HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

THE GROWING PROBLEM OF IDENTITY THEFT AND ITS ECONOMIC AND SOCIAL IMPACT

Report of the Standing Committee on Access to Information, Privacy and Ethics

Pierre-Luc Dusseault
Chair

MAY 2015

41st PARLIAMENT, SECOND SESSION

THE GROWING PROBLEM OF IDENTITY THEFT AND ITS ECONOMIC AND SOCIAL IMPACT

Report of the Standing Committee on Access to Information, Privacy and Ethics

Pierre-Luc Dusseault
Chair

MAY 2015

41st PARLIAMENT, SECOND SESSION

STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

CHAIR

Pierre-Luc Dusseault

VICE-CHAIRS

Patricia Davidson
Scott Simms

MEMBERS

Charlie Angus
Charmaine Borg
Ray Boughen
Paul Calandra
Larry Maguire
Tilly O'Neill Gordon
Bob Zimmer

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

Scott Andrews
John Carmichael
Jacques Gourde
Laurie Hawn
Pat Martin
Mathieu Ravignat

CLERKS OF THE COMMITTEE

Joann Garbig
Chad Mariage

LIBRARY OF PARLIAMENT
Parliamentary Information and Research Service

Maxime-Olivier Thibodeau
Miguel Bernal-Castillero
Dara Lithwick

THE STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

has the honour to present its

SEVENTH REPORT

Pursuant to its mandate under Standing Order 108(3)(*h*), the Committee has studied the growing problem of identity theft and its economic impact and has agreed to report the following:

TABLE OF CONTENTS

THE GROWING PROBLEM OF IDENTITY THEFT AND ITS ECONOMIC AND SOCIAL IMPACT

INTRODUCTION

On 7 November 2013, the House of Commons Standing Committee on Access to Information, Privacy and Ethics (the Committee) passed the following motion to study the issue of identity theft:

> That the Committee study the growing problem of identity theft and its economic impact upon citizens and businesses and the steps that businesses and law enforcement agencies are taking to protect Canadians from identity theft; and that the Committee report its findings to Parliament.[1]

Identity theft occurs when someone acquires and collects someone else's personal information for criminal purposes, mainly "identity fraud." "Identity fraud" is the actual deceptive use of someone else's identity, for example to abuse the other person's credit card data, access bank accounts and transfer balances, make purchases, or impersonate the other person to obtain a loan, government services, and more.

The Committee's study began on 1 April 2014 and ended on 23 February 2015. During the 10 meetings dedicated to this study, the Committee heard from 39 witnesses from government departments and agencies, law enforcement agencies, interest groups, universities, law firms, credit reporting agencies, banks, and information technology companies.

1 House of Commons, Standing Committee on Access to Information, Privacy and Ethics, *Minutes of Proceedings*, 2nd Session, 41st Parliament, 7 November 2013. The same motion was passed during the 1st Session of the 41st Parliament, though the Committee did not undertake the study of the issue prior to the end of the session.

DEFINING IDENTITY THEFT AND ITS ECONOMIC IMPACT

A. Canadian legislation concerning identity theft

Bill S-4: An Act to amend the Criminal Code (identity theft and related misconduct)

In January 2010 Bill S-4, An Act to amend the Criminal Code (identity theft and related misconduct), came into force.[2] The bill created several new *Criminal Code* offences that specifically target the aspects of identity theft that were not covered by existing provisions. The three main new offences that were created by Bill S-4 are as follows: obtaining and possessing identity information with the intent to use it in a crime (new subsection 402.2(1) of the *Criminal Code*); trafficking of identity information knowing it will be used in a crime (new subsection 402.2(2) of the *Criminal Code*); and unlawfully possessing or trafficking government-issued identity documents (new section 56.1 of the *Criminal Code*).

Identity theft and federal privacy laws

Canada's federal private sector privacy law, the *Personal Information Protection and Electronic Documents Act*[3] (PIPEDA), applies to commercial activities across the country, save in three provinces recognized as having substantially similar legislation.[4] Both British Columbia and Alberta have statutes called the *Personal Information Protection Act*, or PIPA,[5] while in Quebec *An Act Respecting the Protection of Personal Information in the Private Sector*[6] is in force. As well, the *Privacy Act*[7] (comparable to provincial statutes) regulates federal public sector activities.

---

2 Bill S-4 received Royal Assent on 22 October 2009 and became S.C. (2009), c. 28.

3 *Personal Information Protection and Electronic Documents Act* (S.C. 2000, c. 5).

4 New Brunswick, Ontario and Newfoundland and Labrador have enacted privacy legislation that applies to the health sector and that is considered substantially similar.

5 British Columbia, *Personal Information Protection Act*, [SBC 2003] c. 63; Alberta, *Alberta's Personal Information Protection Act*, (SA, 2003, c. P-6.5). Note that in the Supreme Court of Canada decision *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62, rendered on 15 November 2013, the Supreme Court of Canada held that the Alberta PIPA unjustly restricted the collection, use and disclosure of personal information which violated a union's expressive rights under section 2(*b*) of the *Canadian Charter of Rights and Freedoms*. The Court declared the Alberta PIPA to be invalid but granted a suspension to the declaration of invalidity for a period of 12 months to enable Alberta's legislature to decide how to amend the PIPA to bring it into constitutional conformity. On 30 October 2014, the Court granted Alberta a six-month extension.

6 Quebec, *An Act Respecting the Protection of Personal Information in the Private Sector*, (c. P-39.1).

7 *Privacy Act* (R.S.C., 1985, c. P-21).

These data protection laws apply to the collection, use, and disclosure of the personal information collected by private and public organizations. PIPEDA and its provincial counterparts play an important role in helping to reduce the risk of identity theft by requiring that private sector organizations take appropriate security measures to collect only the personal information that is required for a given transaction, and to securely destroy information that is no longer required. The *Privacy Act* establishes similar limits on the collection, use and disclosure of personal information by the federal government.

The Office of the Privacy Commissioner of Canada (OPC) has published several guidance documents for businesses and consumers regarding identity theft.[8] For example, in one fact sheet, the OPC advises Canadian retailers to help safeguard their customers' personal information (as required under PIPEDA) by not printing full credit card numbers on customer receipts, "because if the receipt is lost, stolen or discarded, the number can be used to commit credit card fraud, identity theft or other crimes."[9]

In another fact sheet titled "Best Practices for the use of Social Insurance Numbers in the private sector," the OPC explains why businesses should not use a social insurance number (SIN) as a general identifier and posits that organizations should restrict their collection, use and disclosure of SINs to the purposes of the Act,[10] that is, to the purposes of income reporting. Nonetheless, as noted by the OPC, "there is no law prohibiting an organization from asking for a customer's SIN, or a customer from supplying the SIN, for purposes other than income reporting." There are two issues identified by the OPC: First, SINs are pieces of personal information that can be used to steal someone's identity if not properly safeguarded. Second, as SINs are personal information, PIPEDA applies to the collection, use and disclosure of SIN information.

Finally, in a fact sheet titled "Businesses and Identity Theft," the OPC details the relationship between PIPEDA and the prevention of identity theft.[11] The fact sheet emphasizes how, under PIPEDA, businesses have the responsibility to protect customer information and reduce the risk of identity theft. One issue of increasing recurrence is that of data breaches:

> Sensational headlines about massive data breaches and the risk of identity theft have alarmed Canadians. The concern is clearly justified. This kind of fraud has claimed millions of victims across North America.
>
> …

---

8 A list of publications on identity theft can be found on the website of the Office of the Privacy Commissioner under the topic *Identity Theft and Fraud*.

9 Office of the Privacy Commissioner of Canada, *Fact Sheets: Truncated Credit Card Numbers*, December 2009. Credit card companies such as Visa and MasterCard now require retailers to truncate the card numbers on receipts.

10 Office of the Privacy Commissioner of Canada, *Fact Sheets: Best Practices for the use of Social Insurance Numbers in the private sector*, July 2004. See also Office of the Privacy Commissioner of Canada, *Fact Sheets: Social Insurance Number*, April 2008.

11 Office of the Privacy Commissioner of Canada, *Fact Sheets: Businesses and Identity Theft*, March 2007.

> [I]t is essential for businesses and other organizations — small and large — to develop comprehensive plans to protect the personal information they are entrusted with.
>
> Protecting personal information is the law in Canada.
>
> …
>
> What can businesses do to guard against identity theft? In a nutshell, they need to start handling personal information as they would actual cash. After all, personal information is a goldmine for identity thieves and organized criminals.
>
> Minimizing the identity theft risk means making the fundamental privacy principles enshrined under the *Personal Information Protection and Electronic Documents Act* (PIPEDA) part of an organization's culture.[12]

As noted in the OPC's 2012–2013 annual report to Parliament on the *Privacy Act,* "significant data breaches and leaks of personal information" are a growing concern for Canadian citizens.[13] Such breaches can increase the risk of identity theft.[14] In the report, the ex-Privacy Commissioner calls for mandatory data breach reporting in both the private and public sectors as a means to improve cybersecurity.

---

12 Ibid.

13 Office of the Privacy Commissioner of Canada, *Annual Report to Parliament 2012-2013: Report on the Privacy Act,* October 2013.

14 As noted by the ex-Privacy Commissioner, Jennifer Stoddart, with respect to an audit of breaches at the Canada Revenue Agency, "A breach involving an inappropriate access to — or disclosure of — sensitive taxpayer information can have serious impacts on the individual or individuals affected. In the worst case scenario, such a breach can result in identity theft, financial fraud and personal embarrassment for the affected taxpayers."

OVERVIEW OF THE ECONOMIC IMPACT OF IDENTITY THEFT AND FRAUD

A. Issues identified by credit reporting agencies

Consumer credit reporting agencies (also called credit bureaus), such as Equifax Canada, Forrest Green and TransUnion Canada, collect and market data about the credit history of consumers. According to the Financial Consumer Agency of Canada (FCAC), a federal regulatory agency whose mandate is to protect and inform consumers of financial products and services, the credit history of consumers summarizes the types of credit they use, such as credit cards, loans and financing plans.[15] The credit history also shows whether payments were made on time. It relies on information sent by consumer credit reporting agencies. These agencies provide information about the credit history of consumers in two ways: a credit report and a credit score.

Credit reports are based on the credit history of consumers and include their personal information, including their financial information, such as bank accounts, credit already in use (credit cards, lines of credit and loans), bankruptcy or court decisions that relate to credit, debts that were referred to collection, and a list of all the inquiries made about a consumer's credit.

Credit scores indicate the risk that a consumer represents to potential lenders, in comparison to other consumers. The credit reporting agencies use a scale from 300 to 900 to give a score to a consumer. The closer the score is to 900, the lower the agencies consider the risk to be for lenders.[16]

Equifax Canada

On behalf of Equifax Canada, John Russo addressed three key concerns about identity theft:

1. the steady rise in identity-related crime since 1998;
2. the existence of two types of identity theft: real and synthetic; and
3. the most worrisome aspects of identity theft and the steps consumers and businesses can take to avoid them.[17]

---

15 Government of Canada, Financial Consumer Agency of Canada, *About FCAC*.

16 Government of Canada, Financial Consumer Agency of Canada, *Credit Report and Credit Score*.

17 House of Commons, Standing Committee on Access to Information, Privacy and Ethics, (ETHI), *Evidence*, 2nd Session, 41st Parliament, 27 May 2014, 1105 (John Russo, Vice-President, Legal Counsel and Chief Privacy Officer, Equifax Canada Co.).

Mr. Russo explained that the rising number of data breaches, the increased use of electronic delivery channels and networks, and the influence of social media in our society has led to a steady rise in identity-related crime.[18] He drew on statistics from the Canadian Anti-Fraud Centre, noting that the number of Canadian identity theft victims increased by 14% in 2013.[19]

Mr. Russo noted that an identity-related crime always starts with the theft of personal information.[20] According to Equifax, the increase in the amount of personal information lost or stolen is due in part to rogue or careless employees or unauthorized access at various institutions ranging from retailers, health care providers, financial institutions and government.[21] Mr. Russo said that the increase in identity-related crime also stems from data breaches. He gave the following example: "[A]t our bureau, over the past 18 months, we have protected more than 1.5 million Canadian credit files with credit alerts or credit monitoring as a direct result of data breaches, and these numbers are steadily on the rise."[22]

Mr. Russo cited recent statistics demonstrating that "the bulk of these threats to personal information are through malicious or criminal attacks on an organization's database" and that "[d]ata breaches are truly becoming a treasure trove for fraudsters."[23] His remarks are based on a recent study by the Ponemon Institute, which found that 42% of identity-related incidents involved a malicious or criminal attack. The study also found that more consumers terminated their relationship with the company that had the breach; the average churn rate increased by 15% between 2013 and 2014.[24]

Mr. Russo mentioned that there are numerous cases where rogue employees, or "foot soldiers," sell personal information in credit applications from their place of employment to organized crime.[25] Many police investigations on identity theft show that stolen personal information is frequently found by chance during traffic stops and other searches.[26]

According to Mr. Russo, between 1998 and 2003 Canada experienced a 500% growth in identity theft reports. Growth leveled between 2004 and 2005, but in 2008

---

18 Ibid.

19 Ibid.

20 Ibid.

21 Ibid.

22 Ibid.

23 Ibid.

24 Ibid.

25 Ibid.

26 Ibid.

returned to the highs of 2003 when fictitious — or synthetic — identity crimes started to blossom.[27]

Synthetic or fictitious identity crime occurs when stolen personal information is used to make up a non-existent person or information about an identity is simply made up.[28] Mr. Russo explained that this type of identity is often created by using the SIN of someone who is deceased or who has not yet been granted credit, such as a child.[29] The perpetrator can then conduct hundreds of thousands of dollars in financial transactions before abandoning the identity of the synthetic person they originally created and disappearing without a trace.[30] According to Mr. Russo:

> [W]e commonly see tens, or even hundreds, of fictitious identities operated by the same group at the same time. Organized crime plays a big role in this, with the proceeds of these crimes being used to finance a wider range of other global activities, possibly even terrorism.[31]

Equifax Canada estimates that synthetic or fictitious identity fraud costs Canadians potentially $1 billion a year in losses.[32] According to Mr. Russo, fictitious identity creation generates tens of millions of dollars for organized crime groups each year.[33] Equifax sees on average 1,300 fictitious consumer files created each month in Canada by fraudsters and other organized criminals.[34]

As to the third point raised by Mr. Russo, that is, the most worrisome aspects of identity theft and the steps consumers and businesses can take to avoid them: the issues Equifax Canada has identified follow, while the proposed steps will be addressed later in this report.

