayment Practices Regulation

Prohibited practices for collection agencies	<p>12(1) No collection agency or collector may</p> <p>(a) collect or attempt to collect money for a creditor except on the belief in good faith that the money is due and owing by the person to the creditor;</p> <p>(b) charge any fee to a person for whom the collection agency or collector acts in addition to those fees provided for in the agreement with that person;</p> <p>(c) if a collection agency,</p> <p style="padding-left: 20px;">(i) carry on the activities of a collection agency in a name other than the name in which it is licensed unless it has received the approval of the Director to do so, or</p> <p style="padding-left: 20px;">(ii) when using an automated call system, fail to identify the debtor by name when the call is answered by another person or when leaving a message for the debtor, or to provide a contact number for the debtor to call;</p> <p>(d) if a collector, collect or attempt to collect a debt without providing</p> <p style="padding-left: 20px;">(i) the collector's name as shown on the collector's licence in all contacts and correspondence, and</p> <p style="padding-left: 20px;">(ii) the name of the collection agency as shown on the collection agency licence in all contacts and correspondence with the debtor;</p> <p>(e) make any arrangement with a debtor to accept a sum of money that is less than the amount of the balance due and owing to a creditor as final settlement without the prior express consent of the creditor;</p>
--	---

- (f) fail to provide any person for whom the collection agency or collector acts with a written report on the status of that person's account in accordance with this Regulation;
- (g) make any personal call or telephone call for the purpose of collecting or attempting to collect a debt on any day except between 7 a.m. and 10 p.m. in Alberta;
- (h) directly or indirectly threaten or state an intention to proceed with any action for which the collection agency or the collector does not have the prior express consent of the creditor or for which there is no lawful authority;
- (i) contact or attempt to contact the debtor, any member of the debtor's household, any relative of the debtor, the debtor's employer or any neighbour, friend or acquaintance of the debtor by any means in such a manner as to constitute harassment, including without being limited to
 - (i) the use of threatening, profane, intimidating or coercive language,
 - (ii) the use of undue, excessive or unreasonable pressure, or
 - (iii) the use of telephone or e-mail to call or send messages excessively;
- (j) give any person, directly or indirectly, by implication or otherwise, any false or misleading information, including, but not limited to, references to the police, a law firm, prison, credit history, court proceedings or a lien or garnishment;
- (k) continue to collect or attempt to collect money from, or continue to communicate with,
 - (i) the person, where the person has informed the collection agency or the collector that the person is not the debtor, unless the collection agency or collector first takes all reasonable precautions to ensure that the person is in fact the debtor, or
 - (ii) the debtor, where the debtor has informed the collection agency or the collector by any verifiable means, including, but not limited to, personal service, certified mail, courier, facsimile, or e-mail, or by any other method, that the debt is in dispute and that the debtor wishes the creditor to take the matter to court;
- (l) contact a debtor's spouse or adult interdependent partner, relative, neighbour, friend or acquaintance unless the contact is limited to the purpose of obtaining the debtor's residential address, personal telephone number or employment telephone number;
- (m) contact the debtor's employer for any purpose other than to

confirm the debtor's employment status, business title and the address of the business, in preparation for legal proceedings;

(n) contact the debtor when the debtor has notified the collection agency in writing to communicate only with the debtor's representative and has provided a current address and telephone number for the representative, and the representative

(i) makes reasonable arrangements to discuss the debt with the collection agency or collector, and

(ii) discusses the debt with the collection agency or collector in accordance with the arrangements;

(o) contact a debtor at the debtor's place of employment if the debtor

(i) requests the collection agency or collector not to contact the debtor there,

(ii) makes reasonable arrangements to discuss the debt with the collection agency or collector, and

(iii) discusses the debt with the collection agency or collector in accordance with the arrangements;

(p) communicate information about the debt or the existence of the debt with any person except the debtor, a guarantor of the debt, the debtor's representative or the creditor of the debt unless the debtor has expressly consented to the communication;

(q) indicate to the debtor or any other person contacted for the purpose of collecting the debtor's debt that the collection agency or the collector is part of a law firm or the legal department of a business, including a legal department of the collection agency itself or of the creditor of the debt;

(r) if a collector, indicate to a debtor that the collector is a legal collector, litigation specialist or the like;

(s) charge any fee to a debtor beyond the debt that is due and owing from the debtor to the creditor, excluding a reasonable fee for a dishonoured cheque, if the fee was disclosed to the debtor in writing prior to the submission of the cheque;

(t) refuse to provide sufficient information on request to the debtor to ensure that the debtor is aware of the identity of the original and current creditor of the debt and the details of the debt;

(u) enter into or arrange wage assignments with a debtor or the employer of a debtor;

(v) exceed 3 unsolicited contacts on behalf of the same creditor with a debtor in any period of 7 consecutive days, not including contacts

with a third party to locate a debtor, mistaken contact with a third party, or contacts by traditional mail;

(w) cancel or alter a payment agreement with a debtor if the debtor has complied with the terms of the agreement and the debtor's financial circumstances have not changed materially, unless the debtor has misrepresented the debtor's financial circumstances;

(x) pursue a non judgment debt where the last payment or written acknowledgement by the debtor is more than 6 years previous;

(y) do anything that is prohibited by this Regulation.

(2) A term of an agreement entered into by a collection agency is void if that term

(a) misrepresents the rights and powers of a person collecting or attempting to collect a debt,

(b) misrepresents the obligations or legal liabilities of a debtor,

(c) is misleading as to its true nature and purpose, or

(d) otherwise contravenes the Act or this Regulation.

(3) Notwithstanding section 110(2) of the Act, a collection agency must not enter into an agreement or contract with or make a request of a representative or employee of the collection agency who is exempt under that section to undertake any action that contravenes this section.

(4) Subsection (1)(m), (v) and (w) come into force on March 1, 2006.

AR 194/99 s12;3/2006

2.4.3. Freedom of Information and Protection of Privacy Act, R.S.A. 2000, c. F-25

Protection
of
information

38 The head of a public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.

1994 cF 18.5 s36;1996 c28 s21

Use of
personal
information

39(1) A public body may use personal information only

(a) for the purpose for which the information was collected or compiled or for a use consistent with that purpose,

(b) if the individual the information is about has identified the information and consented, in the prescribed manner, to the use, or

(c) for a purpose for which that information may be disclosed to that

public body under section 40, 42 or 43.

(2) Despite subsection (1), but subject to subsection (3), a post secondary educational body may use personal information in its alumni records for the purpose of its own fund raising activities.

(3) A post secondary educational body must, when requested to do so by an individual, discontinue using that individual's personal information under subsection (2).

(4) A public body may use personal information only to the extent necessary to enable the public body to carry out its purpose in a reasonable manner.

