A Stolen Life:
Ameliorating the Impact of Database Breaches on Canadians

by

Dennis Anthonipillai

B.A. (Psychology), University of Victoria, 2017

Project Submitted in Partial Fulfillment of the
Requirements for the Degree of
Master of Public Policy

in the
School of Public Policy
Faculty of Arts and Social Sciences

SIMON FRASER UNIVERSITY
Spring 2020

Approval

Name:	**Dennis Anthonipillai**
Degree:	**Master of Public Policy**
Title:	***A Stolen Life: Ameliorating the Impact of Database Breaches on Canadians***
Examining Committee:	**Chair:** Dominique Gross Professor, School of Public Policy, SFU
	Maureen Maloney Senior Supervisor Professor
	Yushu Zhu Internal Examiner Assistant Professor
Date Defended/Approved:	March 30, 2020

Ethics Statement

The author, whose name appears on the title page of this work, has obtained, for the research described in this work, either:

a. human research ethics approval from the Simon Fraser University Office of Research Ethics

or

b. advance approval of the animal care protocol from the University Animal Care Committee of Simon Fraser University

or has conducted the research

c. as a co-investigator, collaborator, or research assistant in a research project approved in advance.

A copy of the approval letter has been filed with the Theses Office of the University Library at the time of submission of this thesis or project.

The original application for approval and letter of approval are filed with the relevant offices. Inquiries may be directed to those authorities.

Simon Fraser University Library
Burnaby, British Columbia, Canada

Update Spring 2016

Abstract

Database breaches on companies put at risk a large amount of personal information that can be accessed by third parties. Canadians, in general, will feel the impact of these database breaches through their identities being used in fraudulent activity. The literature suggests that database breaches are a large and growing issue, identity theft is rising, and the current victims are not given enough options to protect themselves from the identity theft that uses information obtained in database breaches. This paper attempts to fill the gaps in the Canadian regulatory environment by evaluating policies for either reducing the impact of database breaches or reducing the impact on victims of identity theft. Four policy options are presented with a focus on creating a strong regulator, enacting baseline standards, comprehensive reporting and data collection, or protection services.

Keywords: Database Breach; Identity Theft; Personal Information; Cybersecurity

Table of Contents

List of Tables

List of Figures

List of Acronyms

ACORN	Australian Cybercrime Online Reporting Network
ASEAN	Association of Southeast Asian Nations
CCPA	California Consumer Privacy Act
Cifas	Credit Industry Fraud Avoidance Scheme
CNIL	Commission nationale de l'informatique et des libertés an independent regulatory body overseeing privacy and data protection
DVS	Document Verification Service
EU	European Union
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
ICO	The Information Commissioner's Office
LAC	Library and Archives Canada
OECD	Organisation for Economic Co-operation and Development
PIPA	Personal Information Protection Act
PIPEDA	The Personal Information Protection and Electronic Documents Act
SFU	Simon Fraser University
SHIELD	Stop Hacks and Improve Electronic Data Security Act
SIN	Social Insurance Number
SMB	Small and Medium-sized Business
UK	United Kingdom

Executive Summary

Database breaches occur when there is an unauthorized acquisition or access to a computerized database. The issue is that the personal information that is compromised by a database breach can lead to negative impacts that include identity theft. This paper explores mitigation policies that Canada can take to address the impact of database breaches. To start, I explore what a database breach is, who the stakeholders are, the impacts, and the policy responses the literature recommends. I then investigate the primary impacts which are identity theft and the overall impacts on victims. Identity theft from these breaches impacts anyone and everyone. Identity theft occurs when someone takes your personally identifying information to assume an individual's identity. This fake identity can be used to open bank accounts, apply for loans, or make purchases under someone's name. The issue of identity theft is large as it is the fastest growing crime in Canada.