Mr. Russo noted a study by ABI Research that found that “hacktivism” is on the rise: “hacktivism” now represents 47% of all activity around cyber-threat groups. The word “hacktivism” is a combination of the words “hack” and “activism” and is the illegal use of computers to promote a violent political agenda. Mr. Russo said hacktivist activities may not seem connected to identity theft on the surface, but the release of personal information that can later be used to create a synthetic or real identity poses a serious financial risk to consumers.[35]

---

27 Ibid.

28 Ibid.

29 Ibid.

30 Ibid.

31 Ibid.

32 Ibid.

33 Ibid.

34 Ibid.

35 Ibid.

Another source of concern for consumers and businesses, according to Mr. Russo, is that one in every three consumers affected by a data breach becomes a true victim of identity theft, as reported in a North American study by Javelin Strategy and Research.[36] This is up from one in four in 2012.[37]

In response to questions from Committee members, Carol Gray, President of Equifax Canada, said that 25% to 30% of Canadians request access to their credit file, and that this percentage varies with age — elderly people tend to access their credit file less frequently than younger people.[38] To give an idea of the volume of credit files at Equifax, Mr. Russo said that files from its members are accessed 150,000 times a day, and 50 million trade lines are updated each month.[39]

Forrest Green

On behalf of Forrest Green, Murray Rowe, Jr., President, focused his comments on First Nations communities and credit reporting agencies. He told Committee members that Forrest Green believes that First Nations communities are one of the most vulnerable to fraud and financial abuse.[40] A lack of credit bureau data on First Nations members means they are more susceptible to fraud.[41] Mr. Rowe described their situation as follows:

> In many cases, they don't understand the concept of how credit bureaus function. They rarely check their credit reports, and as a result, individuals I've spoken with are keenly monitored; they get a call from a collection agency....[42]

Moreover, according to Mr. Rowe, individuals on reserve are difficult to find in cases where an agency such as his wants to warn them that they have been victims of fraud.[43] As well, these individuals rarely contact credit reporting agencies.[44] Mr. Rowe presented the Committee with data showing that less than 5% of First Nations members have viewed their credit report: according to Mr. Rowe, the reality is closer to 1%.[45]

Mr. Rowe also drew the Committee's attention to identity verification. When people apply for low-wage jobs, data from credit reporting agencies is often used to analyze applicants' credit history.[46] Mr. Rowe finds it ironic that the people who are most

36 Ibid., 1110.

37 Ibid.

38 Ibid., 1135 (Carol Gray, President, Equifax Canada Co.).

39 Ibid., 1140 (Russo).

40 Ibid., 1115 (Murray Rowe, Jr., President, Forrest Green Group of Companies).

41 Ibid.

42 Ibid.

43 Ibid.

44 Ibid.

45 Ibid.

46 Ibid.

vulnerable and who most need a job are those who are most likely to be discriminated against because of a poor credit rating.[47] He believes relationships should be examined between lack of data or poor data, fraud, identity theft and vulnerability.[48]

Based on the conclusions of the House of Commons Standing Committee on Aboriginal Affairs and Northern Development, Mr. Rowe said Aboriginal communities tend not to trust organizations that gather data because they do not trust or have not bought into the concept of sharing data.[49]

TransUnion Canada

Todd Skinner, President of TransUnion Canada, told the Committee that TransUnion is regulated by consumer and privacy legislation and that consent is required to obtain a credit file.[50]

According to Mr. Skinner, identity theft falls into three categories: "a data breach or a compromise, the actual potential ID theft that happens as a result of that, and the fraud that occurs after that."[51]

Mr. Skinner noted that it is consumers and companies who inform TransUnion of data breaches.[52] However, companies do not always report their data breaches as recommended by the OPC in its publication titled "Key Steps for Organizations in Responding to Privacy Breaches."[53]

According to TransUnion's statistics, the number of data breaches reported over the past five years has decreased by 30%, while the number of potential victims has increased by 600%.[54] Mr. Skinner said that 8% of reported data breaches are from financial institutions, while 70% of these breaches are from the medical, service or retail industry.[55] Mr. Skinner noted that the number of data breaches reported from government, insurance companies and finance companies is very small.[56]

---

47 Ibid.

48 Ibid.

49 Ibid.

50 Ibid., 1120 (Todd Skinner, President, TransUnion Canada).

51 Ibid.

52 Ibid.

53 Ibid. See: Office of the Privacy Commissioner of Canada, Guidelines, *Key Steps for Organizations in Responding to Privacy Breaches*.

54 ETHI, *Evidence*, 2nd Session, 41st Parliament, 27 May 2014, 1120 (Skinner).

55 Ibid.

56 Ibid.

According to Mr. Skinner, the number of confirmed victims of identity fraud is up by 100%.[57] He noted that many consumers report these frauds to the Canadian Anti-Fraud Centre and that there has been a 300% increase in the number of fraud alerts placed.[58] He said, however, that there is still work to do.[59]

As to data breaches, Mr. Skinner said that the cost is borne by the consumer "unless the companies or government bodies that have caused the compromise are willing to step up and pay for the damages that are created."[60] Mr. Skinner told the Committee that the costs should be borne by the companies that compromise the consumer's personal information, even if not all companies do this or invest in solutions to mitigate the risk of these data breaches occurring.[61]

Mr. Skinner also drew the Committee's attention to the fact that there is no automated method whereby the private sector can confirm whether a particular piece of ID has been issued by the government or whether that actual ID belongs to the individual who claims it's theirs.[62]

B. Issues identified by the banking industry

Canadian Imperial Bank of Commerce

On behalf of the Canadian Imperial Bank of Commerce, Philip Fisher said that identity theft is not a new or growing issue, but an "evolving issue."[63] What has changed is how fraud is performed: the theft of receipts, bills or wallets or telephone-based fraud is over.[64] According to Mr. Fisher, it is now about advanced persistent threats, merchant breaches, malware and phishing.[65] The risk concerning the integrity of personal identity is no longer the same because of advances in technology and the dispersal of personal information across the Internet.[66]

For the Committee's study, Mr. Fisher highlighted the importance of agreeing on a common definition of identity theft. He said that financial institutions do not all use the same definition of identity theft, which in part explains the challenge in obtaining aggregate

---

57 Ibid.

58 Ibid.

59 Ibid.

60 Ibid., 1125.

61 Ibid.

62 Ibid.

63 ETHI, *Evidence*, 2nd Session, 41st Parliament, 29 May 2014, 1105 (Philip Fisher, Senior Director, eChannels Risk Management, Integrated Business Control Services, Canadian Imperial Bank of Commerce).

64 Ibid.

65 Ibid.

66 Ibid.

data on this problem.[67] Mr. Fisher cited the definition in the *Criminal Code*, which describes identity theft as knowingly obtaining or possessing another person's identity information for the purposes of committing an offence.[68] Identity information includes "name, address, date of birth, written signature, electronic signature, user name, credit card number, debit card number, financial institution account number, social insurance number, driver's licence, and password."[69]

According to Mr. Fisher, financial institutions typically use a narrower definition of identity theft and tend to monitor and report fraud based on type, which is generally based on the source of the stolen information or how it is exploited.[70]

He gave the copying of magnetic strip data at the point of sale or automated banking machines as an example. The information is typically used to create counterfeit cards or make card-not-present purchases.[71] According to Mr. Fisher, banks do not generally count this type of fraud as identity theft because of the limited amount of information involved.[72]

However, information obtained from a consumer's computer that is infected with malicious software is the type of fraud that is concerning because of the amount of information at risk and the difficulty in identifying the issue and remediating it.[73]

Mr. Fisher told the Committee about a type of fraud undergoing evolution: email fraud or phishing to collect personal information, such as sign-on credentials or credit card information, to access online accounts.[74] Mr. Fisher also said that fraudsters are increasingly attempting to broaden the types of information being stolen.[75]

Mr. Fisher gave other examples of fraud, like the theft of a person's mail and third-party data breaches, such as with merchants and data processors.[76] He said that, depending on the merchant, these breaches can involve large numbers of consumers.[77]

---

67 Ibid.

68 Ibid.

69 Ibid.

70 Ibid.

71 Ibid.

72 Ibid.

73 Ibid.

74 Ibid.

75 Ibid.

76 Ibid.

77 Ibid.

Other banks

Paul Milkman, on behalf of TD Bank Financial Group, made a distinction between the crime of identity theft and that of the active use of stolen identity to commit financial fraud.[78] Since there is a relationship between identity theft and financial fraud, he said that banks must have seamless prevention strategies for these two crimes and that banks' interests are aligned with those of their customers in preventing these crimes.[79]

Ed Rosenberg, from BMO Financial Group, said that the speed with which BMO's internal controls and processes evolve means that the quality and security of documents can be inconsistent across jurisdictions and that there are few reliable ways to universally authenticate documentation.[80]

RBC's representative, Jay Stark, said that, in addition to leading to substantial financial losses and other negative consequences for consumers, identity theft may fund further criminal activity, including terrorist activities.[81]

Mr. Stark noted that the various stakeholders who have appeared as part of the Committee's study have differing opinions on the definition and extent of identity theft as well as solutions to address this issue.[82]

Mr. Stark also noted that the banks' strategies have led to fraud migration: the use of chips and PINs has led to increases in cross-border and card-not-present fraud.[83]

---

78 Ibid., 1115 (Paul Milkman, Senior Vice-President, Head of Technology Risk Management and Information Security, TD Bank Financial Group).

79 Ibid.

80 Ibid., 1120 (Ed Rosenberg, Vice-President and Chief Security Officer, Legal, Corporate and Compliance Group, BMO Financial Group).

81 Ibid., 1125 (Jay Stark, Vice-President, Internal Audit Services, Personal and Commercial Banking, RBC).

82 Ibid.

83 Ibid.

STEPS TAKEN OR PROPOSED BY BUSINESSES TO PROTECT CANADIANS FROM IDENTITY THEFT

A. Measures taken or proposed by businesses to combat identity theft in Canada

Credit reporting agencies

Equifax Canada

According to Mr. Russo, from Equifax Canada, while Canadian businesses have taken a number of steps to prevent identity theft, there are only so many they can take.[84] He emphasized the sheer number of electronic transfers of personal information when processing financial transactions, with thousands of personal credit reports electronically transmitted every day.[85] Furthermore, thousands of credit applications, from bank loans to car financing, are processed every day.[86]

According to Mr. Russo, "[t]he financial services and credit industries continue to do their part for victims of identity-related crimes by investing millions of dollars each year to detect identity fraud as quickly as possible."[87]

Mr. Russo argued that, with fictitious identity creation on the rise, our laws, our security and our prevention tactics must change as criminals evolve.[88] He said that legislation, law enforcement and solutions from organizations like Equifax must all contribute to solving the problem.[89]

Mr. Russo took advantage of his appearance before the Committee to offer some advice to consumers. First, consumers should "check their credit file at least once every quarter to spot any abnormalities or possible fraud on their file."[90]

Second, victims of a data breach should ask the organization responsible for the breach to provide them, at its expense, with credit monitoring services for at least

84 ETHI, *Evidence*, 2nd Session, 41st Parliament, 27 May 2014, 1105 (Russo).

85 Ibid.

86 Ibid.

87 Ibid.

88 Ibid.

89 Ibid.

90 Ibid.

12 months following the breach.[91] According to Mr. Russo, it is during the 12 months following a data breach that most identity theft crimes are committed.[92]

Third, Mr. Russo said that consumers must be vigilant and not provide unnecessary personal information, such as a social insurance number or date of birth, for a simple retail or rental transaction.[93]

In short, combatting identity-related crime starts with education and awareness from Canadian households and consumers, according to Mr. Russo.[94] Education and awareness is especially important in light of data breach incidents where corporations have been hacked or maliciously attacked for consumers' sensitive and confidential personal information.[95]

In response to questions from Committee members about ways to encourage consumers to request access to their credit report, Mr. Russo said Equifax Canada works with schools in the Junior Achievement program to educate young Canadians about what a credit report is, how to read it and what impacts their credit score in preparation for when they are able to access credit.[96] Tara Zecevic, also from Equifax Canada, added that education and financial literacy are key components of preventing consumer debt.[97]

Forrest Green

According to Mr. Rowe, from Forrest Green, education will help reduce the vulnerability of First Nations members with respect to identity fraud caused by not having credit data.[98] According to Mr. Rowe:

> We need to talk and we can't just rely on leaders today. They haven't been educated. They can't tell their children how to formulate a good credit report because no one's told them, no one's educated them.[99]

Mr. Rowe said there is a link between this need for financial education and the discrimination First Nations members face in obtaining credit from financial institutions. An informal survey done by Forrest Green of five bands found that interest rates are 300% higher for Aboriginal communities, even after ministerial loan guarantees are taken

---

91 Ibid.

92 Ibid.

93 Ibid., 1110.

94 Ibid., 1105.

95 Ibid.

96 Ibid., 1220.

97 Ibid., 1220 (Tara Zecevic, Vice-President, Decision Solutions, Equifax Canada Co.).

98 Ibid., 1115 (Rowe).

99 Ibid.

into account, which guarantee 100% of the loan.[100] According to Mr. Rowe, the systemic problem in the banking community with Aboriginals and the way credit reporting agencies gather and distribute information are problems that need to be examined with Aboriginal communities.[101]

TransUnion Canada

TransUnion's data shows a lack of awareness in industries outside the financial sector about the problem of identity theft.[102] The solution is for more education in this area on the obligations resulting from a data breach and security protocols to prevent such a breach.[103]

In the same vein, Mr. Skinner said TransUnion supports the provisions of Bill S-4 concerning data breach notification.[104] He said that, while he did not want consumers to be inundated with notifications, there were benefits to customers receiving notification where there is a material risk of harm.[105]

According to Mr. Skinner, data breaches increase call volumes to TransUnion and Equifax centres and requests for alerts to consumer disclosures.[106] He said these organizations have invested in technology to make their response to consumers as effective as possible and to help contribute to the 300% increase in the number of fraud alerts placed by consumer bureaus he alluded to earlier.[107] Mr. Skinner said that the measures taken by credit reporting agencies reduce the number of cases of fraud and that he is pleased that this number is not increasing at the same rate as potential victims.[108]

Mr. Skinner stressed that the first thing to do in the event of a data breach is to notify the OPC.[109] In this regard, Mr. Skinner informed the Committee that TransUnion supported the amendments to PIPEDA in Bill S-4. According to Mr. Skinner, after an

---

100 Ibid., 1140.

101 Ibid.

102 Ibid., 1125 (Skinner).

103 Ibid.

104 Ibid. On 21 April 2015, the House of Commons Standing Committee on Industry, Science and Technology adopted Bill S-4, An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act, and reported it to the House the next day without amendment.

105 ETHI, *Evidence*, 2nd Session, 41st Parliament, 27 May 2014, 1125 (Skinner).

106 Ibid.

107 Ibid.

108 Ibid.

109 Ibid.

organization has confirmed a loss of financial data, it must notify Equifax and TransUnion, which, in turn, should place fraud alerts to reduce the likelihood of identity theft.[110]

TransUnion's Measures consist of working with police authorities to report suspected activities, according to Mr. Skinner. TransUnion receives information about suspected activities, enters it into its fraud database, and reports it to financial institutions.[111] Preventing these crimes requires better technology to ensure that identity cards are not easily replicated and authenticated.[112] Moreover, truly solving the problem requires the sharing of information between government agencies and the financial sector.[113] According to Mr. Skinner, fraudsters take advantage of this lack of sharing.[114]

Given the lack of an automated method allowing the private sector to confirm whether a piece of ID has been issued by the government or whether the ID actually belongs to the individual who claims it's theirs, Mr. Skinner argued that TransUnion and Equifax Canada could help by "being the conduit to financial institutions," since they already provide identity verification in their Anti-Money Laundering and Know Your Customer monitoring.[115]

In response to questions from Committee members about how to encourage consumers to request access to their credit report, Ms. Banfield said that, in addition to campaigns in schools, a lot of information is available on TransUnion's website from their work with police services and many agencies.[116]

Banking industry

Canadian Imperial Bank of Commerce

According to Mr. Fisher, from the Canadian Imperial Bank of Commerce, some identity theft issues flagged by the banking industry over time have led to mature and robust controls to identify and respond to them.[117] However, other identity theft issues are newer and controls are still evolving.[118]

---

110 Ibid.

111 Ibid.

112 Ibid.

113 Ibid.

114 Ibid.

115 Ibid. On this point, Mr. Skinner referred to the RCMP document, "National Identity Crime Strategy."

116 ETHI, *Evidence*, 2nd Session, 41st Parliament, 27 May 2014, 1220 (Ms. Chantal Banfield, Vice-President and General Counsel, TransUnion Canada).