1994 cF 18.5 s37;1999 c23 s24

Disclosure
of personal
information

40(1) A public body may disclose personal information only

- (a) in accordance with Part 1,
- (b) if the disclosure would not be an unreasonable invasion of a third party's personal privacy under section 17,
- (c) for the purpose for which the information was collected or compiled or for a use consistent with that purpose,
- (d) if the individual the information is about has identified the information and consented, in the prescribed manner, to the disclosure,
- (e) for the purpose of complying with an enactment of Alberta or Canada or with a treaty, arrangement or agreement made under an enactment of Alberta or Canada,
- (f) for any purpose in accordance with an enactment of Alberta or Canada that authorizes or requires the disclosure,
- (g) for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body having jurisdiction to compel the production of information or with a rule of court that relates to the production of information,
- (h) to an officer or employee of the public body or to a member of the Executive Council, if the information is necessary for the performance of the duties of the officer, employee or member,
- (i) to an officer or employee of a public body or to a member of the Executive Council, if the disclosure is necessary for the delivery of a common or integrated program or service and for the performance of the duties of the officer or employee or member to whom the information is disclosed,
- (j) for the purpose of enforcing a legal right that the Government of Alberta or a public body has against any person,

- (k) for the purpose of
 - (i) collecting a fine or debt owing by an individual to the Government of Alberta or to a public body, or to an assignee of either of them, or
 - (ii) making a payment owing by the Government of Alberta or by a public body to an individual,
- (l) for the purpose of determining or verifying an individual's suitability or eligibility for a program or benefit,
- (m) to the Auditor General or any other prescribed person or body for audit purposes,
- (n) to a member of the Legislative Assembly who has been requested by the individual the information is about to assist in resolving a problem,
- (o) to a representative of a bargaining agent who has been authorized in writing by the employee the information is about to make an inquiry,
- (p) to the Provincial Archives of Alberta or to the archives of a public body for permanent preservation,
- (q) to a public body or a law enforcement agency in Canada to assist in an investigation
 - (i) undertaken with a view to a law enforcement proceeding, or
 - (ii) from which a law enforcement proceeding is likely to result,
- (r) if the public body is a law enforcement agency and the information is disclosed
 - (i) to another law enforcement agency in Canada, or
 - (ii) to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority,
- (s) so that the spouse or adult interdependent partner, relative or friend of an injured, ill or deceased individual may be contacted,
- (t) in accordance with section 42 or 43,
- (u) to an expert for the purposes of section 18(2),
- (v) for use in a proceeding before a court or quasi-judicial body to which the Government of Alberta or a public body is a party,
- (w) when disclosure is by the Minister of Justice and Attorney General or an agent or lawyer of the Minister of Justice and Attorney General to a place of lawful detention,
- (x) for the purpose of managing or administering personnel of the Government of Alberta or the public body,
- (y) to the Director of Maintenance Enforcement for the purpose of enforcing a maintenance order under the Maintenance Enforcement Act,

(z) to an officer of the Legislature, if the information is necessary for the performance of the duties of that officer,

(aa) for the purpose of supervising an individual under the control or supervision of a correctional authority,

(bb) when the information is available to the public,

(bb.1) if the personal information is information of a type routinely disclosed in a business or professional context and the disclosure

(i) is limited to an individual's name and business contact information, including business title, address, telephone number, facsimile number and e-mail address, and

(ii) does not reveal other personal information about the individual or personal information about another individual,

(cc) to the surviving spouse or adult interdependent partner or a relative of a deceased individual if, in the opinion of the head of the public body, the disclosure is not an unreasonable invasion of the deceased's personal privacy,

(dd) to a lawyer or student-at-law acting for an inmate under the control or supervision of a correctional authority,

(ee) if the head of the public body believes, on reasonable grounds, that the disclosure will avert or minimize an imminent danger to the health or safety of any person, or

(ff) to the Administrator of the Motor Vehicle Accident Claims Act or to an agent or lawyer of the Administrator for the purpose of dealing with claims under that Act.

(2) Notwithstanding subsection (1), a post-secondary educational body may disclose personal information in its alumni records for the purpose of fund-raising activities of the post-secondary educational body if the post-secondary educational body and the person to whom the information is disclosed have entered into a written agreement

(a) that allows individuals a right of access to personal information that is disclosed about them under this subsection, and

(b) that provides that the person to whom the information is disclosed must discontinue using the personal information of any individual who so requests.

(3) Notwithstanding subsection (1), a post-secondary educational body may, for the purpose of assisting students in selecting courses, disclose teaching and course evaluations that were completed by students.

(4) A public body may disclose personal information only to the extent necessary to enable the public body to carry out the purposes described in

subsections (1), (2) and (3) in a reasonable manner.

RSA 2000 cF 25 s40;2002 cA 4.5 s38;2003 c21 s11

2.5. Quebec

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

Confidentiality.

53. Nominative information is confidential, except in the following cases:

1) where its disclosure is authorized by the person concerned by the information; in the case of a minor, the authorization may also be given by the person having parental authority;

2) where it relates to information obtained in the performance of an adjudicative function by a public body performing quasi-judicial functions; the information remains confidential, however, if the body obtained it when holding a sitting in camera or if the information is contemplated by an order not to disclose, publish or distribute.

1982, c. 30, s. 53; 1985, c. 30, s. 3; 1989, c. 54, s. 150; 1990, c. 57, s. 11.

Identifying information.

54. In any document, information concerning a natural person which allows the person to be identified is nominative information.

1982, c. 30, s. 54.

Release.

59. A public body shall not release nominative information without the consent of the person concerned.

Conditions.

Notwithstanding the foregoing, a public body may release nominative information without the consent of the person concerned in the following cases and strictly on the following conditions:

1) to the attorney of that body if the information is required for the purposes of a prosecution for an offence against an Act administered by that body or to the Attorney General, if the information is required for the purposes of a prosecution for an offence against an Act applicable in Québec;

2) to the attorney of that body, or to the Attorney General where he is acting as the attorney of that body, if the information is required for purposes of judicial proceedings other than those contemplated in

paragraph 1;

3) to a person responsible by law for the prevention, detection or repression of crime or statutory offences, if the information is required for the purposes of a prosecution for an offence against an Act applicable in Québec;

4) to a person to whom the information must be disclosed because of the urgency of a situation that threatens the life, health or safety of the person concerned;

5) to a person authorized by the Commission d'accès à l'information, in accordance with section 125, to use the information for study, research or statistics purposes;

6) (paragraph repealed);

7) (paragraph repealed);

8) to a person, body or agency, in accordance with sections 61, 67, 67.1, 67.2, 68 and 68.1;

9) to a person involved in an incident that has been the subject of a report by a police force; in the case of information on the identity of any other person involved in the incident, except a witness, an informer or a person whose health or safety could be endangered by the release of such information.