I use a jurisdictional scan of policies in the UK, the U.S, and Australia to identify the scale of database breaches and their impacts, initiatives to reduce the impacts of breaches, and the state of identity theft and identity theft reduction initiatives. The U.K, at the time of this study, was under the jurisdiction of the EU and their policies namely the *General Data Protection Regulation* (GDPR). This powerful regulation has been adopted by some states and has set a new standard for data protection and cybersecurity. I identify four potential policy options for consideration. The four policy options are either to enhance a strong regulator to give large fines when there is a lack of effort to reduce the impact or incidence of a breach, create baseline cybersecurity standards, create a comprehensive identity theft reporting and data collection system, or provide identity theft protection services.

With these policy options in mind, I have conducted four semi-structured interviews with experts in the field to explore the impact of the options. These options were then evaluated using five criteria: security & protection, compliance issues, efficiency, cost, and stakeholder acceptance. Security & protection was given more weight due to it being the primary policy objective. Very strong regulations come with its difficulties in enforcing compliance in smaller businesses. The policy option to introduce mandatory baseline cybersecurity standards does not directly impact the wellbeing of victims which is its only weakness with a medium impact on the risk of identity theft.

Comprehensive identity theft reporting was compared against identity theft protection services to see which option more impact would the wellbeing of victims. Comprehensive reporting systems are impactful after identity theft and have no real impact on the wellbeing of victims of a database breach.

The recommendation is to adopt both baseline cybersecurity standards and identify ways to introduce more identity theft protection mechanisms to reduce the loss of identity theft from occurring.

Chapter 1.

Introduction

A database breach is an unauthorized access to a database that can compromise the security of personal information. From 2018 - 2019, at least 28 million Canadians have been impacted by a database breach[1]. The largest database breach in 2019 impacted LifeLabs, the largest medical diagnostic lab in Canada, which had compromised the personal information of 15 million Canadians[2]. Companies of all sizes are experiencing a drastic increase in the number of breaches. When a database is breached, the hackers or state actors will have access to personal information such as full names, addresses, emails, driver's licenses, and Social Insurance Numbers (SIN) numbers. The primary consequence of database breaches is identity theft[3]. Information obtained in database breaches is either used by the hacker or sold on online markets.

Identity theft refers to when a third party uses the identity of another person for an illegal purpose. Identity theft has three steps, the acquisition of the information, the modification of information and finally, the fraud itself. There has been a 12-year rise in the incidence of identity theft. From 2008 to 2018, there has been a 46% increase and recently from 2017 to 2018, there has been a 12% increase.

There is a rising incidence of database breaches which puts Canadians at greater risk of identity theft. The primary concern of this paper is to identify potential policy options for the federal government to mitigate the impacts of database breaches on Canadians. This is done in four steps. First, I explore the literature surrounding database breaches, identity theft, and victims. Second, I conduct a case-study analysis of the United Kingdom, the United States, and Australia. The case study explores the impacts of database breaches and what is being done by the jurisdictions to mitigate the impact. Third, I use the findings of the case study to inform 4 semi-structured interviews.

[1] Shah 2019

[2] Abedi 2019

[3] Commonwealth of Australia 2014

Fourth, I use the findings of the interviews and case-study analysis to identify gaps for potential policy options to mitigate the impact of database breaches

Chapter 2.

Background

The analysis investigates and defines database breaches, identity theft, and victims of identity theft. The literature informed the definition of terms, characterization of stakeholders, and a description of impacts. First, I explore and define database breaches and the stakeholders, impacts, and responses. Second, I investigate identity theft and define the victims of identity theft. Last, I describe the Canadian federal regulatory framework regarding database breach mitigation and identity theft reduction initiatives.

2.1. Database Breaches and Impacts

2.1.1. Definition of Terms

Database breaches are an "unauthorized acquisition or access of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector"[4]. So long as there is personal information collected and stored in a database, there is a risk that your personal information can be accessed, stolen, and eventually used. The information obtained in the database breach can be used by the hackers to conduct identity fraud of some sort, or they can sell it to a third party through the internet who will then use this information to commit identity fraud. Hacking is the most common method of conducting a database breach, shown with almost 60% of all breaches being caused by hacking[5]. Hacking includes phishing, ransomware, malware, and skimming.