117 ETHI, *Evidence*, 2nd Session, 41st Parliament, 29 May 2014, 1105 (Fisher).

118 Ibid.

Mr. Fisher said that, even though financial institutions have fraud detection controls in place, to effectively combat identity theft there needs to be a coordinated effort among financial institutions, consumers and government.[119] As an example of this partnership, Mr. Fisher noted the anti-tamper hardware on automated banking machines (ABMs), which has led to a sharp decline in ABM tampering.[120]

While emphasizing the important role consumers play in combatting identity theft, he noted that consumers are not fraud specialists and need financial institutions and government agencies to inform them about the risks and provide them with the tools to protect themselves against identity theft.[121] Good examples of the tools available are transactional alerts and free credit bureau monitoring offered by some financial institutions.[122]

Mr. Fisher also emphasized the government's role in protecting consumers from identity theft and advocated for stronger controls in this area.[123]

TD Bank Financial Group

Mr. Milkman believes preventing identity-related crime is a shared responsibility between banks and their customers.[124] In this regard, TD Bank Financial Group has a four-step process aimed at making its customers responsible for protecting their personal information by asking them to:

1. be careful about sharing information: ask how the information will be used, why it is needed, with whom it will be shared, and how it will be safeguarded; never disclose their personal information number, social insurance number or passwords; and not use banking passwords with social media;[125]

2. use appropriate security measures: keep account statements in a safe place and take advantage of technologies that enhance security and privacy when using the Internet, such as digital signatures, anti-virus software, personal firewalls and data encryption;[126]

---

119 Ibid.

120 Ibid., 1110.

121 Ibid., 1105.

122 Ibid.

123 Ibid.

124 Ibid., 1115 (Milkman).

125 Ibid.

126 Ibid.

3. check statements for accuracy: check account statements or online statements to ensure all transactions and charges are correct and access their credit report from a credit reporting agency once a year to ensure it is accurate;[127]

4. guard their cards, cheques and ID: when travelling, carry only the credit cards they need; do not carry their social insurance card; and make a list of all their cards and numbers and store this list securely.[128]

According to Mr. Milkman, banks "make significant investments to maintain strong security standards to protect our systems and customer information against unauthorized access and use."[129] For example, he said that TD's systems have been designed to "ensure that the personal identification number, password, or other access codes are always held private and confidential."[130]

According to Mr. Milkman, banks have taken steps to make online transactions more secure.[131] For example, Mr. Milkman said that at TD these steps include:

> [C]omprehensive threat intelligence, access management controls, transaction logging and analysis, secure firewalls, constant monitoring to proactively identify unusual customer account activity, phishing and spam protection, and the highest levels of encryption available to ensure that data can only be decoded and read by the customer or byour system.[132]

BMO Financial Group

On behalf of BMO Financial Group, Ed Rosenberg gave the Committee examples of steps the bank has taken to combat identity theft, such as hosting anti-fraud sessions for its employees, making anti-phishing brochures available for its branch customers, providing fraud avoidance tips on its bank statements, and getting out its prevention message on Twitter and Facebook.[133]

Mr. Rosenberg emphasized the cooperation between bank management and employees to develop programs to prevent and detect criminal risk in such areas as

---

127 Ibid.

128 Ibid.

129 Ibid.

130 Ibid.

131 Ibid.

132 Ibid., 1120.

133 Ibid. (Rosenberg).

managing cash, credit and transaction processing, client and financial information management, and regulatory compliance.[134]

Mr. Rosenberg said that BMO Financial Group collaborates on initiatives organized as an industry by and through the Canadian Bankers Association (CBA) to identify criminals and work with law enforcement to prosecute them.[135]

According to Mr. Rosenberg:

> The adoption of chip and PIN standards alone has cost the industry millions of dollars to reduce the risk of card fraud in Canada.[136]

Mr. Rosenberg said that the use of new technologies by organized crime has led the banking industry to put industry forums and collaborative tools in place to share fraud-related information and preventive controls.[137] Most notably through the CBA, banks liaise with various parties, for example Internet service providers for cybercrime, insurance companies for common fraud, and law enforcement agencies for sharing trends.[138] Mr. Rosenberg added that this type of collaboration is also done internationally.[139]

RBC

According to Mr. Stark, from RBC, an appropriate response to identity theft must optimize relationships among the following "four fraud management pillars:" consumer impact or inconvenience, fraud losses, the cost to banks and society, and risk management.[140]

Mr. Stark said that the fight against fraud must balance what he called "key fraud management strategies:" intelligence; prevention, such as consumer awareness and education; detection; and regression or root cause analysis.[141] In his opinion, the most powerful fraud strategies in the past decade have been advancements in detection analysis.[142]

---

134 Ibid.

135 Ibid.

136 Ibid.

137 Ibid.

138 Ibid.

139 Ibid.

140 Ibid., 1125 (Stark).

141 Ibid.

142 Ibid.

Mr. Stark said the strategies have been successfully applied to various schemes, including debit and credit card lending and cheque fraud.[143] According to Mr. Stark, RBC's fraud losses last year were the lowest in over a decade.[144]

Scotiabank

On behalf of Scotiabank, Jennifer Frook focused her remarks on the following points related to identity theft: training and education, prevention, detection and mitigation, and collaboration.[145] She said that at Scotiabank an important part of protecting its customers from identity theft and other forms of fraud is providing its staff with training and empowering its customers with information on data security.[146]

As an example of steps taken by Scotiabank to ensure the integrity of its customers' information, Ms. Frook said that chip technology, which is already used by all Canadian banks in the credit cards and debit cards they issue, is also used in Scotiabank ATMs.[147] Scotiabank debit cards are also equipped with Interac Flash technology, which uses secure chip processing technology to prevent skimming and counterfeit fraud.[148] Its retail credit cards are equipped with a similar Visa payWave functionality.[149]

Ms. Frook also mentioned an alert service that sends Scotiabank customers emails or text messages to help them monitor activity on their accounts.[150]

Ms. Frook said that, in the channels and products offered by Scotiabank, there are fraud controls in place to detect suspicious activity and prevent fraudsters from accessing its system.[151]

Ms. Frook also explained the steps banks take when customers' personal identification information is stolen: they first notify the customer that their card and/or account was compromised and then block the stolen credential and replace it with a new one, for example by replacing a comprised credit card or by resetting the customer's password.[152]

---

143 Ibid.

144 Ibid.

145 Ibid., 1130 (Jennifer Frook, Director, Shared Services, Fraud Management Office, Scotiabank).

146 Ibid.

147 Ibid.

148 Ibid.

149 Ibid.

150 Ibid.

151 Ibid.

152 Ibid.

According to Ms. Frook, Scotiabank monitors account activity for fraudulent or suspicious transactions.[153] It updates customer profiles to include notes that the customer had been a victim of identity theft so that bank employees can take appropriate steps when authenticating customers on their account.[154] According to Ms. Frook, Scotiabank indemnifies customers who have been victims of identity theft for their loss and makes them whole.[155]

Ms. Frook also said that "[b]anks also collaborate and voluntarily report to the OPC any material or systemic breaches of personal information."[156]

As to the collaboration made necessary because identity theft nearly always takes place outside the banking environment, Ms. Frook said that Scotiabank provides information on its own internal tracking of fraud to other organizations such as Visa, American Express, Interac, law enforcement agencies, and the CBA.[157]

According to Ms. Frook:

> These groups also compile information from other financial institutions and provide industry metrics and benchmarks from which we can measure our own mitigation of various types of fraud, many of which were enabled by some sort of theft of a customer's personal information.[158]

As an example of this type of collaboration, Ms. Frook said that the CBA fraud specialists group has a mandate to work together on fraud prevention and share information and best practices.[159]

Information technology companies

Rogers Communications

On behalf of Rogers Communications, Kenneth Engelhart shared a report with the Committee, published that very morning, on the number and types of information requests on Rogers' clients that the company received from government and law enforcement

153 Ibid.

154 Ibid.

155 Ibid.

156 Ibid.

157 Ibid., 1135.

158 Ibid.

159 Ibid.

agencies in 2013.[160] Rogers encouraged the federal government to "issue its own report to shed more light on these requests."[161]

The table below shows the six types of requests established by Rogers and the number of requests it received in each category.

Breakdown of 2013 Requests

Customer name/address checks	87,856
Court order/warrant	74,415
Government requirement letter (compelled to provide under a federal/provincial law)	2,556
Emergency requests from police in life-threatening situations	9,339
Child sexual exploitation emergency assistance requests	711
Court order to comply with an international Mutual Legal Assistance Treaty request	40
Total	174,917

Notes:

1. These statistics include the following scenarios: (a) The information requested was provided; (b) Partial information was provided; (c) No information was provided because it doesn't exist or the person is not a Rogers customer; and (d) We rejected the request or successfully fought it in court.

2. These statistics do not include informal requests such as phone calls from law enforcement looking for information they would require a warrant for. These requests are rejected because there is no legal authority and no formal response is provided.

Source: Rogers Communications, *2013 Transparency Report*, p. 2.

The report notes for each category the legal authority under which Rogers provides information, such as the PIPEDA, the *Criminal Code*, or the *Income Tax Act*.

It should be noted that the report does not show the number of requests that resulted in Rogers actually releasing the information. In this regard, Mr. Engelhart made the following clarification:

---

160 ETHI, *Evidence*, 2nd Session, 41st Parliament, 5 June 2014, 1110 (Kenneth Engelhart, Senior Vice-President, Regulatory and Chief Privacy Officer, Rogers Communications Inc.). The report is called the *2013 Transparency Report*.

161 Ibid.

> [W]e do not answer all requests that we receive. If we consider an order to be too broad, we push back and if necessary go to court to oppose the request.[162]

According to Mr. Engelhart, the category that attracts the most attention is customer name and address checks.[163] Mr. Engelhart said that very often the police are not sure which carrier they need to seek a warrant for. For example, they may ask Rogers to verify whether a person who lives at a certain address or who has a certain phone number is a Rogers customer.[164] In such cases, Rogers responds yes or no, according to Mr. Engelhart.[165]

Rogers believes this collaboration with the police is useful because the information provided to police stops them from seeking a warrant against the wrong carrier or the wrong person.

Mr. Engelhart noted that some American agencies have expressed great interest in acquiring metadata without search warrants. Mr. Engelhart assured the Committee that Rogers had not, does not and would not release metadata to any law enforcement agency in Canada without a search warrant.[166]

Google

With respect to the transparency report shared by Rogers Communications representatives during their testimony before the Committee, Colin McKay, from Google, noted that Google publishes a similar report every six months on its website.[167] It is interesting to note that Google's report on Canadian user data requests shows that Google produced "some data" for 33% of the requests made between January and June 2014.[168]

Providing examples of easy-to-guess passwords, Mr. McKay said that experience has shown that the weakest link in the information security chain is often the user.[169]

According to Mr. McKay, Google builds systems and tools that alert its users to possible attempts to access their accounts and information, gives them information about

---

162 Ibid.

163 Ibid.

164 Ibid.

165 Ibid.

166 Ibid.

167 Ibid., 1115 (Colin McKay, Head, Public Policy and Government Relations, Google Inc.).

168 Google, Transparency Report, User data requests, *Canada*. Google also provides a list of businesses that have published transparency reports, including Rogers and Telus.

169 ETHI, *Evidence*, 2nd Session, 41st Parliament, 5 June 2014, 1115 (McKay).

sites that may try to inject malware and take over their computer, and invests a lot of effort to make the most secure networks in the world.[170]

Mr. McKay emphasized the track record of Google's email service, Gmail, when it comes to protecting users from spam.[171] According to Mr. McKay:

> [W]hen a spammer tries a new type of junk mail, our systems often identify and block it from Google accounts within minutes and if it does happen to land in your inbox, you could press one button sending our systems a signal that we should consider similar messages as spam.[172]

As to search results on the Google website, Mr. McKay said that Google's technology examines billions of URLs across the web, looking for sites that could inject malicious code into users' computers, trick users into downloading software containing a virus, or try to pass off a phishing site as a legitimate financial site.[173]

Mr. McKay noted that each day Google finds more than 7,500 unsafe sites and shows warnings on up to six million Google search results and one million downloads.[174]

According to Mr. McKay, more than one billion users are protected against phishing and malware every day because of warnings Google shows users about unsafe websites.[175] Moreover, Google shares this data with other browsers, like Safari and Firefox.[176]

Mr. McKay said that Google's offices in California, New York, Munich, Zurich and Montreal have a team of more than 250 security engineering experts whose job is to help the company remain competitive in information security.[177]

Mr. McKay told the Committee that in 2011 Google had launched a two-step verification process in which users had to verify their identity with a password and another passcode delivered to a phone or separate USB device on their computer, for example.[178] According to Mr. McKay, this two-step process provides a stronger layer of sign-in security.[179]

---

170 Ibid.

171 Ibid.

172 Ibid.

173 Ibid.

174 Ibid.

175 Ibid.

176 Ibid.

177 Ibid.

178 Ibid., 1120.

179 Ibid.

As to networks, Mr. McKay said that over the past year Google had expanded session-wide Secure Sockets Layer (SSL) encryption to open by default when users sign in to Gmail, Google Search, Google Docs and other services.[180] According to Mr. McKay, this protection stops others from snooping on a user's activity when they are on an open network.[181]

Mr. McKay also noted that Google has encrypted the data that flows between its data centres and that its security experts are continually extending and strengthening this protection across more services and links.[182]

Mr. McKay added that Google has paid out nearly $3 million over the past four years to identify security exploits and weaknesses in its programs and services, and patches are rolled out to resolve the issues identified by security researchers.[183]

The Committee believes it is good practice for information technology companies to publish a report showing requests from government agencies for the release of personal information. The Committee notes that this type of report is more useful when it shows how often a company actually released information.

180 Ibid.

181 Ibid.

182 Ibid.

183 Ibid.

CRITIQUES OF THE MEASURES TAKEN BY BUSINESSES AND SUGGESTED IMPROVEMENTS

A. Committee members' questions to the credit reporting agencies

In response to questions from members of the Committee regarding the fees consumer credit reporting agencies charge to send credit files electronically, representatives from these agencies explained that they charge these fees because they have to cover the cost of keeping offices open for consumers, which is required under Canadian law.

Property and civil rights being an exclusive power of the provinces under the Canadian Constitution, which includes contractual relations and consumer protection, many provinces have adopted statutes aimed at the consumer credit reporting agencies' activities. Some of these provincial statutes provide that credit agencies must have a place of business open to the public in their province.[184] With respect to federal legislation, PIPEDA, insofar as it applies, imposes certain obligations on these organizations regarding the protection of personal information.

Ms. Banfield, appearing on behalf of TransUnion, said that the costs incurred by TransUnion also included investing in telephone technologies, such as interactive voice response systems, so consumers can confirm their identity over the phone and then have their credit file mailed to them.[185] Mr. Russo, appearing on behalf of Equifax, pointed out that consumers can access their credit file 365 days a year.[186] Access is free if they request their credit file by mail; however, online access costs $15.50 through Equifax.[187]

These two witnesses explained the practice in place at Equifax and TransUnion — to have consumers pay to access their credit files — by comparing Canadian and American legislation.[188] In the United States, the *Fair and Accurate Credit Transactions Act of 2003* gives consumers the right to consult their credit file online for free once a year.[189] Equifax and TransUnion use the system they do because Canadian legislation does not include a similar requirement, but imposes other requirements that involve additional costs.

---

184 For example, subsection 4.2(1) of Prince Edward Island's *Consumer Reporting Act* provides that "Every consumer reporting agency registered under this Act shall operate from a fixed place of business in Prince Edward Island that shall be open to the public during normal business hours."

185 ETHI, *Evidence*, 2nd Session, 41st Parliament, 27 May 2014, 1130 (Banfield).

186 Ibid., (Russo).

187 Equifax Canada, *Equifax Credit Report*.

188 ETHI, *Evidence*, 2nd Session, 41st Parliament, 27 May 2014, 1130 (Banfield and Russo).

189 United States Government, *Fair and Accurate Credit Transactions Act of 2003*, section 211.

In response to questions from Committee members about making legislative changes so credit reporting agencies could reduce expenses and offer information to consumers electronically, Ms. Banfield said that they have advocated for these changes every time consumer reporting legislation has been reviewed in the various provinces.[190] Mr. Russo added that it is not just provincial legislation that imposes obligations on credit reporting agencies, but also PIPEDA, and that amendments to that act would also have to be made.[191]

The Committee believes that the questions it put to the consumer credit reporting agencies regarding charging fees to consumers to receive a credit file electronically were not adequately answered. In particular, the Committee notes that there is no causal link between the legislation these agencies are subject to and their decision to charge consumers a fee to receive their credit files electronically. In light of all the testimony heard as part of its study, the Committee is of the opinion that giving consumers increased access to their credit files would contribute to reducing identity crimes.