1982, c. 30, s. 59; 1983, c. 38, s. 55; 1984, c. 27, s. 1; 1985, c. 30, s. 5; 1987, c. 68, s. 5; 1990, c. 57, s. 13.

Qualified person.

62. Every 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.

Categories.

Moreover, the person must belong to one of the categories of persons referred to in subparagraph 4 of the second paragraph of section 76 or in subparagraph 5 of the first paragraph of section 81.

Unnecessary information.

64. No person may, on behalf of a public body, collect nominative information if it is not necessary for the carrying out of the attributions of the body or the implementation of a program under its management.

1982, c. 30, s. 64.

Destruction.

73. When the object for which nominative information was collected has been achieved, the public body shall destroy the document, subject to

the Archives Act (chapter A-21.1).

1982, c. 30, s. 73; 1983, c. 38, s. 56.

Powers.

124. The Commission may prescribe conditions applicable to a personal information file with which the public body must conform and respecting, in particular,

1) the kind of information that may be collected and the purposes for which it may be kept;

2) the use to which the file may be put;

3) the security measures that must be taken to ensure the confidentiality of nominative information;

4) the categories of persons who have access to nominative information in the discharge of their duties and, where such is the case, the special restrictions and conditions of access;

5) the special conditions to which the maintenance of the file may be subject, where such is the case.

1982, c. 30, s. 124; 1990, c. 57, s. 28.

Regulations.

155. The Government may make regulations

1) prescribing fees for the transcription, reproduction or transmission of documents or nominative information, and the terms and conditions of payment of the fees;

2) providing for total or partial exemption from the payment of fees under this Act;

3) defining what constitutes a document produced by or for another public body, for the purposes of section 48;

4) prescribing the rules according to which the collection of nominative information must be made;

5) fixing appropriate security standards to ensure the confidentiality of the information entered in a personal information file;

6) prescribing the particulars to be given by the public bodies to the Commission in relation to their personal information files;

7) designating, according to the standards provided for in the regulation and for the purposes of the second paragraph of section 28, the public bodies that must refuse to release or to confirm the existence of information obtained through their internal security service.

Categories.

The Government, in exercising its power to make regulations, may

establish categories of persons, public bodies, information, documents and files.

1982, c. 30, s. 155; 1990, c. 57, s. 39.

2.5.2. *An Act Respecting the Protection of Personal Information in the Private Sector,*
R.S.Q., c. P-39.1

Necessary
information.

5. Any person collecting personal information to establish a file on another person or to record personal information in such a file may collect only the information necessary for the object of the file.

Lawful
means.

Such information must be collected by lawful means.

1993, c. 17, s. 5.

Safety
measures.

10. Every person carrying on an enterprise who collects, holds, uses or communicates personal information about other persons must establish and apply such safety measures as are appropriate to ensure the confidentiality of the information.

1993, c. 17, s. 10.

Use of file.

12. Once the object of a file has been achieved, no information contained in it may be used otherwise than with the consent of the person concerned, subject to the time limit prescribed by law or by a retention schedule established by government regulation.

1993, c. 17, s. 12.

Consent.

13. No person may communicate to a third person the personal information contained in a file he holds on another person, or use it for purposes not relevant to the object of the file, unless the person concerned consents thereto or such communication or use is provided for by this Act.

1993, c. 17, s. 13.

Validity of
consent.

14. Consent to the communication or use of personal information must be manifest, free, and enlightened, and must be given for specific purposes. Such consent is valid only for the length of time needed to achieve the purposes for which it was requested.

Validity of consent. Consent given otherwise than in accordance with the first paragraph is without effect.

1993, c. 17, s. 14.

2.5.3. Consumer Protection Act, R.S.Q., c. P-40.

Writing to be signed. **27.** Subject to section 29, the merchant must sign the written contract duly filled out, give it to the consumer and grant him a sufficient time to become aware of its terms and scope before signing it.

1978, c. 9, s. 27; 1999, c. 40, s. 234.

Where signed. **28.** Subject to section 29, the signature of the parties must appear on the page of each copy of the contract, at the end of all the conditions.

1978, c. 9, s. 28.

Credit cards. **29.** Sections 27 and 28 do not apply to a contract extending variable credit made for the use of what are commonly called credit cards. In the case of such a contract, the issue of the card is in lieu of the merchant's signature and the use of the card by the consumer is in lieu of the consumer's signature.

1978, c. 9, s. 29.

Loss or theft. **123.** In case of loss or theft of a credit card, the consumer incurs no liability for a debt resulting from the use of such card by a third person after the issuer is notified of the loss or theft by telephone, telegraph, written notice or any other means.

1978, c. 9, s. 123.

Liability limited. **124.** Even where such notice is not given, the liability of the consumer whose credit card is lost or stolen is limited to the sum of \$50.

2.6. Manitoba

2.6.1. Personal Investigations Act, C.C.S.M. c. P34

No 5 No personal reporter, user or personal reporting agency, or any of their

divulging of contents of personal report	<p>employees, shall knowingly divulge the contents of any personal report or personal file to any person other than to</p> <ul style="list-style-type: none"> (a) a user or his or her agent, who requires the information for purposes of a decision in respect of a subject's application for credit, insurance, employment or tenancy or any other legitimate business purpose; or (b) the assignee of an agreement for credit, insurance or tenancy; or (c) any federal, provincial or municipal government or any agencies thereof, or any police officer acting in that capacity; or (d) the subject of the report on the request of the subject; <p>and any failure to comply with this provision is an offence under this Act.</p> <p>S.M. 2005, c. 6, s. 5.</p>
Disclosure of personal file information	<p>8(1) Any person may enquire of a personal reporting agency at any time, but not more frequently than at intervals of six months, unless a notification has been received under section 7, as to whether the personal reporting agency maintains a personal file on the person and if the personal reporting agency maintains such a file, the personal reporting agency shall disclose to that person the information as required under subsection 7(2) upon payment by the person of such fee as may be prescribed by the regulations.</p>
Right to protest information	<p>8(2) A person who receives information under subsection (1) has the right to protest the information in accordance with section 10 and the personal reporting agency is subject to the obligations set out in section 11.</p> <p>S.M. 2005, c. 6, s. 7.</p>
Verification of information	<p>11(1) Where the subject files a protest with a user or a personal reporter, or any person files a protest with a personal reporting agency, the user, personal reporter or personal investigation agency shall immediately</p> <ul style="list-style-type: none"> (a) attempt to verify the information and where the factual or investigative information cannot be verified, expunge the information from the personal file; or (b) where the veracity of the information is sustained, record the protest in the personal file; and report the action taken (c) to the subject of the personal report or personal file; and (d) to any person to whom the personal report may have been furnished within the previous 60 days.