Database breaches happen when the security is low enough that a reasonably skilled hacker can gain access[6]. The higher the security, the more difficult it is for a hacker to access the database. There are primary factors in breaching a database includes the: the amount of data needed to gain access to the database, the skill

[4] Anandarajan, D'Ovidio, and Jenkins 2013

[5] Identity Theft Resource Center 2018

[6] Roberds and Schreft 2009

necessary to access the database, and the amount of information that could be obtained through the database. Database attempts can happen at any company, while successful attempts are more likely to happen at companies with weaker cybersecurity mechanisms.

2.1.2. Stakeholders

All companies that hold the personal data of people would be a stakeholder in legislation or actions targeting database breaches and the use of that data. This would include large companies, banks, and credit bureaus such as Google, Equifax, TransUnion, CIBC, T.D., BMO, and RBC[7]. Canadian citizens who share their personal information with a third party or apply for credit in Canada are also a stakeholder in database breaches since it is their data that is compromised.

2.1.3. Impact of Database Breaches

In 2019, the Office of the Privacy Commission of Canada (OPC) reported that from November 1st, 2018 and October 2019 there have been 446 database breaches that have impacted at least 19 million Canadians. Of these breaches, 58% were conducted by a third party, 22% were from accidental disclosures, 12% is from physical loss, and 8% of that was from physical theft[8]. Physical loss can include losing hardware that contains personal information. Physical theft can include the theft of computer hardware that contains personal information.

[7] Dusseault 2015

[8] OPC blogger 2019

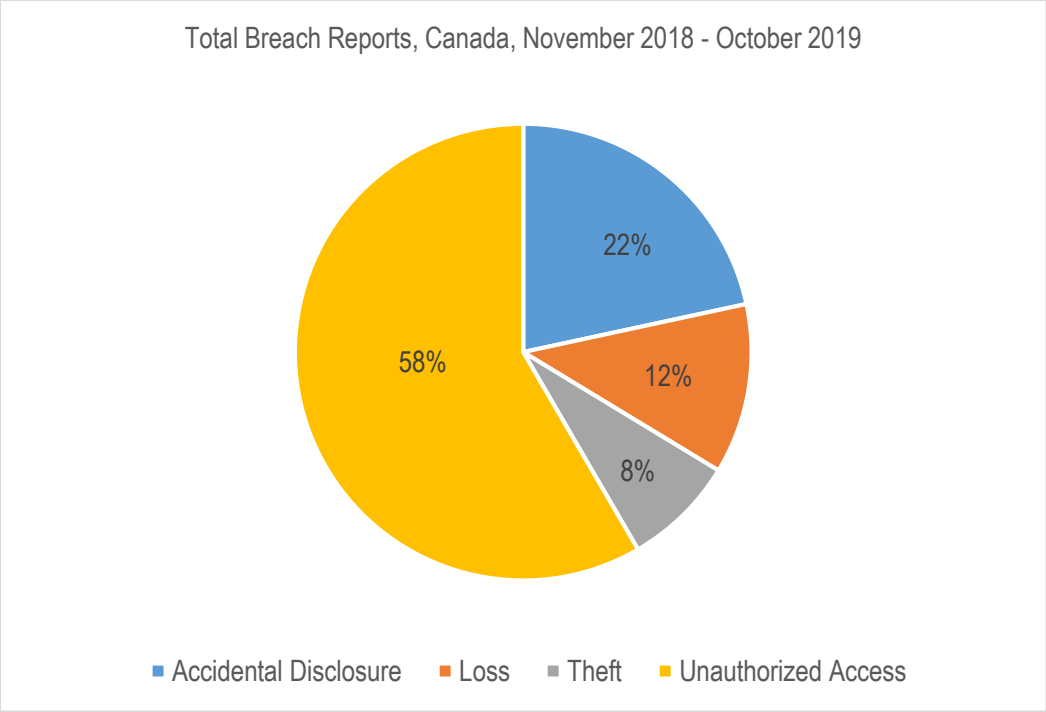

Figure 1: Type of Database Breaches in Canada, 2018-2019[9]

As noted in Figure 1, unauthorized access is the most common cause of a database breach. In Canada, a database breach costs 4.44M in 2019 on average, which is the fourth highest globally[10]. The cost per record in Canada is $187, while the average size of a database breach is 23,000 records[11]. These do not include the costs to consumers from the information obtained in the database breach. Increasing cybersecurity practices including encryption, data loss prevention, and security by design, were all associated with lower costs for companies. Encryption specifically saved companies $360,000 on average and an incident response team saves $1.23M when there is a breach. The report recommends having an incident response team so that when there is a breach, it can be contained fast to avoid other potential costs[12].