Recommendation 1: The Committee urges consumer credit reporting agencies to provide Canadian consumers with electronic access to their credit file free of charge at least once a year.

B. Critiques of the Measures Taken by Businesses and Suggested Improvements by Academics and Experts in the Field

José Manuel Fernandez, Professor at the École polytechnique de Montréal

José Manuel Fernandez, Professor at the École polytechnique de Montréal, used the example of the Heartbleed bug, which affected the web servers of the Canada Revenue Agency (CRA) and led to the unauthorized disclosure of at least 900 social security numbers of Canadian taxpayers, to illustrate that the information technology (IT) infrastructure in place in Canada represents a risk in terms of identity theft.[192] According to Mr. Fernandez, "Heartbleed is really about the pitiful state of our information infrastructure and how we have let it become that way."[193]

Mr. Fernandez explained that the social insurance numbers that were leaked could be used by fraudsters to steal the victims' identities and then carry out fraudulent banking transactions, ruin their credit histories or gain unauthorized access to computer email accounts and social networking accounts.[194]

---

190 ETHI, *Evidence*, 2nd Session, 41st Parliament, 27 May 2014, 1150 (Banfield).

191 Ibid., (Russo).

192 ETHI, *Evidence*, 2nd Session, 41st Parliament, 29 April 2014, 1100 (José Manuel Fernandez, Assistant Professor, Department of Computer and Software Engineering, École Polytechnique de Montréal, As an Individual).

193 Ibid.

194 Ibid.

However, Mr. Fernandez also said that identity theft is only one problem among many, and that it is probably one of the least important ones. He believes that identity theft is just the tip of the iceberg.[195]

Rather, Mr. Fernandez believes the most important considerations for data security are "cybercrime, cyber-espionage, cybersabotage, and their impending doom."[196]

According to Mr. Fernandez, "credible experts have estimated the cost of cybercrime worldwide at hundreds of billions of dollars a year."[197] He mentioned that Symantec, an information software company, estimated that the cost of cybercrime in Canada was $3 billion in 2013.[198]

To illustrate that cybercrime is alive and well, Mr. Fernandez added that

> [c]ybercriminals use infected computers in corporations, government offices, and in homes of unsuspecting consumers, to turn a profit by a variety of means. This can include Internet banking fraud, which is the most common, but also Internet publicity fraud, extortion, and also traditional forms of fraud and con artistry.[199]

Mr. Fernandez believes that cybercrime is a growth industry with international ramifications that "involves a complex network of criminal groups that work together."[200] He referred to survey results published by the European Union that show that between 30% and 35% of the users surveyed reported that their computers had been infected in the last year.[201]

Mr. Fernandez held a clinical trial at the École Polytechnique in 2012 with 50 subjects whose personal computer activity was monitored for four months. The findings showed that 5% of their computers were infected by dangerous malware and that 20% of them were infected by some kind of harmful software, despite the fact that they all had up-to-date anti-virus software installed.[202] Mr. Fernandez's analysis showed that, "if none of them had any anti-virus installed, 38% of them would have been infected."[203] He concluded that would mean that two out of every five Canadians could have infected computers.[204]

---

195 Ibid.

196 Ibid.

197 Ibid.

198 Ibid.

199 Ibid.

200 Ibid.

201 Ibid.

202 Ibid., 1105.

203 Ibid.

204 Ibid.

According to Mr. Fernandez, cybercriminals have been investing their phenomenal profits in research and development and they have developed hacking tools and techniques that baffle computer security experts:[205]

> [I]t's probable that they have overall been investing more R and D in developing the tools than all of the computer security industry. So we're losing the war. We are in an arms race and from a technical point of view we're losing and we know that. We don't say it very often very publicly, but it is true.[206]

Mr. Fernandez also noted that, more and more, banks are starting not to pay when their clients are victims of cybercrime.[207]

According to Mr. Fernandez, the technological advantage held by cybercriminals has been used for other purposes in the past, such as child pornography, which led law enforcement to establish specialized teams.[208] But this technological advantage has also led to the cyber-espionage and cybersabotage threat:

> We're just starting to find out right now how much foreign intelligence agencies and foreign economic interests have been rifling through our computers here, government computers, Canadian businesses, and Canadian citizens, for over a decade.[209]

The root causes of identity theft, cyber-espionage and cybersabotage are all linked to how our IT infrastructure is managed, said Mr. Fernandez. He pointed out that computer and Internet technologies are being used for purposes other than those originally intended:

> A case in point is the World Wide Web. The World Wide Web was invented by researchers in Switzerland to have an interactive way of sharing research data, and 30 years later it's running the worldwide economy. It wasn't meant for that.[210]

Mr. Fernandez said that security and accountability mechanisms were not built into these technologies.[211] However, he added that technological solutions have been developed, and they are being taught in engineering schools.[212] It is the incentives to implement these technological solutions that are missing.[213]

In conclusion, Mr. Fernandez said that various sectors of society will have to collaborate, including professional associations, educators, industry, the public service and

---

205 Ibid.

206 Ibid.

207 Ibid.

208 Ibid.

209 Ibid.

210 Ibid.

211 Ibid.

212 Ibid., 1110.

213 Ibid.

law enforcement agencies, in order to attack the root causes of the problems he identified, and that appropriate legislative measures will also be needed.[214]

Susan Sproule, Professor, Brock University

Susan Sproule, Assistant Professor in Finance, Operations and Information Systems at Brock University, began by saying that one of the key points to consider in fighting identity theft and identity fraud is that they are two different problems.[215] She explained the distinction as follows:

> Identity theft is a problem of personal and agency guardianship, that is, keeping personal information secure. Identity fraud is a problem of authentication, or being able to determine that the person who is presenting identification is really who they say they are.[216]

According to Ms. Sproule, this distinction is important because both crimes can occur separately: the identity thief and the fraudster are usually two different people.[217] Furthermore, she said that cases of identity theft, including data breaches, are rarely linked to cases of identity fraud because the information goes through an intermediary.[218]

While pointing out that everyone has a responsibility to look after their own personal information, which means keeping identification documents secure and not giving out personal information unnecessarily, she noted that it is impossible to prevent identity fraud.[219] She said, "Once my information has been compromised, the only thing I can do is help detect it and report it as soon as possible."[220]

Ms. Sproule also believes that organizations have a role to play in preventing both identity theft and identity fraud:[221]

> They can prevent identity theft by keeping any of my information they possess secure. They can prevent identity fraud by ensuring they have proper authentication processes in place whenever identification is issued or is checked.[222]

She added that organizations are responsible for detecting identity fraud as well as identity theft when personal information has been compromised.[223] Another indication that

---

214 Ibid., 1115.

215 Ibid., 1120 (Susan Sproule, Assistant Professor, Finance, Operations and Information Systems, Brock University, As an Individual).

216 Ibid.

217 Ibid.

218 Ibid.

219 Ibid.

220 Ibid.

221 Ibid.

222 Ibid.

identity theft and identity fraud are two different issues is that two different areas within an organization are responsible for them: security services are responsible for physical security and IT services are responsible for systems security.[224]

Ms. Sproule pointed out that many of the challenges in addressing identity theft and fraud are linked to the terminology being used: many members of the general public do not know what these terms mean.[225] Added to this lack of understanding among potential victims is an overall lack of information about the problem.[226] She said:

> Credit card fraud and debit card fraud are investigated and handled internally by the credit card companies and the banks. Only a small proportion of those cases are ever referred to police. A Statistics Canada survey on fraud in retail businesses showed that between 40% and 50% of cases were never reported to police. Less than 40% of individual victims ever report to police.[227]

She explained that businesses tend to fear negative publicity, and victims do not want to admit that they failed to protect their personal information.[228] Both businesses and individuals often believe that the police cannot do anything, she said, and in many cases they are right.

Organizations bear most of the financial loss associated with identity theft and fraud, which Ms. Sproule believes causes two problems: first, the organizations are reluctant to reveal what these costs are and, second, "the costs alone don't provide strong incentives to prevent identity theft and fraud."[229] She mentioned that losses due to identity fraud are passed on to consumers in the form of higher prices, fees or rates.[230]

Ms. Sproule also pointed out that the lack of data breach notification requirements in Canadian legislation means that the reputation of organizations whose data is breached may not even suffer.[231] She was pleased that Bill S-4 includes measures to address this issue.[232]

As regards the overall cost of identity theft and fraud to society, Ms. Sproule mentioned that various studies show that between 20% and 40% of consumers say they have adjusted their online behaviours because they are concerned about identity theft.

---

223 Ibid.

224 Ibid., 1125.

225 Ibid.

226 Ibid.

227 Ibid.

228 Ibid.

229 Ibid.

230 Ibid.

231 Ibid.

232 Ibid.

She believes this means that Canadian businesses are not benefiting from all of the advantages that electronic commerce should be bringing.[233]

Ms. Sproule made two recommendations to the Committee. First, she said that credit reporting agencies should be more responsive to consumers.[234] She believes that, in order for consumers to be able to detect fraud, they must have increased access to and greater control over their credit files.[235] She summarized the credit file issue as follows:

> Credit reporting agencies have to provide a free copy of your credit report each year, but they make this as difficult as possible. To get a free copy, you have to fill out a form, copy a multitude of documents, send it all off in the mail, and wait a couple of week[s] for them to mail you back a report. They provide online service. Online service is more secure, and it has to be less expensive to provide, but they'll charge you $24 for that.[236]

As for theft protection products, which Equifax and TransUnion offer for $15 to $17 a month, Ms. Sproule made the following observation: "By offering these products, they are profiting from the problem, which provides little incentive for them to reduce or eliminate the threats."[237]

Ms. Sproule's second recommendation addressed the need to collect data regularly and periodically so trends can be identified and "effective educational initiatives and effective policy" can be designed.[238] Like other witnesses, she believes that, since there is no single measure for identity theft and fraud, an identity theft and fraud index is needed, which would work like a consumer price index or a purchasing activity index.[239] In her words,

> [t]his index would bring in information from regular surveys of consumers, surveys of businesses, as well as reports from law enforcement, from credit reporting agencies, from privacy commissioners, victim services, and any other groups.[240]

The Committee recognizes the merits of these recommendations about credit reporting agencies and establishing an identity theft and fraud index.

Benoît Dupont, Director, International Centre for Comparative Criminology

In line with Ms. Sproule's testimony, Benoît Dupont emphasized the lack of information about the current scope of the problem. He said that there is not enough

---

233 Ibid.

234 Ibid.

235 Ibid.

236 Ibid.

237 Ibid., 1130.

238 Ibid.

239 Ibid.

240 Ibid.

information on the actual number of victims and the evolution of this trend, no clear breakdown of the types of identity theft, and not enough information on the identity thieves themselves.[241]

According to Mr. Dupont, the lack of information also extends to what is known about organizations — which ones are most effective in the fight against identity theft, which ones are most exposed, and which ones have been successful at preventing identity theft.[242]

With regard to banks in particular, Mr. Dupont noted that they invest significant amounts in anti-fraud technologies and have an advanced capacity to identify and block identity theft attempts.[243] However, the lack of information about identity theft means that

> we don't know which one of the five or six big banks perform the best, and also the worst, and what types of retail or service businesses are leaking disproportionate amounts of personal information to offenders. All organizations are not equal when faced with the problem of identity theft. [244]

Mr. Dupont explained that the missing information could be used to help design and implement more effective prevention strategies "that would target and reinforce the weakest points in the payment ecosystem first."[245] Furthermore, it could be used to better inform stakeholders about the need to create new regulatory tools that would compel companies to protect their customers' personal information and notify them when a breach occurs, not only from a privacy perspective but also from a security perspective.[246] According to Mr. Dupont, the missing information would also help ensure that these regulatory tools are reasonable and do not unduly burden businesses.[247] In addition, this information would help the International Centre for Comparative Criminology and especially law enforcement agencies focus their limited resources on the most dangerous and prolific offender networks.[248]

On a more positive note, Mr. Dupont identified several measures that have helped reduce the number of cases of identity theft and fraud in Canada in recent years, such as chip and PIN technology on credit and debit cards, and advances in anti-fraud technologies in the banking sector. He believes that these measures show that organizational changes can produce systemic outcomes across the country.[249]

---

241 Ibid., (Benoît Dupont, Director, International Centre for Comparative Criminology).

242 Ibid., 1135.

243 Ibid.

244 Ibid.

245 Ibid.

246 Ibid.

247 Ibid.

248 Ibid.

249 Ibid.

However, the problem with chip and PIN technology is that the United States has been slower to adopt this technology, so fraudsters can still capture data from the magnetic stripes on the back of credit and debit cards.[250]

Mr. Dupont used statistics from Interac to calculate that the total amount of dollar losses attributed to fraud by Interac decreased by 36% between 2004 and 2012, even though the number of transactions conducted by debit card had increased by 53%.[251] This means that fraud is decreasing while the number of transactions is increasing.

Mr. Dupont observed a similar trend for credit cards: total losses increased by 94% between 1999 and 2012, but credit card transactions increased by 212%.[252] He also calculated that the average loss per dollar was about 2¢ for Interac transactions and about one sixth of a cent for credit card transactions.[253] These ratios have not changed very much in the last 10 years, which Mr. Dupont said shows that identity theft is not as dire as some companies make it seem.[254]

Philippa Lawson, Associate at the University of Ottawa's Canadian Internet Policy and Public Interest Clinic

Like other witnesses, Philippa Lawson, an Associate at the University of Ottawa's Canadian Internet Policy and Public Interest Clinic, said that she was unable to provide the Committee with numbers on identity-related crime in Canada because there is a dearth of data in this area.[255]

Ms. Lawson made five suggestions for Canadian policy and law reform as regards identity crime. Her first suggestion was to enact security breach notification laws.[256] In her opinion, Bill S-4, which has provisions to that effect, proposes a model for reporting breaches to the Privacy Commissioner that is based on inappropriately high standards.[257] As a result, corporations could "avoid accountability for inadequate security measures."[258]

Ms. Lawson's second suggestion addressed PIPEDA reform. She believes PIPEDA is not taken seriously by corporations because it lacks teeth.[259] Ms. Lawson

---

250 Ibid.

251 Ibid.

252 Ibid.

253 Ibid.

254 Ibid.

255 Ibid., 1140 (Philippa Lawson, Barrister and Solicitor, Associate, Canadian Internet Policy and Public Interest Clinic, University of Ottawa, As an Individual).