Personal reporting agency outside Manitoba	11(2) Where a personal report is made by a personal reporting agency to a user in Manitoba and the office of the personal reporting agency is not located in the Province of Manitoba, the user is responsible for complying with subsection (1).
User outside Manitoba	11(3) Where a personal reporting agency makes a report to a user whose office is located outside Manitoba, the personal reporting agency is responsible for complying with subsection (1).
Agreement not to disclose information void	14 Any contract, agreement or understanding entered into between a personal reporter and any user whereby the parties agree to refuse to disclose any information to the subject of a personal report is void and the making of such an agreement or understanding is an offence against this Act; but a user may refer the subject of a report to the personal reporting agency for discussion of the content of any report supplied by the said agency.
Exemption from civil liability	16 No user, personal reporter or personal reporting agency is civilly liable to the subject of a personal report or personal file, unless the user, reporter or agency, as the case may be is or ought to be reasonably aware that part or all of the information in the report or personal file is false, or misleading, or was obtained negligently.
Void agreements	18 No agreement, oral or written shall provide or contain any provision, express or implied whereby the parties to the agreement agree that this Act or any provision thereof shall not apply to the agreement or to the parties; and any agreement so made is void and the making of such an agreement is an offence.

2.6.2. The Consumer Protection Act, C.C.S.M. c. C200

Prohibitions	98 No person, whether on his own behalf or on behalf of another, directly, or through others, shall with respect to any loan of money to which this Act applies, or to any hire-purchase or sale of goods or services, or both
	...
	(f) make telephone calls or personal calls of such nature or with such frequency as to constitute harassment of the debtor, his spouse or common-law partner or his family; or
	...

Limitation on issuance of credit card	114(1) No person shall issue, renew or substitute a credit card to another person except on the written or verbal request of that other person.
Onus of proof	114(2) The onus of proof that a request for a credit card was in fact made lies on the issuer.
Liability where credit card lost	116(1) Despite any agreement entered into before or after the coming into force of this Part, where a holder has lost a credit card or a credit card has been stolen, the holder is not liable for any debt incurred through its use after he or she has notified the issuer in accordance with subsection (1.2) that the card is lost or stolen and is no longer in his or her possession or control.
Liability for unauthorized use of credit card information	116(1.1) Despite any agreement entered into before or after the coming into force of this Part, where a debt has been incurred through the unauthorized use of credit card information, the holder is not liable for the debt if he or she notifies the issuer of the unauthorized use in accordance with subsection (1.2) within 30 days after the date of issue of the first credit card statement to include the debt.
Methods of giving notice	116(1.2) For the purposes of subsections (1) and (1.1), notice to the issuer must be given by personal delivery or by registered mail, fax, e-mail or another method that is capable of providing the holder with confirmation of delivery of the notice.
Liability of credit card holder	116(2) A holder is not liable for any debt in excess of the lesser of <ul style="list-style-type: none"> (a) \$50.; or (b) the maximum amount of credit that is available to the holder under a written agreement with the issuer; where the debt is incurred by use of the credit card by an unauthorized person prior to the time at which the holder gave notice to the issuer pursuant to subsection (1).
Liability of card holder where card surrendered	116(3) Where a card issuer, either directly or through a person acting as agent of the issuer, obtains surrender of a credit card by a card holder, the card holder is not liable for any use of the card after it has been surrendered.
Duties of agent upon surrender of credit card	116(4) Where any person as an agent of the issuer of a credit card, accepts the surrender of a credit card from a card holder he shall

- (a) give the card holder a receipt for each card surrendered; and
- (b) immediately forward each credit card to the card issuer with notice of surrender; and
- (c) be responsible for any unauthorized use of any surrendered credit card between the time of surrender and transmittal of the credit card to the issuer.

Onus of
proof in
disputes

117 Where a dispute arises between a holder and an issuer under section 116 the burden of proof rests with the issuer to show that the debt was incurred by the holder or a person authorized by the holder to use the card.

2.6.3. Bill 200 - The Personal Information Protection and Identity Theft Prevention Act

Consent
required

7(1) Except where this Act provides otherwise, an organization shall not, with respect to personal information about an individual,

- (a) collect that information unless the individual consents to the collection of that information;
- (b) collect that information from a source other than the individual unless the individual consents to the collection of that information from the other source;
- (c) use that information unless the individual consents to the use of that information; or
- (d) disclose that information unless the individual consents to the disclosure of that information.

Organization
cannot
require
greater
consent

7(2) An organization shall not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal information about an individual beyond what is necessary to provide the product or service.

Individual
may limit
consent

7(3) An individual may give consent subject to any reasonable terms, conditions or qualifications established, set, approved by or otherwise acceptable to the individual.

Form of
consent

8(1) An individual may give his or her consent in writing or orally to the collection, use or disclosure of personal information about the individual.

Giving information may be deemed consent

8(2) An individual is deemed to consent to the collection, use or disclosure of personal information about the individual by an organization for a particular purpose if

- (a) the individual, without actually giving the consent referred to in subsection (1), voluntarily provides the information to the organization for that purpose; and
- (b) it is reasonable that a person would voluntarily provide that information.

Notice in place of consent

8(3) Notwithstanding subsection 7(1), an organization may collect, use or disclose personal information about an individual for particular purposes if

- (a) the organization
 - (i) provides the individual with a notice, in a form that the individual can reasonably be expected to understand, that the organization intends to collect, use or disclose personal information about the individual for those purposes, and
 - (ii) with respect to that notice, gives the individual a reasonable opportunity to decline or object to having his or her personal information collected, used or disclosed for those purposes;
- (b) the individual does not, within a reasonable time, give the organization a response to that notice declining or objecting to the proposed collection, use or disclosure; and
- (c) having regard to the level of the sensitivity, if any, of the information in the circumstances, it is reasonable to collect, use or disclose the information as permitted under clauses (a) and (b).

Information to be used only for purpose it was collected

8(4) Subsections (2) and (3) are not to be construed so as to authorize an organization to collect, use or disclose personal information for any purpose other than the particular purposes for which the information was collected.

Manner of giving consent

8(5) Consent in writing may be given or otherwise transmitted by electronic means to an organization if the organization receiving that transmittal produces or is able at any time to produce a printed copy, image or reproduction of the consent in paper form.

Limitations on collection	11(1) An organization may collect personal information only for purposes that are reasonable.
Purpose determines if what collected is reasonable	11(2) Where an organization collects personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is collected.
Limitations on use	16(1) An organization may use personal information only for purposes that are reasonable.
Purpose determines if use reasonable	16(2) Where an organization uses personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is used.
Limitations on disclosure	19(1) An organization may disclose personal information only for purposes that are reasonable.
Purposes determine if disclosure reasonable	19(2) Where an organization discloses personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is disclosed.
Protection of information	34(1) An organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against risks such as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.
Notice if control of information lost	34(2) An organization must, as soon as reasonably practicable and in the prescribed manner, notify an individual if personal information about the individual that is in its custody or under its control is stolen, lost or accessed in an unauthorized manner.
Exception re law enforcement agency investigation	34(3) The requirement to notify an individual under subsection (2) does not apply where <ul style="list-style-type: none"> (a) the organization is instructed to refrain from doing so by a law enforcement agency that is investigating the theft, loss or unauthorized accessing of the personal information; or (b) the organization is satisfied that it is not reasonably possible for the

personal information to be used unlawfully.