Although the numbers we see in costs to companies seem to be high, the issue is that many companies do not act on reducing these costs. A reason could be that in

[9] Ibid

[10] IBM Security and Ponemon Institute 2019

[11] Ibid

[12] Ibid

the long run, there is little to no long-term economic impact on larger companies[13]. What this means, however, is that costs to the overall economy are larger than the costs to any specific company.[14]

2.1.4. Database Breaches and Identity Theft

The Canadian government does not currently collect publicly available information on the relationship between database breaches and the incidence of identity theft. However, a study conducted in the U.S found that identity theft is one of the most common outcomes from database breaches[15]. Those who have been impacted by a database breach are 31.7% more likely to experience identity fraud compared to just 2.8% of individuals not notified of a data breach in 2016[16].

There is a link between database breaches and an increased risk of identity theft. Information obtained in a database breach is then either sold on online markets or used by the hacker[17]. These marketplaces prioritize credit card and bank account information. When this information is sold on online marketplaces, it is sold in bulk and contains personally identifiable information that can be used to commit an identity-related crime in the future. There is a cost to all stakeholders when there is a database breach the researchers report that the median value of goods obtained through fraud is $1350 per stolen identity. There are additional costs, including the time of discovering how it happened, contacting all relevant parties, resolving identity theft, and "breach costs." A breach cost is where the company notifies those whose records have been compromised. The costs associated with the breach costs include the notification costs ($13 per data record breached), labour costs ($30 due to lost productivity per record), and the costs of managing legal liabilities ($11). These costs impact the victim, the company, and the government[18].

---

[13] (Richardson, Smith and Watson 2019)

[14] Ibid

[15] Tatham 2018

[16] Ibid

[17] Verizon 2019

[18] Roberds and Schreft 2009

2.2. Identity Theft

2.2.1. Definition of Terms

Identifiable information. The Government of Canada defines personal information in the *Personal Information Protection and Electronic Documents Act* (PIPEDA)[19]. Personal information includes age, name, ID numbers; income; ethnic origin; blood type; opinion; evaluations; comments; social status; disciplinary actions; employee files; credit records; loan records; medical records; and intention to acquire goods, acquire services, or change jobs.

Identity Theft. Identity Theft is defined as "the fraudulent use of another person's identification to gain an advantage, obtain property, disadvantage another person, avoid or defeat or obstruct the course of justice[20]." That is to say, the procuring of identifiable information is identity theft when the stolen identifiable information is used to gain an advantage. The process of identity theft has three components the acquisition of personal information, the sale or modification of the information, and the fraud itself[21]. Identity theft can include financial identity theft, medical identity theft, criminal identity theft, driver's license identity theft, social security, identity theft, synthetic identity theft, child identity theft, and business identity theft.

Victims of Identity Theft. Victims of identity theft come from all geographical regions and all socio-economic backgrounds. Victims include both individuals and businesses. All people who give their personal information to any service online or have something as innocuous as a bank account is at risk.

2.2.2. Techniques of Identity Theft

Identity theft can happen with the use of a variety of techniques[22]. There are three modes of identity theft, physical theft, technology-based theft, and social engineering. Of these modes, the authors identify 23 different techniques employed by

[19] Office of the Privacy Commissioner of Canada 2020

[20] Ibid

[21] Ibid

[22] Canadian Internet Policy and Public Interest Clinic 2007b

identity thieves. Identity theft techniques involving physical theft include dumpster diving, change of address, skimming, insider theft, purchasing stolen information, and identity consolidation. Online techniques include phishing, pharming, spyware, keyloggers, malware, and viruses; internet searches, google hacking; and exploring computer systems' security vulnerabilities. Keyloggers are programs that record button presses on the computer to copy passwords. Spamming and phishing techniques are used to dupe people who think they are receiving legitimate communications. Social engineering happens when hackers use bits of personal information to convince customer service representatives to hand over more information. These are methods that are used either to access a database or commit identity theft.