256 Ibid.

257 Ibid.

258 Ibid.

259 Ibid., 1145.

noted that PIPEDA is intended to protect consumers from identity theft and fraud, but practices that violate the Act continue to be widespread in the marketplace.[260]

She also noted that Bill S-4 would make it easier for the Privacy Commissioner to publicly identify corporate offenders and take action against those that fail to adhere to compliance agreements, which are significant improvements over the current situation.[261] However, Ms. Lawson said that these measures were not enough to make our data protection laws effective.[262]

Third, Ms. Lawson suggested that the best form of protection against new-account fraud is credit freezing. Credit freezes prevent credit bureaus from sharing a consumer's credit reports.[263] In her opinion, this is a particularly helpful measure for elderly people and those who do not need to borrow money.[264] Ms. Lawson explained that offering credit freezes is not in the interest of credit bureaus because issuing credit reports is their primary service.[265] She gave the example of the United States, where almost all of the states now require that credit freezes be offered to consumers at no fee or at a very low fee in order to prevent identity theft.[266]

While acknowledging that consumer protection is an area of provincial responsibility, Ms. Lawson noted that the federal government "should be working with the provinces … to ensure that consumers across Canada have the tools they need to prevent, detect, and mitigate the effects of identity crime, including the ability to freeze their credit reports upon request."[267]

Her fourth suggestion was to coordinate victim assistance initiatives. She noted that, despite the fact that the Canadian Identity Theft Support Centre provides data to the Canadian Anti-Fraud Centre, the anti-fraud centre does not even acknowledge the existence of the theft support centre.[268] This example clearly shows that

> [t]here needs to be some coordination and cooperation between these two government-funded agencies so that each can focus on its mandate rather than trying to compete with the other for funds and public profile.[269]

---

260 Ibid.

261 Ibid.

262 Ibid.

263 Ibid.

264 Ibid.

265 Ibid.

266 Ibid.

267 Ibid.

268 Ibid.

269 Ibid.

Lastly, Ms. Lawson said that Canada should develop a national strategy to combat identity-related crime to better understand and address these crimes.[270] This strategy should be driven by senior officials and involve all key stakeholders.[271] In the same vein as Ms. Sproule and Mr. Dupont, Ms. Lawson said that the first pillar of a national strategy should be to develop mechanisms to gather reliable, comprehensive data on the incidence, types and costs of identity crime in Canada.[272]

Ms. Lawson suggested that Canada look to the United States, where a special task force was established in 2006 to develop a comprehensive national strategy to combat identity theft.[273] High-level executives from all pertinent government agencies sat on this task force, which examined the issue from all angles and published a comprehensive strategic plan to combat identity theft in the United States.[274] According to Ms. Lawson, this plan, which called for a coordinated national approach to policy and law reform, has now been largely implemented.[275] She concluded that consumers and victims of identity theft in the United States now have many more tools at their disposal to prevent and deal with identity theft than Canadians do.[276]

Éloïse Gratton, Partner and Co-Chair, Privacy, McMillan LLP

Éloïse Gratton also mentioned that PIPEDA does not give any real incentive for companies and organizations to comply with the Act or to implement appropriate security measures.[277] She said the worst case scenario for a company that does not comply with the Act is that their reputation might be tarnished.[278] A company also runs the risk that the Federal Court will order it to pay damages: the Court has made a few such rulings in the last 10 years, most of which awarded small amounts.[279]

Ms. Gratton also pointed out that there are no incentives at the federal level for class-action lawsuits over privacy violations, which could push companies to comply with the Act.[280] Ms. Gratton suggested that a provision similar to section 26 of *An Act to Establish a Legal Framework for Information Technology* in Quebec could be included

---

270 Ibid., 1150.

271 Ibid.

272 Ibid.

273 Ibid.

274 Ibid.

275 Ibid.

276 Ibid.

277 ETHI, *Evidence*, 2nd Session, 41st Parliament, 1 May 2014, 1145 (Éloïse Gratton, Partner and Co-Chair, Privacy, McMillan LLP, As an Individual).

278 Ibid.

279 Ibid.

280 Ibid.

in PIPEDA.[281] This provision includes an additional requirement for companies preparing to give or send information to a third party in an outsourcing situation.

Ms. Gratton referred to a number of studies whose findings show that most data breaches occur as a result of human error, saying that this shows that companies are not taking employee training very seriously as regards privacy protection.[282] With regard to mandatory breach notification, Ms. Gratton said that European countries and most states in the United States have laws to that effect.[283] The only Canadian province to introduce such legislation is Alberta, where businesses can be fined up to $100,000.[284] Ms. Gratton observed that

> this breach notification obligation in their law has increased the reporting of security breaches, and it has also increased the privacy training. Businesses are more inclined and are more motivated to spend, because they realize that it's going to be an obligation to disclose the breach if there is such a breach.[285]

As regards Bill S-4, Ms. Gratton said that it is not perfect, but it is better than nothing, because it would create an incentive for businesses to disclose a breach.[286] Ideally, Ms. Gratton said,

> [t]here should be clear monetary penalties for not reporting security breaches to individuals and to the privacy commissioners. There should be a duty to report a breach as soon as possible.[287]

Ms. Gratton believes that the Privacy Commissioner should be given the power to order an organization to report a breach to customers, and that these orders should be made public and the organization should be named.[288] This would create the necessary incentive for organizations to invest in preventive measures, which would be beneficial in addressing financial harm resulting from identity theft.[289]

Ms. Gratton also suggested having a uniform breach notification law, which could be based on the breach notification act drafted by the Uniform Law Conference of Canada several years ago.[290]

---

281 Ibid., 1150.

282 Ibid.

283 Ibid., 1155.

284 Ibid.

285 Ibid.

286 Ibid.

287 Ibid.

288 Ibid.

289 Ibid.

290 Ibid.

Avner Levin, Associate Professor at Ryerson University

Avner Levin's testimony focused on the role of banks in combatting identity theft.[291] He mentioned a study he carried out on the financial aggregator industry.[292] This industry pulls information together for customers who have multiple sources of financial information — credit cards, chequing accounts and savings accounts from various banks — and makes it available to the customer on their computer, tablet or phone.[293]

Mr. Levin's research focused on identifying consumer attitudes about these services and the security measures in place to protect customer information and address privacy concerns.[294] Mr. Levin and his colleagues wanted to meet with these companies and discuss their work in confidence, without attributing the information to them, but no one from the industry agreed to talk to his team because they did not see any advantage to meeting with them.[295] According to Mr. Levin's interpretation of PIPEDA, these companies should be able to provide the general information he wanted.[296]

Mr. Levin told the Committee that he and his colleagues have been trying for several years to obtain information from banks about identity theft and breaches related to identity theft.[297] Mr. Levin said that they approached banks individually and collectively, through the Canadian Bankers Association (CBA), but they have not received any responses.[298]

According to Mr. Levin, the answers to the questions he wanted to ask the banks would also help the Committee in its work, such as: what are the sources of fraud, what percentage is attributable to consumers' practices, and what percentage of identity theft is because people have easy passwords or fail to hide their PIN when they enter it, or because people are negligent and write down their PIN.[299]

With regard to criminals, Mr. Levin was looking for information about the percentage of identity theft attributable to people placing devices on automated banking machines to steal PINs or using skimmers on point-of-sale terminals to steal information, as well as what percentage of identity crime would be characterized as petty crime or as organized crime, the percentage resulting from rogue employees, and the percentage that

---

291 Ibid., 1200 (Avner Levin, Associate Professor, Ryerson University, As an Individual).

292 Ibid.

293 Ibid.

294 Ibid.

295 Ibid.

296 Ibid.

297 Ibid., 1205.

298 Ibid.

299 Ibid.

originates outside of Canada in countries where a lot of criminal activity takes place.[300] Mr. Levin believes that the government and Parliament will not be able to implement appropriate policies to address identity theft without this information.[301]

Mr. Levin said that the most recent data publicly available is from 2012 on the CBA site and from mid-2013 on the Canadian Anti-Fraud Centre site, but the data is not broken down by category, which means it cannot be used to establish an adequate strategy for the future.[302]

According to Mr. Levin, banks have a key role to play in fighting identity theft; they must be transparent and accountable.[303] He said that addressing identity theft is part of the "corporate responsibility" of banks as an industry group.[304]

Mr. Levin also urged the Committee to call on banks to share this information with the public and with academics, or at the very least with Committee members, so that the Committee would have the information it needs to accomplish the work it has begun.[305]

On 31 March 2015, Mr. Levin submitted a brief to the Committee about the lack of publicly available information on identity theft. In this brief, he noted that bank representatives who appeared before the Committee showed that they did not share a common definition of "identity theft," which would explain why they do not report or compile aggregate information about identity theft.

In his brief, Mr. Levin also compared Canada with the United States, where many states require banks to disclose identity theft and information security breaches. He quoted a number of news stories that broke in early 2015 about identity theft involving Canadian banks. According to Mr. Levin, the reported incidents "demonstrate the importance of providing public information to guide policy, and the weakness of the claims made by the banks in their appearance that identity theft occurs largely outside their operations."[306]

Mr. Levin believes that these cases are not isolated incidents: the media also reported a large-scale attack against more than 100 banks in over 30 countries, including Canada. Cumulative losses of this attack are estimated to be $1 billion. In Mr. Levin's opinion, if the public were better informed about this type of incident and the associated attack vectors that are used, it would "assist in combatting identity theft and

---

300 Ibid.

301 Ibid.

302 Ibid.

303 Ibid.

304 Ibid.

305 Ibid.

306 Avner Levin, "The Lack of Publicly Available Information on Identity Theft", 31 March 2015.

determining the most significant threats that need to be addressed by banks and their customers."[307]

Mr. Levin's brief also included three recommendations for the banking sector, which the Committee has incorporated into its own recommendations below.

In light of all of the testimony heard, and Mr. Levin's testimony in particular, the Committee makes the following recommendations regarding the banking sector:

> **Recommendation 2: The Committee urges Canadian banks to adopt, as a common definition of identity theft, the definition that appears in the current *Criminal Code* of Canada and to compile data on identity theft accordingly.**
>
> **Recommendation 3: The Committee urges Canadian banks to make public the information they have on identity theft. The information should include unsuccessful as well as successful attempts to steal personal information and should also include information about the source of the attack.**
>
> **Recommendation 4: The Committee invites Canadian banks to invest in technological measures to protect customer information. These measures should include audit systems that log the number of times customer records are accessed and how they are accessed.**

307 Ibid.

CRITIQUES OF THE MEASURES TAKEN BY BUSINESSES AND SUGGESTED IMPROVEMENTS BY CONSUMER PROTECTION ORGANIZATIONS, VICTIMS' RIGHTS ORGANIZATIONS AND NON-GOVERNMENTAL ORGANIZATIONS

A. Canadian Identity Theft Support Centre

The Canadian Identity Theft Support Centre is a non-profit organization that provides a toll-free number, live step-by-step support and online resources to help victims deal with the fallout of identity theft.[308] The Canadian Identity Theft Support Centre also provides information on preventing identity-related crimes and advice about protective measures that can reduce the risk of identity theft.

Kevin Scott, President and founder of the Canadian Identity Theft Support Centre, approached the issue from the victims' perspective.[309] Mr. Scott told the Committee about the confusion experienced by victims of identity theft: "They don't know where to turn, they don't know what to do, and they don't know how to get out of the maze."[310]

To regain control after their identity has been stolen, individuals need to speak with 15 to 20 organizations, and each of these organizations has its own procedures and explanations for how to address the issue.[311] According to Mr. Scott, it takes victims roughly 400 hours to work through the confusion, including dealing with the emotional consequences of identity theft.[312]

This information was provided by the Identity Theft Resource Center in San Diego, an organization the Canadian Identity Theft Support Centre has been working closely with since it was launched.[313] Mr. Scott informed the Committee that this organization has succeeded in streamlining the process so that the 400 hours of confusion that an identity theft victim experiences is reduced to 15 to 20 hours through the use of "a very systematic tool kit of forms, scripts, and so on to basically get the individual out of this quagmire."[314]

---

308 Canadian Identity Theft Support Centre, "Press Releases", *Media*.

309 ETHI, *Evidence*, 2nd Session, 41st Parliament, 3 June 2014, 1215 (Kevin Scott, President, Canadian Identity Theft Support Centre).

310 Ibid., 1220.

311 Ibid.

312 Ibid.

313 Ibid., 1215.

314 Ibid., 1220.

James Dorey, Executive Director of the Canadian Identity Theft Support Centre, explained that the organization focuses on three main streams: victim support, education and prevention, and research and data collection.[315]

As part of its victim support services, the Canadian Identity Theft Support Centre has developed fact sheets to help victims of identity theft and has put together a "Victim Toolkit" that has all the forms victims need in one booklet and walks them through the steps they need to take from beginning to end to regain their identity.[316] Mr. Dorey said that all of these resources are available on the Centre's website. The Centre has also set up a 1-800 number and a call centre so that people can speak to a real person on the other end of the line.[317]

Mr. Dorey explained to the Committee that the Canadian Identity Theft Support Centre has established partnerships with other Canadian organizations, including Equifax. This relationship is helpful when a victim's credit rating information is affected.[318]

As regards education and prevention, Mr. Dorey mentioned that the Centre has published four manuals that are available on its website: one for youth, one for seniors, one for the general public and one that focuses on online situations.[319] He added that the Centre has also put together a new education and outreach program for the two demographic groups that are increasingly being affected by identity theft: young people and seniors.[320]

Lastly, Mr. Scott noted that more than 100,000 people in Canada are currently dealing with identity theft.[321] He also recommended that the Committee include the following points in its recommendations:

> [I]ncreased victim support from government and the private sector, increased education and outreach, and also the development of a national index of what's going on with identity theft.[322]

The Committee took note of the Canadian Identity Theft Support Centre's recommendations and kept the victim's perspective in mind in its consideration of all the evidence it heard and in drafting the recommendations that stem from it.

---

315 Ibid., 1225 (James Dorey, Executive Director, Canadian Identity Theft Support Centre).

316 Ibid.

317 Ibid.

318 Ibid.

319 Ibid.

320 Ibid.

321 Ibid., 1230 (Scott).

322 Ibid.

B. Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic

The Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC) is based at the Centre for Law, Technology & Society at the University of Ottawa's Faculty of Law.[323] CIPPIC's mandate is to advocate in the public interest on issues that have both legal and technological implications.

In 2007, CIPPIC published a number of documents on identity theft,[324] including a working paper entitled *Identity Theft: Introduction and Background*. The paper provides information on the history, characteristics, causes and extent of identity theft, and also addresses the challenges of defining the term "identity theft" and of measuring its size and impacts. It identifies the key stakeholders for studying the issue of identity theft and analyzes the impact of technology, including the widespread use of the Internet, on identity theft.[325]

Tamir Israel appeared before the Committee on behalf of the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic.[326] He said that identity theft is "the crime of the information age."[327] Mr. Israel explained how the information collected and analyzed by the United States Federal Trade Commission's Consumer Sentinel Network showed that, of the more than 2 million consumer complaints in 2013, more people complained about identity theft than any other category.[328] Mr. Israel also explained that, since identity theft is a vehicle for a range of identity crimes, such as false identities that are then used to carry out other crimes, it is difficult to measure the economic and social costs of identity theft.[329]

According to Mr. Israel, identity thieves are taking full advantage of new technologies by using information available on social media and mobile devices.[330] Illegal online markets for identities have been established, where email account access, credit card numbers, and full identity profiles can be bought and sold en masse.[331] He cited figures from an Organisation for Economic Co-operation and Development study in 2009, which estimates that email addresses can be purchased for prices ranging from

---

323 Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC), *About the Clinic*.

324 CIPPIC, "Project Publications", *Privacy, Identity Theft*.

325 CIPPIC, *Identity Theft: Introduction and Background*, CIPPIC Working Paper No. 1 (ID Theft Series), March 2007, Ottawa, 21 pages.

326 ETHI, *Evidence*, 2nd Session, 41st Parliament, 3 June 2014, 1230 (Tamir Israel, Staff Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic).

327 Ibid.

328 Ibid.

329 Ibid.

330 Ibid.

331 Ibid.

US$1.70 to US$15 per megabyte, and that access to compromised email accounts ranges from US$1 to US$20, depending on black market fluctuations.[332]

He also said that it is difficult to measure the economic cost of the time, effort and trauma involved in recovering from identity theft.[333]

Mr. Israel identified three components that he believes need to be included in any response to identity theft: prevention, research and education, and victim support. He also mentioned another essential component, which is investigation and enforcement.[334]

Mr. Israel believes that many measures taken over the last few years have improved the ability of various Canadian organizations to investigate identity crimes and to address the offences that facilitate identity crimes.[335] These organizations include the Office of the Privacy Commissioner of Canada, the Competition Bureau, and various law enforcement agencies.[336]

Despite these measures, which include adding provisions to the *Criminal Code* and adopting *Canada's Anti-Spam Legislation*, it is important to recognize that "identity theft is here to stay, and an enforcement solution alone will not be enough to address the problem," he said.[337]

Mr. Israel believes that more needs to be done to protect personal information so that it does not end up in the hands of identity thieves, and that this will require stronger data protection frameworks, including a stronger PIPEDA and a stronger *Privacy Act*.[338]

As regards PIPEDA, Mr. Israel said that it must play a central role in the fight against identity theft.[339] He believes that social networks and mobile devices are a repository for information, and that this information is often disclosed in unexpected ways to the general public and to invisible third-party applications.[340] He also made the following comments about data security:

> PIPEDA also obligates organizations to put in place reasonable technical and other safeguards in order to prevent unauthorized access to customer data. Security breaches

---

332 Ibid.

333 Ibid.

334 Ibid.

335 Ibid.

336 Ibid.

337 Ibid.

338 Ibid.

339 Ibid.

340 Ibid.

> are not only becoming more frequent with each passing year, but the number of identities exposed with each breach is increasing dramatically.[341]

Mr. Israel pointed out that Symantec's 2014 *Internet Security Threat Report* "registered a 260% annual increase in the number of identities exposed by each average breach, meaning that these are essentially cyber-breaches targeting large repositories of data in one go."[342] He believes this makes the adoption of strong technical safeguards a very important tool in preventing identity theft.[343]

The overview Mr. Israel gave of the situation shows that the need for a rigorously enforced and applied PIPEDA framework has never been greater, yet the current framework does not reflect this need.[344] To support his views, he quoted former Privacy Commissioner of Canada Jennifer Stoddart in the Committee's report entitled *Privacy and Social Media in the Age of Big Data*:

> [W]ith the emergence of Internet giants, the balance intended by the spirit and letter of PIPEDA is at risk, and the risk of significant breaches and of unexpected, unwanted, and even intrusive use of people's information calls for commensurate safeguards and financial consequences not currently provided for in PIPEDA.