Right of
action

34(4) An individual may commence an action in a court of competent jurisdiction against an organization for damages arising from its failure to

(a) protect personal information that is in its custody or under its control; or

(b) provide an individual notice under subsection (2), if it was not reasonable for the organization to have been satisfied that the personal information that was stolen, lost or accessed in an unauthorized manner would not be used unlawfully.

Other rights
not affected

34(5) The right of action under this section is in addition to any other right of action or remedy available at law. But where the court deems it just, damages awarded in an action under this section may be taken into account in assessing damages in any other proceeding arising out of the failure of the organization to protect personal information in its custody or under its control.

2.7. Saskatchewan

2.7.1. Credit Reporting Act, S.S. 2004, c. C-43.2

To whom
credit
reports
may be
provided

17(1) No credit reporting agency shall knowingly provide to any person any information from the files of the credit reporting agency except in a credit report provided:

(a) to a person who the credit reporting agency has reason to believe:

(i) intends to use the information in connection with:

(A) the extension of credit to the consumer to whom the information relates; or

(B) the purchase or collection of a debt of the consumer to whom the information relates;

(ii) intends to use the information in connection with the entering into or renewal of a tenancy agreement;

(iii) intends to use the information for employment purposes;

(iv) intends to use the information in connection with the underwriting of insurance involving the consumer;

(v) intends to use the information to determine the consumer's eligibility for any matter pursuant to any Canadian law, if the information is relevant to the eligibility requirement;

(vi) has a direct business need for the information in connection with

a business or credit transaction involving the consumer that is not mentioned in subclauses (i) to (v);

(vii) intends to use the information for the purpose of updating the information in a credit report previously provided to the person for one of the reasons mentioned in subclauses (i) to (vi);

(b) to a law enforcement agency in Canada for an investigation or for a prosecution;

(c) in response to a court order;

(d) in accordance with the written instructions of the consumer to whom the information relates; or

(e) in response to an order or direction made by the registrar pursuant to this Act.

(2) No person shall knowingly obtain any information from the files of a credit reporting agency respecting a consumer except for the purposes described in subsection (1).

(3) Notwithstanding subsections (1) and (2), a credit reporting agency may provide identifying information respecting any consumer, limited to the consumer's name, address, former addresses and places of employment to the following, even though the information is not intended to be used for a purpose mentioned in subsection (1):

(a) the Government of Canada;

(b) the Government of Saskatchewan;

(c) the government of any other province or territory of Canada;

(d) an agency of a government mentioned in clauses (a) to (c);

(e) a municipality in Canada or any agency of a municipality;

(f) a police officer acting in the course of his or her duties.

2004, c.C-43.2, s.17.

Disclosure
to
consumer
by credit
reporting
agency

21(1) Subject to subsections (2) and (3), on receipt of a request by a consumer, a credit reporting agency shall:

(a) clearly and accurately disclose to the consumer, without charge:

(i) the nature and substance of all information in its files respecting the consumer at the time of the request;

(ii) the sources of its information, unless the consumer is able to readily ascertain those sources;

(iii) the names of any person to whom a credit report has been provided within the preceding six months respecting the consumer;

and

(iv) the contents of any written or oral credit report respecting the consumer made to any other person; and

(b) inform the consumer of his or her right to dispute any information contained in the file pursuant to Division 3 and the manner in which a dispute may be made.

(2) A credit reporting agency shall make the disclosures required pursuant to subsection (1) to the consumer:

(a) in person, if the consumer appears in person;

(b) by telephone, if the consumer has made a written request for telephone disclosure; or

(c) by mail, if the consumer has made a written request for disclosure by mail.

(3) The credit reporting agency shall require the consumer to submit reasonable identification before making the disclosure required pursuant to subsection (1).

(4) A credit reporting agency making a disclosure pursuant to clause (2)(a) shall allow the consumer to be accompanied by one witness who shall identify himself or herself to the credit reporting agency and in whose presence the credit reporting agency shall make the disclosure.

(5) If a consumer requests a copy of the material mentioned in clause (1)(a), the credit reporting agency shall provide a copy to the consumer.

(6) Every credit reporting agency shall provide trained personnel to explain to a consumer any information provided to the consumer pursuant to this section.

2004, c.C-43.2, s.21.

Investigation
by credit
reporting
agency

24(1) If a credit reporting agency receives notification of a dispute pursuant to section 23, the credit reporting agency shall investigate within a reasonable time.

(2) If, as a result of an investigation pursuant to subsection (1), any information in the file respecting the consumer is found to be incomplete or inaccurate or can no longer be verified, the credit reporting agency shall, within a reasonable time:

(a) update the information by completing or correcting the information and deleting any information that cannot be verified;

(b) notify the consumer in writing of the changes; and

(c) notify any person in writing who received a credit report respecting

the file within six months preceding the changes, unless the consumer requests that notification not be given.

(3) If, as a result of an investigation pursuant to subsection (1), the credit reporting agency is of the opinion that the information in the file respecting the consumer is complete, accurate and verified, the credit reporting agency shall advise the consumer in writing of his or her right to file a written statement of not more than 200 words setting out the nature of his or her dispute respecting the information.

(4) If a statement of dispute is filed by a consumer pursuant to subsection (3), the credit reporting agency shall provide a copy of the statement of dispute:

(a) to any person who received a credit report respecting the file within six months preceding the date the consumer filed a notification of dispute pursuant to section 23, unless the consumer requests that a copy of the statement of dispute not be provided; and

(b) in any subsequent credit report containing the information that the consumer disputes.

2004, c.C-43.2, s.24.

Waiver of benefits ineffective; inclusion of certain clauses forbidden

29 Every agreement or bargain, verbal or written, express or implied, that states or implies any of the following is void:

(a) that the provisions of this Act or the regulations made pursuant to this Act do not apply;

(b) that any right or remedy provided by this Act or the regulations made pursuant to this Act does not apply;

(c) that any right or remedy provided by this Act or the regulations made pursuant to this Act is in any way limited, modified or abrogated.

2004, c.C-43.2, s.29.

2.7.2. The Consumer Protection Act, S.S. 1996, c. C-30.1

Limitation of liability for unauthorized use of credit card

75.2(1) This section applies notwithstanding any agreement to the contrary that:

(a) was entered into before the coming into force of this section; or

(b) is entered into on or after the coming into force of this section.