2.2.3. The Scale of Identity Theft

The primary impact of a database breach on Canadians is identity theft. The primary outcome of a database breach is identity theft at a rate of 31.7% of breach victims in 2016 reporting theft. Those who are notified of being a victim of identity theft in 2016 reported at a rate of 2.8%. In the U.S, the Federal Trade Commission (FTC) reports that identity theft accounted for 13.86% of all consumer complaints in 2017. Database breaches increase the ease of committing identity theft and identity-related fraud. There has been a 12-year rise in the incidence of reported identity theft. Between 2017 and 2018, the government noted a 12% increase. In real terms, there were 3,745 incidents of identity theft reported to police and 15,839 incidents of identity fraud reported to the police[23]. The number only captures those who have taken steps to report to the police. Many victims do not report to all of the departments they are asked to. For example, the Canadian Anti-Fraud Centre in 2018, received 9,886 reports of identity theft and 9,173 complaints from victims of identity fraud. They estimate the 9,173 complaints represent only 5% of actual victims. The conservative estimate about the true number of victims is that 42 in 100,000 Canadians have been impacted by identity fraud[24].

[23] Statistics Canada 2019

[24] Northcott 2018

2.2.4. Impact on Victims

The impact on the pockets of victims is noticeable. In 2014, the Canadian Anti-Fraud Centre reported that those in their 50s reported a dollar loss of nearly 10 million, while businesses reported a dollar loss of 26 million[25]. These losses were large in 2014. The financial losses rose to $11.7 million and jumped to $21.2 million due in 2018[26]. Official statistics do not report the number of identity-related crimes reported to the Canadian Anti-Fraud Center publicly. Much of this increase is related to the increase of personal information that can be accessed and used for identity fraud

Table 1: Age and Total Reported Dollar Loss, Canada 2014[27]

Age Range	Total Reported Dollar Loss
20's	$1,249,304.68
30's	$2,955,071.14
40's	$5,704,480.31
50's	$9,771,726.81
60's	$8,306,252.15
70's	$5,757,819.29
80's	$2,974,475.51
Business	$26,005,760.24
Deceased	$603,862.77
Unknown	$5,347,870.19

However, financial losses are not the only impact on victims. Studies on victims of identity theft find that they experience strong physical and emotional consequences from the burdens caused by identity theft[28]. Physical consequences can include, changes in stress levels and anxiety. Emotional consequences include 84.1 percent of

[25] Canadian Anti-Fraud Centre 2014

[26] Borzykowski 2019

[27] Ibid

[28] Golladay and Holtfreter 2017

respondents reported issues with their sleep habits, 77.3% reported increased stress, 63.6 reported problems with concentration[29]. These impacts vary based on socio-economic status, age, and race. For example, low-income populations have more difficulty in paying their rent in the event of identity theft.

2.2.5. Options for Victims

Victims of identity theft have difficulty in rectifying financial losses and recovering[30]. When impacted by identity theft there are direct financial losses, indirect financial losses, time spent rectifying the situation, impacts on physical health due to stress, emotional impact, negative impact on relationships. These losses are difficult to rectify even if the bank involved covers their losses. Currently, victims of identity theft have access to websites that provide information. The onus is on the victim to report to multiple bodies, keep track of all information, and continuously reaffirm their identity to these bodies when fraud occurs. Victims are dissatisfied and they do not like the credit issuers, credit reporting agencies, law enforcement, and other organizations that they contact because of how difficult it is to rectify the theft[31].

Canadians have few options. Some companies and credit bureaus offer identity theft insurance and credit monitoring at a cost. This includes services that assist consumers to rectify identity theft as well. However, there are issues for starters insurance companies themselves that have been impacted by database breaches. Equifax[32], the largest credit bureau and identity theft insurance provider was the subject of a database breach that impacted 143 million people, of which 19,000 were Canadians. The second is that the insurance options are expensive. Credit monitoring services cost an average of $19.95 per month in 2019[33].