With regard to Bill S-4, Mr. Israel believes the optional consent orders provided for in the bill will make it easier to enforce PIPEDA.[345] However, he said that full enforcement powers and administrative monetary penalties for non-compliance are required so that companies have effective incentives to comply proactively with their obligations under PIPEDA.[346] As for the breach notification obligations in Bill S-4, Mr. Israel noted that they were "far overdue."[347] In his words,

> [w]hile the breach notification obligation in Bill S-4 is a positive step forward, it is not sufficiently calibrated to deter security breaches. It focuses too closely on the risk of direct harm to an end-user resulting from a specific breach. In reality, in many instances it will be difficult to know whether a particular vulnerability was or was not exploited, meaning that much laxity in technical safeguards will remain unreported. This makes it an ineffective mechanism for encouraging and incentivizing companies to strengthen up their technical safeguards.[348]

Mr. Israel also cited recent cases of high-profile breaches at government departments — such as the loss of an HRSDC hard drive that contained personal

---

341 Ibid.

342 Ibid.

343 Ibid.

344 Ibid.

345 Ibid., 1235.

346 Ibid.

347 Ibid.

348 Ibid.

information of more than 500,000 people who had applied for student loans — to show that the *Privacy Act* is lacking not only a breach notification obligation, but also "the basic obligation to adopt technical safeguards."[349]

Mr. Israel said that, to effectively address the issue of identity theft, education and outreach initiatives are needed in addition to prevention measures.[350] He noted that some government organizations have developed very good consumer education resources that address identity crime. He gave the example of the Competition Bureau's *Little Black Book of Scams*, and mentioned that it was available online.[351] He also mentioned the efforts of non-government organizations, such as the Canadian Identity Theft Support Centre's Victim Toolkit.[352] However, Mr. Israel believes that more should be done, particularly with regard to "education on the victim recovery process."[353]

Mr. Israel also identified a need for coordinated and sustained research on the scope and parameters of identity theft.[354] In his opinion, not enough systematic research has been carried out in this area in Canada since 2006.[355] Some foreign initiatives have provided insight into the scope and parameters of identity theft in Canada, but more Canada-specific research is needed. A breach repository, which was mentioned by the representatives of the Canadian Identity Theft Support Centre during their testimony, would be a step in the right direction.[356]

As regards the recovery process for victims of identity theft, Mr. Israel said that it is very complex, and that victims must deal with "creditors who are reluctant to believe their debt is not theirs."[357] He also pointed out that a bad credit rating can follow victims of identity theft for years.[358]

Mr. Israel emphasized the importance of the standardized documentation provided by organizations such as the Canadian Identity Theft Support Centre to help victims take the steps required to recover their identity after it has been stolen.[359] In his opinion, it is also crucial to ensure that these standardized documents are accepted both by law enforcement and by service providers.[360] He mentioned that cost-free credit freezes and

---

349 Ibid.

350 Ibid.

351 Ibid.

352 Ibid.

353 Ibid.

354 Ibid.

355 Ibid.

356 Ibid.

357 Ibid.

358 Ibid.

359 Ibid.

360 Ibid.

online access to credit reports were other useful and necessary tools to help victims recover their identities.[361] According to Mr. Israel, "the ongoing availability of a victim support centre is essential to the overall recovery process."[362]

In conclusion, he recommended adopting a national strategy to support victims of identity crime that would establish clear parameters for cooperation between the various entities that provide victim support, such as the Canadian Anti-Fraud Centre, the Canadian Identity Theft Support Centre and the various regulatory bodies that address identity theft.[363] This national strategy to support victims of identity crime should also establish a clear road map outlining how the various identity recovery mechanisms would be adopted.[364]

The Committee believes that a national strategy to support victims of identity crime would ensure that efforts to combat identity theft could be coordinated in order to address this crime more effectively.

Recommendation 5: The Committee recommends that the Government of Canada seek provincial and territorial support in considering the establishment of a national strategy to coordinate efforts to combat identity theft and address this crime more effectively.

C. Crime Prevention Association of Toronto

Janet Sherbanowski, the Executive Director of the Crime Prevention Association of Toronto, explained that her organization works with the Competition Bureau and the Toronto Police Services Board on fraud and related issues.[365]

She explained that the Association holds workshops on credit and identity fraud for new immigrants and seniors through the New Horizons for Seniors Program.[366] The Crime Prevention Association of Toronto also collaborates with the Royal Bank of Canada and Scotiabank, which sponsored the "ABCs of Fraud" program until 2011.[367]

Ms. Sherbanowski noted that the Association worked with the Ontario Privacy Commissioner to determine what information should be provided to consumers to help

---

361 Ibid.

362 Ibid.

363 Ibid.

364 Ibid.

365 ETHI, *Evidence*, 2nd Session, 41st Parliament, 23 February 2015, 1530 (Janet Sherbanowski, Executive Director, Crime Prevention Association of Toronto).

366 Ibid.

367 Ibid.

them protect their identity and how to tell them about the risk with big data and the way data is being mined by corporations and perhaps also the government.[368]

According to Ms. Sherbanowski, consumers should be warned when "financial institutions, for instance, in a criminal fashion under-report breaches or thefts of data on credit cards or debit cards."[369] If these breaches are not reported, the Association does not have an opportunity to increase its monitoring services and perhaps to hire more people in police services or government services to look into these issues.[370]

D. Claudiu Popa, Chief Executive Officer, Informatica Corporation, as an Individual

Claudiu Popa explained that his company provides security and privacy consulting services across Canada.[371] According to the research carried out by his organization, the problem of identity theft is not only growing but also transforming, and every year new ways of committing identity theft are emerging around the world.[372]

Mr. Popa cited studies by Intel and McAfee in their 2014 global cybercrime report, which shows that up to $575 billion in annual value is lost as a result of cybercrime, most of which arises from the billions of individual records that are compromised.[373] Mr. Popa said that this is a global issue.

Mr. Popa also quoted the FEC, the FBI and Canadian sources that say it takes at least six months and 200 hours to recover an identity once personal information has been stolen.[374]

Mr. Popa explained that phishing and spear-phishing, which is a targeted attack to gain as much information as possible from the victims, are among the most common practices used to break into organizations, gain access to personal computers, or install software without authorization.[375] He also mentioned that it is inherently difficult to put in place legislation that would protect companies that engage in misleading activities "from acquiring personal information, abusing it, reselling it, and participating in this cycle of cybercrime."[376]

---

368 Ibid., 1535.

369 Ibid.

370 Ibid.

371 Ibid., 1540 (Claudiu Popa, Chief Executive Officer, Informatica Corporation, As an Individual).

372 Ibid.

373 Ibid.

374 Ibid.

375 Ibid., 1545.

376 Ibid.

In the same manner that it is impossible to quantify cybercrime, it is impossible to quantify identity theft, in Mr. Popa's opinion. He pointed out that personal data theft is happening on a massive scale around the world, and that there are links between identity crime and human trafficking and funding terrorism.[377]

Mr. Popa also noted that credit brokerage firm services are being used ineffectively as a knee-jerk reaction to a breach. In his opinion, having an organization that has fallen victim to a data breach offer its affected customers free credit and identity monitoring is an insufficient response.[378] With regard to organizations that find themselves in this situation, he said:

> In many cases these organizations, in their own practices, do not conform to standard best practices for anti-phishing or identity protection. They do not even follow secure development practices for some of the tools they offer. For all intents and purposes, these are very weak controls and the standardization of these safeguards should be revisited.[379]

According to Mr. Popa, stiffer penalties need to be established for complicity within cyberfraud, while ensuring that clemency measures are established for individuals who fall prey to the promise of profits and believe they are working a regular job, and who are not actually part of the organized criminal element.[380]

As regards synthetic identity theft and fraud, Mr. Popa believes they can be identified using big data analytics.[381] In his opinion, banks and insurance companies must work together to identify risk trends and build models that will lead to identifying those responsible.[382]

---

377 Ibid.

378 Ibid., 1550.

379 Ibid.

380 Ibid.

381 Ibid.

382 Ibid.

STEPS THAT GOVERNMENT AGENCIES ARE TAKING TO PROTECT CANADIANS FROM IDENTITY THEFT

As part of its study, the Committee welcomed several government departments and agencies to discuss the programs currently in place to protect Canadians from identity theft and to prevent identity fraud. Throughout this testimony, it was impressed upon the Committee the effectiveness of meaningful collaboration among different public and private sector stakeholders. This collaboration, particularly in efforts to educate the public on the risks of sharing their personal information and on what to do if they become victims of identity theft, is crucial to mitigate the economic impact of identity theft. The following section summarizes their testimony, while providing the Committee's observations on the effectiveness of these efforts and the areas — such as data gathering and information sharing — in which it observes that more can be done.

A. The Canadian Anti-Fraud Centre

The Canadian Anti-Fraud Centre (CAFC) is a joint partnership between the Royal Canadian Mounted Police (RCMP), the Competition Bureau and the Ontario Provincial Police. The CAFC serves as a central repository of data related to fraud, offering a "peer-to-peer type process" so victims can report a fraud and receive counsel on how to prevent that from happening again.[383] The repository allows law enforcement to identify trends and patterns in identity theft and assists them in possible investigations.

Superintendent Jean Cormier, Director of the RCMP's Federal Coordination Centres, told the Committee that, in 2013, "over 24,000 victims of identity crime contacted the CAFC to report losses … to a total of $11 million;" this despite noting that cases reported to the CAFC "represent only 5% of the victims."[384] In his view, "these figures highlight the importance for law enforcement to work collaboratively with domestic and international partners to prevent, detect, and pursue those who engage in [fraud] activities."[385] While the CAFC has been able to build that kind of collaboration between public and private sector actors, Supt Cormier noted that "the difficulties and challenges that we face in regard to working with the private and public sectors and law enforcement are about the ability to share private information in certain instances, which are limited by privacy laws, obviously, and the need for the businesses that we deal with to respect client privilege."[386]

---

383 ETHI, *Evidence*, Meeting No. 17, 2nd Session, 41st Parliament, 3 April 2014, 1130 (Supt Jean Cormier, Director, Federal Coordination Centres, Royal Canadian Mounted Police). See also Canadian Anti-Fraud Centre, *About us*.

384 Ibid., 1105 and 1200.

385 Ibid., 1105.

386 Ibid., 1130.

Within the framework of the CAFC, the Competition Bureau participates in the investigation of large-scale mass marketing fraud (MMF); that is, fraud committed via mass communication media where product or business interests are promoted and affect competition. According to Morgan Currie, Acting Assistant Deputy Commissioner of Competition for the Competition Bureau, "identity theft and money laundering are critical components of various mass marketing fraud schemes" that cost the Canadian economy $10 billion per year.[387]

Like Supt Cormier, Mr. Currie also highlighted the importance of collaboration between public sector actors, noting that the Competition Bureau plays a central role in the CAFC — "the hub of the national network of MMF partnerships" — and that it participates in numerous international partnerships with law enforcement and regulatory authorities.[388] As he put it,

> [t]o effectively counter the threat of mass marketing fraud, investigative law enforcement and regulatory authorities in multiple countries have been: working together to gather and share intelligence on MMF schemes and how to disrupt them; increasing public awareness and education programs to help individuals and businesses recognize these schemes and avoid losses; developing measures to more promptly identify and support victims of mass marketing fraud schemes; and developing and expanding coordinated efforts among law enforcement agencies to fight MMF schemes.[389]

The Committee commends the work being done by the different agencies that comprise the CAFC. This type of collaboration between law enforcement and regulatory authorities is necessary to properly educate, prevent, detect and deter fraudulent activity and facilitate the investigation and prosecution of those involved in these crimes. In particular, the Committee notes the efforts made by the CAFC's fraud prevention campaigns — including Fraud Prevention Month, which takes place in March each year — that aim to educate consumers on "how to recognize, report, and stop various forms of MMF."[390]

The Committee observes, however, the importance of reporting identity fraud. As noted by representatives of both the RCMP and the Competition Bureau, under-reporting is a "big problem" which makes it difficult to properly compile information and assess the extent, prevalence and costs associated with identity fraud. Mr. Benoît Dupont warned about not knowing the size of the problem in terms of the actual number of victims and the evolution of the criminal trend. Regarding the 24,000 victims of fraud that reported their cases to the CAFC in 2013, he noted that

> this is probably a tiny fraction of the overall pool of victims because most of them … never lodge a formal complaint with their police service, some of them because they don't

---

387 Ibid., 1110, 1115 (Morgan Currie, Acting Assistant Deputy Commissioner of Competition, Competition Bureau, Fair Business Practices Branch Division C, Department of Industry).

388 Ibid., 1115.

389 Ibid.

390 Ibid.

> believe the crime is important enough or will attract any interest, others because they're discouraged by their local police service, which is not equipped to deal with this type of crime especially if the amounts involved are below a certain threshold.[391]

In Mr. Dupont's opinion, gaining information on the number of victims, the types of identity theft scams they suffered, the types of identity thieves that operate these scams and where they operate them from can all assist in devising both regulatory and law enforcement strategies for protecting consumer's personal information and focusing resources more effectively. The Committee agrees with this assessment and observes that the CAFC is well-positioned to continue its efforts to encourage all victims of identity fraud to report their cases to the CAFC.

B. National Identity Crime Strategy

Supt Cormier told the Committee about the RCMP's development, in 2012 and in consultation with private and public sector stakeholders, of a National Identity Crime Strategy.[392] As he explained,

> [t]he strategy is supported by three pillars: education and prevention, intelligence enforcement, and prosecution. The strategy calls for the following: identifying priorities and emerging risk, and so analyzing developing trends; relying on the compilation and analysis generated by the criminal intelligence pillar; increasing the intelligence-based investigation project and coordinated disruption efforts; and developing a standard approach for ID fraud as well, and thus to investigations, including creating and adopting a protocol for multi-jurisdictional investigation, because as I said, many times this crime crosses borders.[393]

The strategy, whose implementation began in 2013, seeks to raise "identity crime awareness with the judicial community and government officials from across the country and in other countries."[394] According to Philippa Lawson of the Canadian Internet Policy and Public Interest Clinic, the strategy "is a good start, but it needs a lot more work to get beyond broad generalities and to include the consumer protection angle."[395] In her view, "Canada needs a national strategy to understand and address the specific problem of identity-related crime, a strategy that should be driven by high-level officials and that should involve all key stakeholders … including consumer protection agencies and privacy commissioners at both federal and provincial levels."[396] Ms. Lawson suggests developing mechanisms "to gather reliable, reasonably comprehensive data on the incidence, types, and costs of identity crime in Canada."[397] The Committee agrees; effective data gathering

---

391 ETHI, *Evidence*, Meeting No. 19, 2nd Session, 41st Parliament, 29 April 2014, 1130 (Dupont).

392 RCMP, *National Identity Crime Strategy*.

393 ETHI, *Evidence*, Meeting No. 17, 2nd Session, 41st Parliament, 3 April 2014, 1120 (Cormier).

394 Ibid.

395 ETHI, *Evidence*, Meeting No. 19, 2nd Session, 41st Parliament, 29 April 2014, 1150 (Lawson).

396 Ibid.

397 Ibid.

is crucial in the development of effective policies, strategies and programs to combat identity theft and identity fraud. The Committee takes this element into consideration in its recommendations.