(2) If a credit card is lost or stolen and the credit card issuer is notified of the loss or theft, the credit card holder is not liable for any debt incurred through the unauthorized use of the credit card after the credit card issuer

is notified of the loss or theft.

(3) If a debt is incurred in the name of a credit card holder through the unauthorized use of credit card information and the credit card issuer receives notice of the unauthorized use within 30 days after the date of issuance of the first credit card statement that includes the debt, the credit card holder is not liable for that debt.

(4) Notice pursuant to subsection (2) or (3) may be given orally or in writing.

(5) Subject to subsection (6) and the regulations, the maximum liability of a credit card holder arising from the unauthorized use of a lost or stolen credit card before the credit card issuer receives notice of the loss or theft pursuant to subsection (2) is the lesser of:

- (a) \$50 or any greater amount prescribed in the regulations; and
- (b) the amount fixed or agreed to by the credit card issuer as the maximum amount for which the credit card holder is liable in the event of the unauthorized use of the credit card after its loss or theft.

(6) Subsection (5) does not apply to any transaction or category of transactions exempted by the regulations.

2002, c.16, s.5.

2.8. Nova Scotia

2.8.1. Consumer Reporting Act, R.S.N.S. 1989, c. 93

Confidentiality

9 (1) No consumer reporting agency and no officer or employee thereof shall knowingly furnish any information from the files of the consumer reporting agency except in a consumer report given

- (a) in response to the order of a court having jurisdiction to issue such an order;
- (b) in accordance with the written instructions of the consumer to whom the information relates; or
- (c) to a person who it has reason to believe
 - (i) intends to use the information in connection with the extension of credit to or the collection of a debt of the consumer to whom the information pertains,
 - (ii) intends to use the information in connection with the entering into or renewal of a tenancy agreement by the consumer,
 - (iii) intends to use the information for employment purposes,
 - (iv) intends to use the information in connection with the

underwriting of insurance involving the consumer,

(v) intends to use the information to determine the consumers eligibility for any matter under a statute or regulation where the information is relevant to the requirement prescribed by law,

(vi) otherwise has a direct business need for the information in connection with a business transaction involving the consumer.

(2) No person shall knowingly obtain any information from the files of a consumer reporting agency respecting a consumer except for the purposes referred to in subsection (1).

(3) Notwithstanding subsections (1) and (2), a consumer reporting agency may furnish identifying information respecting any consumer, limited to his name, address, former addresses, places of employment, or former places of employment, to any department of the Province or of Canada or any province thereof, notwithstanding that such information is not to be used for a purpose mentioned in clause (c) of subsection (1).

(4) A consumer reporting agency shall not sell, lease or transfer title to its files or any of them except to another consumer reporting agency registered under this Act. R.S., c. 93, s. 9.

Consent and notice

11 (1) No person shall procure or cause to be prepared a consumer report respecting a consumer

(a) without the express written consent of the consumer; or

(b) unless he notifies the consumer in writing that a consumer report has been or will be requested and advises him not later than ten days after the report has been requested of the name and address of the consumer reporting agency.

(2) The notice and consent referred to in this Section may be contained in an application for credit, insurance, employment or tenancy if it is clearly set forth in type not less than ten point in size above the signature of the consumer.

(3) Where a user of information contained in a consumer report denies a benefit in whole or in part to a consumer, or increases the cost of the benefit to a consumer, the user shall advise the consumer in writing immediately

(a) that a benefit has been denied him in whole or in part or increased in cost;

(b) of his right to have disclosed to him all information pertaining to him in the files of the consumer reporting agency from whom the report was obtained;

- (c) of the name and address of the consumer reporting agency;
- (d) of the source and nature of information obtained elsewhere than from a consumer reporting agency. R.S., c. 93, s. 11.

Disclosure

12 (1) Every consumer reporting agency shall, at the written request of a consumer and during normal business hours, clearly and accurately disclose to the consumer, without charge,

- (a) the nature and substance of all information in its files pertaining to the consumer at the time of the request;
- (b) the sources of its information unless they can be readily ascertained by the consumer;
- (c) the names of the recipients of any consumer report pertaining to the consumer that it has furnished within the preceding twelve months;
- (d) copies of any written report made pertaining to the consumer to any other person or, where the report was oral, particulars of the content of such oral report,

and shall inform the consumer of his right to protest any information contained in the file under Sections 13 and 14 and the manner in which a protest may be made.

(2) A consumer reporting agency may withhold from the disclosures required by subsection (1) any medical information obtained from the consumers own physician and which the physician has specifically requested in writing be withheld from the consumer in his own best interest.

(3) The disclosures required under this Section shall be made to the consumer

- (a) in person if he appears in person and furnishes proper identification;
- (b) by telephone if he has made a written request, with sufficient identification, for telephone disclosure and the toll charge, if any, for the telephone call is prepaid by or charged directly to the consumer.

(4) Every consumer reporting agency shall provide trained personnel to explain to the consumer any information furnished to him under this Section.

(5) The consumer shall be permitted to be accompanied by one other person of his choosing to whom the consumer reporting agency may be required by the consumer to disclose his file.

(6) The consumer reporting agency shall permit the consumer to whom

information is disclosed under this Section to make an abstract thereof.

(7) A consumer reporting agency shall require reasonable identification of the consumer and a person accompanying him before making disclosures under this Section.

(8) A consumer reporting agency shall not require a consumer to give any undertaking or waive or release any right or chose in action as a condition precedent to his access to his file under this Section. R.S., c. 93, s. 12.

Protests

13 (1) Where a consumer disputes the accuracy of any information relating to him in the files of a consumer reporting agency he may file a statement of protest with the consumer reporting agency or the user or both.

(2) Where a statement of protest is filed in accordance with subsection (1), the consumer reporting agency or the user shall immediately

(a) attempt to verify the information and, where the information cannot be verified, expunge the information from the consumers file; or

(b) where the veracity of the information is sustained, record the protest in the consumers file,

and report the action taken

(c) to the consumer; and

(d) to any person to whom it furnished a consumer report within the preceding sixty days.

(3) Where a consumer report is made by a consumer reporting agency to a user in the Province and the office of the consumer reporting agency is not located in the Province, the user is responsible for complying with subsection (2).

(4) Where a consumer reporting agency makes a report to a user whose office is located outside the Province, the consumer reporting agency is responsible for complying with subsection (2).

(5) Where a consumer is dissatisfied by the action taken by the consumer reporting agency or the user under this Section he may appeal to the Director who shall investigate the matter. R.S., c. 93, s. 13.

2.8.2. Vital Statistics Act, R.S.N.S. 1989, c. 494

Penalty for obtaining certificate

49A Every person who obtains or attempts to obtain a birth certificate or a certified copy, photostatic copy or photographic copy of the registration of a birth for a fraudulent or other improper purpose is guilty of an offence

for and liable on summary conviction to a penalty not exceeding fifty thousand
improper dollars or to imprisonment for not more than two years or to both. 2001, c.
purpose 45, s. 2.