Canadians have the option to place a fraud alert as well. This will notify credit issuers that the credit application could be fraudulent. Recently, some companies have provided some credit monitoring services free of charge for a limited time. For example,

---

[30] Dusseault 2015

[31] Identity Theft Resource Centre 2018

[32] CBC News 2019

[33] Ligaya 2017

Desjardins Bank offers five years of identity theft protection, which includes protection, support, and reimbursement when there is the theft of identity since they have been impacted by a breach[34]. When identity theft occurs from the database breach is when you have access to other services.

2.3. Current Regulatory Framework

2.3.1. Database Breach Initiatives

In 2000, Canada was one of the first countries to adopt legislation against database breaches and identity theft with the *Personal Information Protection and Electronic Documents Act* (PIPEDA). This law came into full force in June 2009. The PIPEDA regulates the collection and treatment of personal data across private-sector organizations that have businesses that operate in Canada for profit. This applies to organizations that are in provinces without similar protections. Provinces with similar protections to the PIPEDA include Alberta, British Columbia, and Quebec. The PIPEDA has ten principles for businesses to ensure accountability; identifying purposes, consent, limited collection, limiting use, disclosure, and retention; accuracy, safeguards, openness, individual access, and challenging compliance[35].

In 2018, the PIPEDA was amended to include mandatory breach notification requirements to include mandatory reporting to the Privacy Commissioner of Canada of breaches that pose a significant risk to the individual and to notify individuals of breaches “when appropriate.” This database breach notification requirement exists on top of the existing legislation and requirements[36]. In this amendment, all organizations need to notify the government when there is a breach that poses a real risk of significant harm. The notification needs to describe what was taken, when it was taken, how it was taken, and what the organization will do to reduce the risk of harm. Organizations that knowingly do not report a database breach when it does pose that harm can be subject to fines on a summary offence not exceeding $10,000, or an indictable offence liable to a fine not exceeding $100,000. The responsibility to notify individuals is on the

[34] Desjardins 2019

[35] Office of the Privacy Commissioner of Canada 2020

[36] Ibid

organization when there is a real risk of significant harm to the individual. More information on the PIPEDA is in Appendix A.

Other than the PIPEDA, the Government of Canada is exploring strengthening the minimum levels of cybersecurity by providing the "CyberSecure" Program[37]. The CyberSecure program is a government-backed program for small to medium-sized businesses (SMBs) to pay third-party security companies to support database protection efforts. The third-party security companies can identify gaps, build security controls, and certify if an SMB has baseline standards according to government standards[38]. The program provides a process and assessment mechanism for SMBs and all organizations to be certified by approved bodies as having appropriate minimum standards. The certification comes with a badge that will show that they are CyberSecure. Baseline cybersecurity controls include a cyber incident response plan, enable security software, user authentication, secure mobile devices, secure websites, etc.[39] These baseline standards are not mandated, they are recommended for SMBs. This solution can be used by larger companies; however, larger companies have more complex information systems that would not be covered under the CyberSecure program. There is no support for SMBs financially to encourage the transition to secure their data.

2.3.2. Identity Theft Reduction Initiatives

The Government of Canada is currently undertaking several programs to educate people about identity theft. Government initiatives include websites, special reports, and public awareness campaigns[40]. If impacted by identity theft, the Government of Canada and British Columbia[41] place the onus of rectifying and identifying the theft on the victim. They are asked to call and notify police, the financial institutions, Canada's Antifraud Centre, Equifax, and TransUnion for a fraud alert. Victims of a database breach can purchase credit monitoring. Credit Monitoring is a service, provided by Equifax, TransUnion, or major banks that contact you regarding suspicious accounts, offer

[37] Soloman 2019

[38] Canadian Centre for CyberSecurity 2019

[39] Ibid

[40]Dusseault 2015

[41] VictimsInfo 2019

identity theft restoration, identity theft assistance, and identity theft insurance services for a price. The issue of credit monitoring needs to involve both credit bureaus since some financial institutions contact one bureau and not the other.