C. Canada's Anti-Spam Legislation

Passed in December 2010 and with most of its provisions in force since 1 July 2014 — while the Committee conducted this study —, Canada's anti-spam Legislation (CASL) sets certain prohibitions that aim "to protect Canadians while ensuring that businesses can continue to compete in the global marketplace."[398] These prohibitions include sending commercial electronic messages, altering transmission data and installing computer programs or software on another person's computer without consent.[399] CASL is enforced through the collaboration of three government agencies: the Canadian Radio-Television (CRTC), which oversees violations to the prohibitions listed; the Competition Bureau, which investigates false and misleading representations and deceptive marketing practices; and the Office of the Privacy Commissioner, which investigates the collection of personal information through illegal access to computer systems and electronic address harvesting. Under the legislation, both the CRTC and the Competition Bureau can issue administrative monetary penalties, while the latter can also seek criminal sanctions under the *Competition Act*.

According to Michael Jenkin, Director General at the Office of Consumer Affairs at the Department of Industry, CASL addresses several major concerns, including

> phishing messages, which are designed to lure recipients to counterfeit websites and trick them into revealing personal information, such as usernames, passwords, and account information; malware, which involves the installation of software on a person's computer, smart phone, or other digital device without their knowledge or consent — these types of spyware and viruses can secretly collect personal information that is then used in identity theft activities — and finally traffic rerouting, which involves secretly redirecting a person's online searches to a malicious destination where attackers can collect personal information for the purposes of carrying out identity thefts.[400]

Mr. Currie, from the Competition Bureau, noted that through this legislation his agency would be "able to more effectively address false or misleading representations and deceptive marketing practices in the electronic marketplace, including false or misleading sender or subject matter information, electronic messages, and locator information such as URLs and metadata."

---

398 ETHI, *Evidence*, Meeting No. 16, 2nd Session, 41st Parliament, 1 April 2014, 1215 (Michael Jenkin, Director General, Office of Consumer Affairs, Department of Industry). See also *Canada's Anti-Spam Legislation*, *About the Law*.

399 An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act [CASL], S.C. 2010, c. 23, ss. 6 and 8.

400 ETHI, *Evidence*, Meeting No. 16, 2nd Session, 41st Parliament, 1 April 2014, 1215 (Jenkin)

The penalty provisions in CASL allow the CRTC and the Competition Bureau to impose maximum administrative monetary penalties of $1 million for individuals and $10 million for businesses.[401] Ms. Gratton noted that these provisions, which may extend liability to administrators, executives and employers, are "quite stiff" resulting in the legislation "being taken seriously" by the companies; that is, companies are deploying many resources to ensure they are in compliance with CASL.[402] In her opinion, the experience from the anti-spam legislation is instructive with regard to enforcement powers and the creation of incentives to motivate companies to invest in identity theft prevention.[403]

The Committee notes that CASL rules about installing computer programs came into effect on 15 January 2015, and that the sections that deal with the private right of action are scheduled to come into force in July 2017. As businesses and individuals adapt and comply with CASL, the Committee remains interested in observing the effects it has on Canadians' privacy and identity interests before deriving the pertinent lessons from CASL's implementation.

D. Modernizing the Administration of Social Insurance Numbers

SINs are used by federal departments and agencies as identifiers for the delivery of programs and services such as employment insurance, Canada student loans, the Canada Pension Plan and old age security, as well as for taxation purposes. Canadian citizens, permanent residents, and temporary residents are assigned a unique SIN to work in Canada or to receive benefits and services from government programs. The Social Insurance Register (SIR) records all SINs along with the information provided by individuals when they apply for a SIN.

Service Canada, an organization within the Department of Employment and Social Development, oversees the issuance of SINs and administers the SIR. While government departments and programs are required to collect and use the SIN, private sector organizations are also authorized to ask for a customer's SIN where there is a specific purpose linked to a government requirement, such as employment or income tax purposes. There is, however, no legislation that prevents private sector organizations from requesting an individual's SIN for other purposes or that compels the individual from providing their SIN.[404]

The Committee heard evidence explaining how practices in the issuance of the SIN and the administration of the SIR have changed "to increase the integrity of the social

---

401 CASL, s. 20(4).

402 ETHI, *Evidence*, Meeting No. 20, 2nd Session, 41st Parliament, 1 May 2014, 1150 (Gratton,).

403 Ibid., 1150, 1215 and 1220 (Gratton).

404 ETHI, *Evidence*, Meeting No. 16, 2nd Session, 41st Parliament, 1 April 2014, 1145 (Louis Beauséjour, Assistant Deputy Minister, Integrity Services Branch, Service Canada, Department of Employment and Social Development). See Service Canada, *The Social Insurance Number Code of Practice*.

insurance number program and to reduce the impact and the incidence of identity fraud."[405] Louis Beauséjour, Assistant Deputy Minister at the Department of Employment and Social Development, told the Committee about two reports by the Auditor General on the SIN program in 1998 and 2002, whose "main findings were that the proof of identity procedure needed to be improved, that existing information sources had to be used more effectively, that the information in the SIN database was not always complete and accurate, and that there were more SINs in circulation than there were Canadians over the age of 20."[406]

As a result of these findings, "important initiatives were implemented with regard to the administration of the SIN and the SIR which had positive consequences on government efforts against identity theft and fraud."[407] These initiatives included the dormant flag, which identifies SINs that have not been active for a period of five or more consecutive years and requires presentation of original proof of identity documents for reactivation; the introduction of an expiry date for social insurance numbers issued to temporary foreign workers; and, the development of a proof-of-identity internal reference website which permits agents responsible for the issuance of SINs have access to detailed information on what to look for in identity documents to ensure their authenticity.

Further, the Department of Employment and Social Development has implemented a certification program to train agents on the issuance and administration of SINs, has introduced the SIN Code of Practice to provide advice to employers, stakeholders, and individuals of what they should do or not do to protect personal information, and has signed agreements with all 10 provinces in order to develop electronic links between provincial vital statistics agencies and the SIR. Since 2014, applications for a SIN can no longer be done by mail but must be in person at a Service Canada point of service — except in the case of individuals in remote areas, under extenuating limitations or residing abroad. Once issued, the SIN is given in paper format as production of the plastic SIN cards has stopped. According to Mr. Beauséjour, "this initiative will contribute to the prevention of identity theft and fraud related to the potential loss or theft of SIN cards."[408]

The Committee was told by Mr. Beauséjour that for fiscal year 2013 Service Canada "had a bit more than 4,500 investigations that led to a conclusion that there was a misuse of the social insurance number."[409] By his estimate, three-quarters of these "were related to a benefits investigation at the same time, and about 1,400 were related to potential issues raised with SIN applications."[410] Where the misuse is related to SIN fraud that could lead to other types of fraud, the case is referred to the RCMP for investigation.

---

405 Ibid., 1100.

406 Ibid., 1105.

407 Ibid.

408 Ibid., 1110.

409 Ibid., 1120.

410 Ibid.

Mr. Beausejour also indicated that in cases where a material breach has occurred "there's an agreement we have in terms of the three characteristics of what is considered a breach that needs to be reported to the Privacy Commissioner." Such breaches involve information that is directly related to personal information that is sensitive, that there is a risk of identity theft or fraud, and if the incident may cause damage to the career, reputation, financial situation, security, health or well-being of the person.

While Mr. Beauséjour indicated that he was "not aware of any misuse of the SIN following a breach involving loss of personal information," the case regarding the lost unencrypted portable storage devices containing the SIN and other information of some 583,000 people by the Department of Employment and Social Development has led to the implementation of "different protection reinforcement measures" and a search for "new ways to reduce the risks associated with the loss of private information."[411]

E. Introduction of the Electronic Passport

The Committee was told about the Passport Program and that it is a collaborative effort across several departments. The Minister of Citizenship and Immigration has overall accountability for the Passport Program, including "issuing, refusing to issue, revoking, withholding, recovering, and providing instructions on the use of Canadian passports."[412] The Passport Program also partners with law enforcement and intelligence agencies in its assessments of individual applicants or passport-holders. The delivery of domestic passport services is the responsibility of the Department of Employment and Social Development, while the Department of Foreign Affairs, Trade and Development is responsible for applications made by Canadians abroad.

According to officials from the Department of Citizenship and Immigration, approximately 5 million applications are made each year and 23 million valid Canadian travel documents are currently in circulation. Passports issued since 1 July 2013 meet "the latest international norms set out by the International Civil Aviation Organization, which represents the gold standard for travel documents."[413] These electronic passports, or ePassports, have an electronic chip embedded in them to provide an additional layer of security to guard against identity theft. According to Lu Fernandes, Director General of the Passport Program Integrity Branch:

> The chip stores the information found on page 2 of the passport, including the bearer's photo, providing border control personnel with an additional tool to validate the passport holder's identity. By accessing the information on the chip and comparing it with the information on page 2 of the book, a border agent can ensure that the information or photo has not been modified.

411 Ibid., 1120, 1150.

412 Ibid., 1200 (Lu Fernandes, Director General, Passport Program Integrity Branch, Department of Citizenship and Immigration).

413 Ibid.

The design of the visa pages in the ePassport provides another layer of security, making the book more difficult to counterfeit. The pages are made up of unique pairs of vignettes that depict recognizable themes, places, and persons in Canada's history. The different images on each page, along with a variety of visible and invisible security features, make it very difficult and extremely expensive for counterfeiters to reproduce a book or substitute a page.[414]

The Committee was told that approximately 66,000 passports are reported lost or stolen annually, the most often scenario being when "individuals have forgotten where they put them, have just misplaced them, or in a move have no idea which box they might be in, and they report them as lost."[415] Once reported lost or stolen, passports are cancelled and the information is reported within 24-hour period to the Canada Border Services Agency (CBSA) and the Canadian Police Information Centre, which subsequently updates the Interpol database. Even in cases where the passport is later found, once cancelled the passport can no longer be used for travel.

The Committee was also told that, in 2013, Passport Canada "refused or revoked approximately 1,370 passport applications. Of those, about 1,000 were refused or revoked for reasons of criminality … About 225 were for entitlement fraud or passport misuse [and] 36 were for citizenship issues, so the individual was not in fact a citizen of Canada."[416] In about 70 cases, the refusal or revocation was on the basis of identity fraud, where the applicants "have stolen the actual documents of an individual, be it a citizenship paper, a birth certificate, or a health card … and used them to apply for a passport."[417] In those cases, applicants are investigated by Passport Canada, notified of the investigation and their application is stopped. Where administrative action is taken, passport service can be withheld for five years from the date of the incident, with exemptions for urgent, compelling, compassionate reasons. The "most serious cases of identity fraud or theft" are referred to the RCMP and it is the RCMP, and not Passport Canada, that investigates the identity theft. According to the Passport Program officials that appeared before the Committee, "the difficulty we have is that we don't know exactly how the documents were stolen … it's a very grey area for us."[418]

F. The Canada Revenue Agency's Integrity Framework

Representatives from the Canada Revenue Agency (CRA) appeared before the Committee to share that agency's work in setting safeguards to protect Canadians' personal information and prevent identity theft. The CRA is among the largest institutions in the Government of Canada and has one of the largest personal information data

414 Ibid., 1205. See also Passport Canada, *About your passport*.

415 Ibid., 1230.

416 Ibid., 1235, 1240.

417 Ibid., 1235 (Peter Bulatovic, Director, Investigation Division, Passport Program Integrity Branch, Department of Citizenship and Immigration).

418 Ibid. and 1240 (Fernandes).

holdings in the country. Typically, for a Canadian taxpayer, the CRA will hold "all of the information on a person's income tax and benefit return" including their SIN, their income, the credits they are applying for and any additional information for specific credits, such as medical information for a disability tax credit. In the case of businesses, the CRA will hold information on the business income, the GST and HST that they have collected on behalf of the governments, as well as any additional information related to credits.[419]

In 2012, the CRA launched its integrity framework to bring together all of its policies, programs and systems in order to ensure "that the high standards established to protect taxpayer privacy are communicated to all employees and managers, and that the CRA's performance against those standards is carefully monitored and reported."[420] Susan Gardner-Barclay, Assistant Commissioner and Chief Privacy Officer at the CRA's Public Affairs Branch told the Committee of other initiatives, including building "front-end controls that ensure employees have only the access to CRA computer systems that they require in order to perform their duties, and strengthening our back-end controls to build on our automated systems so that the CRA can better monitor and analyze the full range of actions performed by employees on their computers."[421] She also spoke of CRA information-sharing protocols and an organization-wide exercise to verify that privacy impact assessments are up to date, all with an aim to prevent breaches of personal information as these "hold the potential for that information to be used in identity theft or other criminal activities."[422] According to Ms. Gardner-Barclays, these initiatives, coupled with efforts to warn Canadians of phishing schemes misrepresenting the CRA, show that "the CRA is working to ensure controls are in place, and that we continue to assess and improve those controls."[423]

Officials told the Committee that there were 2,983 breaches reported on at the CRA in 2013. Of these breaches, misdirected mail constituted "95% of the CRA's information, data and privacy breaches" and, even so, "many of the breaches identified by the CRA do not constitute privacy breaches, as no personal information was disclosed."[424] Yet, according to the same officials, privacy breaches constituted 46% of the reported cases and in 479 cases there was "a reasonable chance of harm to the individual," resulting in the file being reported to the Office of the Privacy Commissioner in accordance with Treasury Board Guidelines.[425] In those cases where the CRA was in contact with taxpayers whose personal information was at risk, the agency would "either provide them

---

419 ETHI, *Evidence*, Meeting No. 18, 2nd Session, 41st Parliament, 8 April 2014, 1200 (Susan Gardner-Barclay, Assistant Commissioner and Chief Privacy Officer, Public Affairs Branch, Canada Revenue Agency).

420 Ibid., 1110.

421 Ibid.

422 Ibid.

423 Ibid.

424 Ibid., 1110, 1145.

425 Ibid., 1145.

with some support with Equifax, the credit services, and/or we can put a flag on their file so that we are aware that there's a concern there might be identity theft."[426]

G. Human Rights Impact Assessment for Security Measures

The Committee heard from Philippe Dufresne, then Director General and Senior General Counsel of the Human Rights Protection Branch at the Canadian Human Rights Commission. Mr. Dufresne informed the Committee of the Human Rights Commission's work on identity certification and "the importance of ensuring that measures used to certify a person's identity comply with human rights principles."[427] In its work, the Human Rights Commission has found that "the most common forms of identity certification tools used are at risk of being discriminatory based on the prohibited grounds of discrimination set out in the *Canadian Human Rights Act*." This is, according to Mr. Dufresne, due to the use of methods that may be inaccessible to an individual or group of individuals, and because decisions rendered by officers in validating identities may lead to discrimination.[428]

To correct this, the Human Rights Commission recommends the use of multi-modal biometric systems that do not rely exclusively on one form of identity certification which can prove to be discriminatory; for example, the use of fingerprints — which can be inaccessible to people who do not have fingers — can be complimented by the use of retina scans, thereby providing a degree of inclusiveness. As Mr. Dufresne put it,

> [i]n dealing with these important issues, human rights law provides guidance for determining whether an otherwise discriminatory measure can be justified. This includes looking at: first, the extent to which the measure is necessary; second, whether there are less discriminatory ways of achieving the same objective; and third, the extent to which the infringement on human rights outweighs the benefits gained by the measure.
>
> Situations may also arise where users may require an exemption. Policies and practices to reasonably accommodate these individuals should therefore be included as part of the development of any measure. Should there be no reasonable alternative for a given biometric, it is up to the organization employing the biometric to demonstrate that sufficient measures have been taken to explore other less discriminatory ways of achieving similar results.[429]

As part of its efforts to encourage organizations to apply a human rights lens to a proposed policy or procedure, the Canadian Human Rights Commission has developed the Human Rights Impact Assessment for Security Measures (HRIA). This tool "outlines the steps to take during a security measure's life cycle to ensure that security standards,

---

426 Ibid., 1120 (Helen Brown, Director General, Security and Internal Affairs Directorate, Finance and Administration Branch, Canada Revenue Agency).