2.8.3. Personal Information International Disclosure Protection Act, S.N.S. 2006, c. 3.

5 (1) A public body shall ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless

- (a) where the individual the information is about has identified the information and has consented, in the manner prescribed by the regulations, to it being stored in or accessed from, as the case may be, outside Canada;
- (b) where it is stored in or accessed from outside Canada for the purpose of disclosure allowed under this Act; or
- (c) the head of the public body has allowed storage or access outside Canada pursuant to subsection (2).

(2) The head of a public body may allow storage or access outside Canada of personal information in its custody or under its control, subject to any restrictions or conditions the head considers advisable, if the head considers the storage or access is to meet the necessary requirements of the public body's operation.

(3) Where the head of a public body makes a decision pursuant to subsection (2) in any year allowing storage or access outside Canada, the head shall, within ninety days after the end of that year, report to the Minister all such decisions made during that year, together with the reasons therefor.

(4) In providing storage, access or disclosure of personal information outside Canada, a service provider shall only collect and use such personal information that is necessary to fulfill its obligation as a service provider, and shall at all times make reasonable security arrangements to protect any personal information that it collects or uses by or on behalf of a public body.

9 (1) A public body shall ensure that personal information in its custody or under its control is disclosed outside Canada only as permitted pursuant to this Section.

(2) A public body may disclose outside Canada personal information in its custody or under its control

- (a) in accordance with this Act;

- (b) where the individual the information is about has identified the information and consented, in writing, to its disclosure inside or outside Canada, as the case may be;
 - (c) in accordance with an enactment of the Province, the Government of Canada or the Parliament of Canada that authorizes or requires its disclosure;
 - (d) in accordance with a provision of a treaty, arrangement or agreement that
 - (i) authorizes or requires its disclosure, and
 - (ii) is made under an enactment of the Province, the Government of Canada or the Parliament of Canada;
 - (e) to the head of the public body, if the information is immediately necessary for the performance of the duties of the head;
 - (f) to a director, officer or employee of the public body or to the head of the public body, if the information is immediately necessary for the protection of the health or safety of the director, officer, employee or head;
 - (g) to the Attorney General or legal counsel for the public body, for use in civil proceedings involving the Government of the Province or the public body;
 - (h) for the purpose of
 - (i) collecting moneys owing by an individual to Her Majesty in right of the Province or to a public body, or
 - (ii) making a payment owing by Her Majesty in right of the Province or by a public body to an individual;
 - (i) for the purpose of
 - (i) licensing or registration of motor vehicles or drivers, or
 - (ii) verification of motor vehicle insurance, motor vehicle registration or drivers' licences;
 - (j) where the head of the public body determines that compelling circumstances exist that affect anyone's health or safety;
 - (k) so that the next of kin or a friend of an injured, ill or deceased individual may be contacted; or
 - (l) in accordance with Section 10 or 11.
- (3) In addition to the authority pursuant to this Section, a public body that is a law enforcement agency may disclose personal information in its custody or under its control to

- (a) another law enforcement agency in Canada; or
- (b) a law enforcement agency in a foreign country under an arrangement, a written agreement, a treaty or an enactment of the Province, the Government of Canada or the Parliament of Canada.

(4) The head of a public body may allow a director, officer or employee of the public body to transport personal information outside Canada temporarily if the head considers it is necessary for the performance of the duties of the director, officer or employee to transport the information in a computer, a cell phone or another mobile electronic device.

2.9. New Brunswick

2.9.1. Collection Agencies Act, N.B. Reg. 84-256

Creditor
conduct

14

No collection agency, branch office of a collection agency or collector, by himself or while employed by a collection agency, shall:

...

- (g) use threatening, intimidating or coercive language, cite loss of employment, loss of community ranking or sufferance of embarrassment or, by the timing of personal or phone contacts to irregular hours, intrude upon the privacy of the home and the family of the debtor, the regular hours being from nine in the forenoon to nine in the afternoon of the same day.

2.10. Prince Edward Island

2.10.1. Consumer Reporting Act, R.S.P.E.I. 1988, c. C-20

Providing
information,
conditions
where
permissible

8. (1) No consumer reporting agency and no officer or employee thereof shall knowingly furnish any information from the files of the consumer reporting agency except

- (a) in response to the order of a court having jurisdiction to issue such an order;
- (b) in accordance with the written instructions of the consumer to whom the information relates;
- (c) in response to an order or direction made under this Act; or
- (d) in a consumer report given to a person who it has reason to believe
 - (i) intends to use the information in connection with the extension of credit to, or the purchase or collection of, a debt of the consumer

to whom the information pertains,

(ii) intends to use the information in connection with the entering into or renewal of a tenancy agreement,

(iii) intends to use the information for employment purposes,

(iv) intends to use the information in connection with the underwriting of insurance involving the consumer,

(v) intends to use the information to determine the consumer's eligibility for any matter under a statute or regulation where the information is relevant to the requirement prescribed by law,

(vi) otherwise has a direct business need for the information in connection with a business transaction involving the consumer.

Certain uses prohibited

(2) No person shall knowingly obtain any information from the files of consumer reporting agency respecting a consumer except for the purposes referred to in subsection (1).

Providing certain information to governments

(3) Notwithstanding subsections (1) and (2), a consumer reporting agency may furnish identifying information respecting any consumer, limited to his name, address, former addresses, places of employment or former place of employment, to the Government of Prince Edward Island or of Canada or any province thereof or of any agency of such government or the government of any municipality in Canada, or any agency thereof, or to any police officer acting in the course of his duties, notwithstanding that such information is not to be used for a purpose mentioned in clause (1)(d).

Transfer of files to another

(4) A consumer reporting agency shall not sell, lease or transfer title to its files or any of them except to another consumer reporting agency registered under this Act. R.S.P.E.I. 1974, Cap. C-18, s.8.

Consumer may request whether report made

10. (1) Every person shall, where requested by a consumer in writing or personally, inform the consumer whether or not a consumer report respecting him has been or is to be referred to in connection with any specified transaction or matter in which such person is engaged, and, if so, of the name and address of the consumer reporting agency supplying the report.

Notification of consumer report

(2) No person shall procure from a consumer reporting agency or cause it to prepare a consumer report containing information respecting a consumer unless he notifies the consumer of the fact before the report is requested or he has already obtained the consent of the consumer, and where the consumer so requests in writing or personally, he shall inform

the consumer of the name and address of the consumer reporting agency supplying the report; the giving of a notice under this subsection by a person proposing to extend credit, or by his assignee, or proposed assignee, shall be deemed to be sufficient notice by both.