Chapter 3.

Methodology

This paper aims to identify what needs to be done by the Canadian federal government to mitigate the impact of corporate database breaches on Canadians. Database breaches on companies pose a risk in increasing this incidence due to the sheer amount of personal information that will be accessed by third parties. The number of people impacted by identity theft keeps growing, database breaches increase the risk of identity theft. The research is conducted using two methodologies including a case study analysis and expert interviews.

3.1. Framework for Analyzing Case Studies

The first methodology aims to identify the policies and programs used by other jurisdictions to reduce the impact of database breaches. The case study analysis will investigate actions taken by Canada, the United Kingdom, the United States, and Australia towards database protections, identity theft, and identity-related crime. The U.K was chosen due to its application of the *General Data Protection Regulation* (GDPR) and how it operates in the U.K. The U.S was chosen because of the states that have recently adopted new database breach mitigation policies, Australia was chosen due to their vulnerability to identity theft and to understand their approach to mitigate those impacts.

This analysis aims to test policies that are different from Canada's current regime and explore its impacts on the incidence of identity theft or database breaches. The cases will be compared with the following criteria: database breach scale and impact, database breach initiatives, and identity theft reduction initiatives.

When looking at the database breach scale and impact this paper considers the relative number and size of database breaches and the impact of legislation on the number and impact of those breaches. The more database breaches, the more consumer information will be compromised. A decrease in this number is the best possible outcome. However, stronger legislation can lead to more accurate and consistent reporting of database breaches. Exploring the database breach scale and

impact will be done by identifying the level policies or programs in place to limit the impact of the breaches themselves.

I investigate identity theft reduction initiatives by exploring the specific policies or programs that have been implemented by the government or the private sector. There will be an explanation of how the policies or program impacts database breach impact or scale. The level to which jurisdictions provide supports for those impacted by identity theft will be examined. Specifically, I examine initiatives that would impact victims of database breaches. The number of options provided to individuals is an indicator of the size of identity theft reduction initiatives.

3.2. Qualitative Interviews with Experts

I connect the findings of the case study analysis with the knowledge of experts or those with experience in dealing with identity theft or an identity-related crime. Interviews are useful in that it gives a unique perspective on the findings of the case study analysis. This unique perspective can also be applied to target policy options. The experts can speak from experience on the topics of real impact and feasibility in the Canadian landscape. The study consisted of 4 semi-structured interviews with experts involved in database breaches, cybersecurity, and identity theft. These interviews were 30-45 minutes in length. The interviews covered findings from the background and case-study analysis with a focus on potential policy options.

3.3. Limitations

There are limitations to this research that centers around issues with time and lack of specific datasets. I was unable to conduct a meaningful survey on those impacted by identity theft from database breaches and how they have dealt with the issue because of a limited amount of time. Also, it is difficult to capture the true impact of database breaches on the incidence of identity theft in number terms. Due to the nature of how identity theft occurs, it is difficult to trace specific events that lead to theft. However, there is an increased risk of identity theft after personal information has been exposed in a database breach. There has been some work done on this topic, the focus of this work is to describe potential methods to either reduce the frequency of breaches, the impact of breaches, and its role in identity theft and related crime.

Chapter 4.

Case-Study Analysis

4.1. Introduction

The focus of this jurisdictional scan is to identify and explore what other jurisdictions have done to address identity theft and database breaches. Database breaches compromise information that can then be used to collect more information and then commit several identity-related crimes. This section will investigate what other countries have done to limit the number of database breaches of reducing the incidence of identity theft from the personal information found in database breaches. The jurisdictions of the U.K, the U.S, and Australia meet the criteria of similar jurisdictional, societal, institutional, and economic similarities to Canada. This allows a meaningful comparison of the impacts of database breaches and identity theft. All cases show a range of potential policy options and their impacts. When policy options are identified, they can be analyzed.

4.2. United Kingdom

4.2.1. Database Breach Scale and Impact

The number of reported database breaches from 59,000 in 2018 to 65,000 in 2019and this increase is attributed to the GDPR forcing companies to report[42]. There is also an increase in breach awareness, consumers are more aware of breaches than they were before the GDPR[43].