427 Ibid., 1100 (Philippe Dufresne, Director General and Senior General Counsel, Human Rights Protection Branch, Canadian Human Rights Commission).

428 Ibid.

429 Ibid.

policies, and practice are both effective and respectful of human rights."[430] The four steps — identifying the appropriate security measure, testing the potential discrimination, improving the security measure, and monitoring for unexpected discrimination — set a proactive approach that "can save time and money, improve a security measure's effectiveness and efficiency, and bolster public support for new and existing security initiatives."[431]

The Committee agrees with Mr. Dufresne's assessment that security can be strengthened by measures that are consistent with human rights principles. The Committee encourages organizations that collect personal information — from government institutions or private companies — to consider implementing tools such as the HRIA that can serve to improve the development of policies that prevent and redress identity theft.

H. Providing Support to Victims

The Committee heard from several witnesses that highlighted the work that is being done to assist victims of identity theft. Several government agencies and programs, such as the CRA, the Competition Bureau and the CAFC have publicly available information on how individuals can protect themselves from identity theft and what steps to take if they suspect they are victims of this crime.[432] As discussed previously, a non-governmental body, the Canadian Identity Theft Support Centre "receives funding from the federal government to provide victims of identity theft with information and support [including] hand-holding through the coping and remediation process, which can be extensive."[433]

Throughout the testimony touching upon the steps that government agencies are taking to protect Canadians from identity theft, the Committee was repeatedly reminded of the need for continuous education and outreach.[434] Initiatives that help individuals protect their personal information require collaborative effort among government agencies, private sector actors and other non-governmental, public-interest organizations. Education and outreach are also required to support those persons that become victims of identity theft and identity fraud. The Committee was similarly reminded of the need for

---

430 Ibid. See also Canadian Human Rights Commission, *The Human Rights Impact Assessment for Security Measures*.

431 Canadian Human Rights Commission, *The Human Rights Impact Assessment for Security Measures*.

432 See, for example, Canada Revenue Agency, *Protect Yourself Against Identity Theft*; Competition Bureau, *The Little Black Book of Scams*; and CAFC, *Identity Theft: Could it Happen to You?*

433 ETHI, *Evidence*, Meeting No. 19, 2nd Session, 41st Parliament, 29 April 2014, 1145 (Lawson).

434 ETHI, *Evidence*, Meeting No. 16, 2nd Session, 41st Parliament, 1 April 2014 (Jenkin); ETHI, *Evidence*, Meeting No. 17, 2nd Session, 41st Parliament, 3 April 2014 (Cormier and Currie); ETHI, *Evidence*, Meeting No. 18, 2nd Session, 41st Parliament, 8 April 2014 (Gardner-Barclay and Brown); ETHI, *Evidence*, Meeting No. 19, 2nd Session, 41st Parliament, 29 April 2014 (Fernandez and Lawson); ETHI, *Evidence*, Meeting No. 26, 2nd Session, 41st Parliament, 3 June 2014 (Dorey, Scott and Israel). See also ETHI, B.C. Freedom of Information and Privacy Association, *Written Submission: Identity theft and its economic impact,* 13 March 2015.

coordinated and sustained efforts to collect information and analyze data on the scope and parameters of identity crime in order to better tailor prevention programs and victim support initiatives.[435]

Lastly, it was impressed on the Committee that "a national strategy on identity crime victim support should be adopted that will establish clear parameters for cooperation between the various entities involved in the victim support process, such as the Canadian Anti-Fraud Centre, the Canadian Identity Theft Support Centre, and the various regulatory agencies that deal with identity theft matters."[436] In the Committee's views, such a strategy could compliment the one developed by the RCMP in 2012 and it makes recommendations with that objective in mind.

For these reasons, the Committee makes the following recommendations:

Recommendation 6: The Committee recommends that the Government of Canada continue to promote efforts and allocate resources to protecting Canadians from identity theft, providing support services to victims of identity theft, and prosecuting those who commit identity crimes.

Recommendation 7: The Committee recommends that the Government of Canada consider ways to further promote collaboration among private and public sector stakeholders, including consumer protection agencies and privacy commissioners at both federal and provincial levels. Such collaboration should extend beyond education and outreach programs to include the development of mechanisms to gather reliable, reasonably comprehensive data on the incidence, types and costs of identity crimes in Canada, and the sharing of that data for research and analysis purposes.

---

435 ETHI, *Evidence*, Meeting No. 19, 2nd Session, 41st Parliament, 29 April 2014 (Fernandez and Lawson); ETHI, *Evidence*, Meeting No. 19, 2nd Session, 41st Parliament, 1 May 2014 (Levin); ETHI, *Evidence*, Meeting No. 26, 2nd Session, 41st Parliament, 3 June 2014 (Dorey, Scott and Israel). See also ETHI, B.C. Freedom of Information and Privacy Association, *Written Submission: Identity theft and its economic impact,* 13 March 2015.

436 ETHI, *Evidence*, Meeting No. 26, 2nd Session, 41st Parliament, 3 June 2014, 1240 (Israel). See also ETHI, *Evidence*, Meeting No. 19, 2nd Session, 41st Parliament, 29 April 2014, 1150 (Lawson);

CONCLUSION AND RECOMMENDATIONS

In light of the testimony heard during the series of meetings held between April 2014 and February 2015, and of the briefs submitted from government departments and agencies, law enforcement organizations, interest groups, universities, law firms, credit reporting agencies, banks and information technology companies, the Committee makes the following recommendations:

Recommendation 1: The Committee urges consumer credit reporting agencies to provide Canadian consumers with electronic access to their credit file free of charge at least once a year.

Recommendation 2: The Committee urges Canadian banks to adopt, as a common definition of identity theft, the definition that appears in the current *Criminal Code* of Canada and to compile data on identity theft accordingly.

Recommendation 3: The Committee urges Canadian banks to make public the information they have on identity theft. The information should include unsuccessful as well as successful attempts to steal personal information and should also include information about the source of the attack.

Recommendation 4: The Committee invites Canadian banks to invest in technological measures to protect customer information. These measures should include audit systems that log the number of times customer records are accessed and how they are accessed.

Recommendation 5: The Committee recommends that the Government of Canada seek provincial and territorial support in considering the establishment of a national strategy to coordinate efforts to combat identity theft and address this crime more effectively.

Recommendation 6: The Committee recommends that the Government of Canada continue to promote efforts and allocate resources to protecting Canadians from identity theft, providing support services to victims of identity theft, and prosecuting those who commit identity crimes.

Recommendation 7: The Committee recommends that the Government of Canada consider ways to further promote collaboration among private and public sector stakeholders, including consumer protection agencies and privacy commissioners at both federal and provincial levels. Such collaboration should extend beyond education and outreach programs to include the development of mechanisms to gather reliable, reasonably comprehensive data on the incidence,

types and costs of identity crimes in Canada, and the sharing of that data for research and analysis purposes.

APPENDIX A:
LIST OF WITNESSES

Organizations and Individuals	Date	Meeting
Department of Citizenship and Immigration	2014/04/01	16
Peter Bulatovic, Director Investigation Division, Passport Program Integrity Branch		
Lu Fernandes, Director General Passport Program Integrity Branch		
Department of Employment and Social Development		
Louis Beauséjour, Assistant Deputy Minister Integrity Services Branch, Service Canada		
Robert Frelich, Director Enterprise Identity Services Divison, Service Canada		
Department of Industry		
Michael Jenkin, Director General Office of Consumer Affairs		
Department of Industry	2014/04/03	17
Morgan Currie, Acting Assistant Deputy Commissioner of Competition Competition Bureau, Fair Business Practices Branch Division C		
Thomas Steen, Major Case Director and Strategic Policy Advisor Competition Bureau, Fair Business Practices Branch		
Royal Canadian Mounted Police		
Jean Cormier, Director Federal Coordination Centres		
Cameron Miller Federal Coordination Centers, Domestic		
Canada Revenue Agency	2014/04/08	18
Helen Brown, Director General Security and Internal Affairs Directorate, Finance and Administration Branch		
Susan Gardner-Barclay, Assistant Commissioner and Chief Privacy Officer Public Affairs Branch		
Canadian Human Rights Commission		
Philippe Dufresne, Director General and Senior General Counsel Human Rights Protection Branch		
Maciej Karpinski, Senior Research Analyst Human Rights Protection Branch		

Organizations and Individuals	Date	Meeting
As individuals	2014/04/29	19
José Manuel Fernandez, Associate Professor Department of Computer and Software Engineering, École Polytechnique de Montréal		
Philippa Lawson, Barrister and Solicitor Associate, Canadian Internet Policy and Public Interest Clinic, University of Ottawa		
Susan Sproule, Assistant Professor Finance, Operations and Information Systems, Brock University		
International Centre for Comparative Criminology		
Benoît Dupont, Director		
As individuals	2014/05/01	20
Éloïse Gratton, Partner and Co-Chair Privacy, McMillan LLP		
Avner Levin, Associate Professor and Director Privacy and Cyber Crime Institute, Ryerson University		
Equifax Canada Co.	2014/05/27	24
Carol Gray, President		
John Russo, Vice-President, Legal Counsel and Chief Privacy Officer		
Tara Zecevic, Vice-President Decision Solutions		
Forrest Green Group of Companies		
Robert K. Groves, Representative Prinicipal, The Aboriginal Affairs Group Inc.		
Murray Rowe, Jr., President		
TransUnion Canada		
Chantal Banfield, Vice-President and General Counsel		
Todd Skinner, President		
BMO Financial Group	2014/05/29	25
Ed Rosenberg, Vice-President and Chief Security Officer Legal, Corporate and Compliance Group		
Canadian Imperial Bank of Commerce		
Philip Fisher, Senior Director, eChannels Risk Management, Integrated Business Control Services		
Royal Bank of Canada		
Jay Stark, Vice-President Internal Audit Services, Personal and Commercial Banking		

Organizations and Individuals	Date	Meeting
Scotiabank	2014/05/29	25
Jennifer Frook, Director Shared Services, Fraud Management Office		
TD Bank Financial Group		
Paul Milkman, Senior Vice-President Head of Technology Risk Management and Information Security		
Canadian Identity Theft Support Centre	2014/06/03	26
James Dorey, Executive Director		
Kevin Scott, President		
Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic		
Tamir Israel, Staff Lawyer		
Google Inc.	2014/06/05	27
Colin McKay, Head, Public Policy and Government Relations		
Rogers Communications Inc.		
Kenneth Engelhart, Senior Vice-President Regulatory and Chief Privacy Officer		
Aaron Storr, Director Law Enforcement Support		
As an individual	2015/02/23	33
Claudiu Popa, Chief Executive Officer, Informatica Corporation		
Crime Prevention Association of Toronto		
Janet Sherbanowski, Executive Director		

APPENDIX B:
LIST OF BRIEFS

Organizations and Individuals

B.C. Freedom of Information and Privacy Association

Digital ID and Authentication Council of Canada

Gagnon, Maxime

Levin, Avner

REQUEST FOR GOVERNMENT RESPONSE

Pursuant to Standing Order 109, the Committee requests that the government table a comprehensive response to this Report.

A copy of the relevant *Minutes of Proceedings* (Meetings Nos. 16-20, 24-27, 33-36) is tabled.

Respectfully submitted,

Pierre-Luc Dusseault

Chair

NDP Supplementary Report on The Growing Problem of Identity Theft and its Social and Economic Repercussions by the Standing Committee on Access to Information, Privacy and Ethics.

While we support the overall conclusions and recommendations of the Committee report, the New Democratic Party believes that the government has failed to address some key aspects of identity theft and its impacts.

The NDP agrees that identity theft is a growing problem that the Canadian Government must take seriously. The fight against identity theft and the protection of personal information are key components of a strong digital economy in Canada. Canadians need to have confidence in the digital technologies that they use. This means that Canadians must feel safe when disclosing their personal information online so that they do not leave themselves vulnerable to identity theft. It is up to government to ensure that Canadians' information is, in fact, safe from theft, and that the information government holds is adequately protected. We need privacy protections and policies that are suited to the 21st century.

The study conducted by the ETHI committee in many ways reiterated the need for the Government and industry leaders to address the growing problem of identity theft. The New Democratic Party makes the following additional common-sense recommendations:

Supplementary recommendation 1: The NDP urges Internet Service Providers and IT companies to publicly and annually report all requests made from government agencies for personal subscriber information. The reports should include the number of requests, the types of information requested and the ISP's responses to the request.

During their respective testimonies, Rogers and Google both stipulated that their organizations have committed to publicly reporting the numbers of requests for personal information made by government agencies. The NDP commends this positive step forward and believes that all Internet service providers and IT companies should follow their lead to increase transparency surrounding government agency requests for personal information. This practice helps Canadians make informed decisions and understand the implications of the potential use of their personal information.

Supplementary recommendation 2: The NDP recommends that the Government publish an annual report containing information on the number of requests made to Internet service providers for personal subscriber information. The reports should include requests broken down by government agencies, the types of information requested and the success of the request.

As suggested by Rogers during their testimony, government agencies must also play a part in shining the light on the millions of requests that are made to Internet service providers by government agencies each year. The NDP believes that Canadians have a right to know when the government requests their personal information. Increased transparency in this area is a must.

Supplementary recommendation 3: The NDP recommends that the Government of Canada develop a targeted strategy to reduce the occurrence of identity theft in First Nations communities.
Testimony heard by the committee by Forest Green made it quite clear that First Nations are particularly vulnerable to having their identities stolen. The NDP thinks that their particular vulnerability requires a targeted strategy. A blanket approach to the problem of identity theft will not adequately address the particular realities of First Nation communities.

Supplementary recommendation 4: The NDP recommends that the Canada Revenue Agency develop guidelines surrounding the use of Social Insurance Numbers by private organizations.
There is currently no law in place that restricts private organizations from requesting Canadians to provide their Social Insurance Numbers (SINs) for purposes other than those relating to employment or taxes. This policy vacuum leads to the potential abuse of SINs that could lead to cases of identity theft.

Supplementary recommendation 5: The NDP recommends that the Government of Canada consider ways in which it could allow private organizations to verify the authenticity of government issued I.Ds.
Testimony given by TransUnion raised the concern that private organizations had no method of verifying the authenticity of government issued I.D. Addressing this problem will help diminish the use of counterfit government I.D.s and thus help reduce the occurrence of identity theft.

Supplementary recommendation 6: The Committee urges that credit monitoring agencies offer credit freezes to their customers.
As highlighted by witness Philippa Lawson, Canadian credit agencies do not currently offer credit freezes that would prevent credit agencies from divulging a customer's credit history. New Democrats believe that many cases of identity theft could be prevented by offering this service.

Supplementary recommendation 7: The NDP recommends that the Government of Canada update the Privacy Act to include mandatory data breach reporting requirements for all government agencies.
When data breaches go unreported, it is impossible for Canadians to take the necessary steps to protect themselves against the threat of identity theft. By refusing to update the Privacy Act to make it mandatory for all government departments to report data breaches, the Government is refusing to give Canadians the tools they need to protect themselves.

Supplementary recommendation 8: The NDP recommends that the Government of Canada give the Privacy Commissioner of Canada order making power to ensure compliance to Canadian privacy laws such as PIPEDA and the Privacy Act.
The Government must give the Privacy Commissioner the tools he needs to do his job to ensure the protection of Canadian's personal information. Unfortunately the

government's refusal to update our privacy laws for the 21st century has put the protection of Canadian's privacy at risk in the modern global economy.

The common sense recommendations found in our supplementary report reiterate the NDP's support for measures that will counter the growing problem of identity theft and ensure that there is a comprehensive plan to address this problem.