Adverse
action

(3) Where a benefit is denied to a consumer or a charge to a consumer is increased either wholly or partly because of information received from a consumer reporting agency, or a person other than a consumer reporting agency, the user of such information shall forthwith advise the consumer at the time such action is communicated to the consumer notice of the fact and, upon the request of the consumer made within sixty days after such notice, shall inform the consumer

(a) of the nature and source of the information where the information is furnished by a person other than a consumer reporting agency; or

(b) of the name and address of the consumer reporting agency, where the information is furnished by a consumer reporting agency,

and the notice required to be given by the user under this subsection shall contain notice of the consumer's right to request the information referred to in clauses (a) and (b) and the time limited therefor. R.S.P.E.I. 1974, Cap. C-18, s.10

Disclosure
by consumer
reporting
agency

11. (1) Every consumer reporting agency shall, at the written request of a consumer and during normal business hours, clearly and accurately disclose to the consumer, without charge, Disclosure by consumer reporting agency

(a) the nature and substance of all information in its files pertaining to the consumer at the time of the request;

(b) the sources of its credit information or personal information;

(c) the names of the recipients of any consumer report pertaining to the consumer that it has furnished, within the preceding twelve months;

(d) contents of any written consumer report pertaining to the consumer made to any other person, or where the report was oral, particulars of the content of such oral report,

and shall inform the consumer of his right to protest any information contained in the file under sections 12 and 13 and the manner in which a protest may be made.

How
disclosure to
be made

(2) The disclosures required under this section shall be made to the consumer

(a) in person if he appears in person and furnishes proper

- identification;
- (b) by telephone if he, with sufficient identification, has made a written request for telephone disclosure and the toll charge, if any, for the telephone call is prepaid by or charged directly to the consumer.
- Trained personnel to be available (3) Every consumer reporting agency shall provide trained personnel to explain to the consumer any information furnished to him under this section.
- Consumer accompanied by another (4) The consumer shall be permitted to be accompanied by one other person of his choosing to whom the consumer reporting agency may be required by the consumer to disclose his file.
- Consumer may make abstract (5) The consumer reporting agency shall permit the consumer to whom information is disclosed under this section to make an abstract thereof.
- Identification of consumer before disclosure (6) A consumer reporting agency shall require reasonable identification of the consumer and a person accompanying him before making disclosures under this section.
- No conditions precedent to disclosure (7) A consumer reporting agency shall not require a consumer to give an undertaking or waive or release any right as a condition precedent to his access to his file under this section. R.S.P.E.I. 1974, Cap. C-18, s.11.
- Disputing accuracy of information **12.** (1) Where a consumer disputes the accuracy or completeness of any item of information contained in his file, the consumer reporting agency within a reasonable time shall use its best endeavours to confirm or complete the information and shall correct, supplement or delete the information in accordance with good practice.
- Correction of information, notices to be sent to (2) Where a consumer reporting agency corrects, supplements or deletes information under subsection (1), the consumer reporting agency shall furnish notification of the correction, supplement or deletion to
- (a) the Registrar and all persons who have been supplied with a consumer report based on the unamended file within sixty days before the correction, supplement or deletion is made;
- (b) the persons specifically designated by the consumer from among those who have been supplied with a consumer report based on the unamended file, where the report contains personal or credit information, within the one year period preceding the correction, supplement or deletion; and
- (c) the consumer.

- User responsible for information, where
- (3) Where a consumer report is made by a consumer reporting agency to a user in Prince Edward Island and the office of the consumer reporting agency is not located in the Province of Prince Edward Island, the user is responsible for complying with subsection (2).
- User located outside province, where
- (4) Where a consumer reporting agency makes a report to a user whose office is located outside Prince Edward Island, the consumer reporting agency is responsible for complying with subsection (2).
- Appeal to Registrar
- (5) Where a consumer is dissatisfied by the action taken by the consumer reporting agency or the user under this section, he may appeal to the Registrar who shall investigate the matter. R.S.P.E.I. 1974, Cap. C-18, s.12.

2.10.2. Conduct of Creditors Regulations, P.E.I. Reg. EC578/83

- Creditor conduct
2. No creditor shall
- (a) collect or attempt to collect money without first being satisfied that the money is owed by the borrower to the creditor;
 - (b) collect or attempt to collect money from or otherwise contact or importune a borrower at his place of employment;
 - (c) make any charge against a borrower in addition to those contained in the agreement with that borrower or in a cost of borrowing statement furnished to the borrower;
 - (d) send any telegram or make any telephone call for the purpose of demanding payment, if the charges are payable by the addressee or the person to whom the call is made;
 - (e) communicate with a borrower after the borrower has notified him in writing to communicate with the designated legal advisor of the borrower;
 - (f) use, without lawful authority, any summons, notice or demand, or other document, expressed in language of the general style or purport of any form used in any court in the province, or printed or written or in the general appearance or format of any such form;
 - (g) in any way abuse or intimidate a borrower either orally or in writing to induce the borrower to pay money or to deliver up possession of property;

2.11. Newfoundland and Labrador

2.11.1. Consumer Reporting Agencies Act, R.S.N.L. 1990, c. C-32

Disclosure of consumer report	<p>19. (1) A consumer reporting agency shall not provide a consumer report except</p> <ul style="list-style-type: none"> (a) in response to an order of a court; (b) in accordance with the written instructions of the consumer to whom the consumer report relates; (c) in response to an order or direction made under this Act; (d) to a person that it has reason to believe <ul style="list-style-type: none"> (i) is involved in a business or credit transaction with the consumer, or (ii) intends to use the consumer report for employment purposes; (e) to the government of the province or of Canada, or to a peace officer acting in the course of his or her duties. <p>(2) A person shall not seek to obtain a consumer report from a consumer reporting agency except for the purposes set out in subsection (1).</p> <p>1977 c18 s19</p>
Personal information	<p>23. A person shall not procure or prepare a consumer report containing personal information from a consumer reporting agency unless that person notifies the consumer in writing of his or her intention to procure or prepare the report, together with the name and address of the consumer reporting agency.</p> <p>1977 c18 s22</p>
Disclosure of file to consumer	<p>24. (1) A consumer reporting agency, during normal business hours, upon the request of a consumer, and without charge,</p> <ul style="list-style-type: none"> (a) shall disclose to the consumer whether or not it has collected or retains consumer information respecting him or her; (b) shall produce for examination in written form, clearly understandable to the consumer, the contents of all the consumer information, except medical information obtained with the written consent of the consumer that the consumer's physician has requested in

writing be withheld from the consumer; and

(c) shall disclose the names of the recipients of a consumer report and the contents of the report, made within a period of 1 year before the request.

(2) The consumer reporting agency concerned shall permit a person to whom consumer information is disclosed under subsection (1) to make a copy.

1977 c18 s23