4.2.2. Database Breach Initiatives

In 2018 the E.U voted to ratify the GDPR that enforces data protection[44]. The GDPR aims to harmonize data privacy laws across Europe, protect and empower E.U citizens, reshape the way organizations across the region approach data privacy. The

[42] Schwartz 2019

[43] Ibid

[44] “General Data Protection Regulation (GDPR) – Official Legal Text” 2019

impetus for the GDPR was to update the 1995 Directive 95/46/EC to capture the current situation surrounding personal data. The GDPR includes OECD Guidelines, the collection limitation principle, data quality principle, purpose specification principle, use limitation principle, security safeguards principle, openness principle, individual participation principle, and the accountability principle. The enforcement of the GDPR is left up to data protection regulators known as supervisory authorities. For example, in France, the CNIL and the ICO in the U.K is responsible for administering data protection standards[45]. There are various requirements by the GDPR such as breach notification requirements, privacy by design and large fines.

The U.K has seen an increase in the number of reported database breaches from 59,000 in 2018 to 65,000 in 2019[46]. This change comes from the database breach notification requirements. These requirements state companies must notify member states when there is a breach within 72 hours and notify customers without delay after becoming aware of a breach[47]. There is also the right to be forgotten, where a person can ask a company to destroy all data collected on them by these companies. There is also the requirement for privacy by design; when systems are designed, it must be done with data protection in mind first. The U.K has seen an increase in the number of reported database breaches from 59,000 in 2018 to 65,000 in 2019[48].

Privacy by design databases the concept that the protection of consumer privacy should be considered in the building of programs, services, and databases. This includes a mandate that there are “data protection officers” who will be the “controllers and processors” who deal with a large scale, special categories of data, or data related to criminal convictions and offences. These data protection officers can be staff or external service providers; their role is to ensure that data privacy is a top concern.

Regulators can fine companies for the misuse of consumer data up to 4% of their annual global turnover or €20 million (whichever is greater). Less severe violations could result in a fine of €10 million or 2% of worldwide annual revenue[49]. These fines are

[45] DLA Piper 2019

[46] Schwartz 2019

[47] District m 2018

[48] Schwartz 2019

[49] “General Data Protection Regulation (GDPR) – Official Legal Text” 2019

orders of magnitude higher than Canada where a company may be fined 10,000 – 100,000 based on the violation. The large fines can hold accountable large companies who would otherwise be easily able to pay 10,000 – 100,000. In July 2019, British Airways was fined £183 million ($315 million) for poor security that led to malware hacking their payment page, which impacted 500,000 customers. In January 2019, Google was fined €50 million in France for insufficient transparency[50]. Even in the U.S as a result of the breach that impacted Equifax, the credit bureau paid $700 million in fines[51]. In Canada, however, the fines were not at that scale.

4.2.3. Identity Theft Impact Reduction Initiatives

From 1999 to 2013, there has been a generally consistent and exponential rise in the number of identity fraud complaints (Table 2). The Credit Industry Fraud Avoidance Scheme (Cifas) reports 174,000 incidents in 2017 and 189,000 incidents in 2018 of identity fraud in the U.K[52]. Cifas reports into the National Fraud Intelligence Bureau, the National Crime Agency, and the National Fraud Database. Cifas states that there is nothing a person can do to protect themselves from a database breach, except, limiting the amount of data that companies may have about you in the first place[53]. However, those who use online services like email, banking, or social media will find it difficult to limit how much data would be accessible. Although not all cases of identity fraud come from database breaches, breaches do allow more people to access personal information to conduct breaches. Below are some examples of policies and programs to reduce the impact of database breaches on individuals.

[50] European Commission 2019

[51] CBC News 2019

[52] Cifas 2020

[53] Ibid

Table 2: Cases of Identity Theft 1999 - 2013, U.K[54]

Year	Cases Recorded
1999	9000
2000	16000
2001	24000
2002	34000
2003	46000
2004	56000
2005	66000
2006	80000
2007	77500
2008	77600
2009	102300
2010	102650
2011	113250
2012	123600
2013	108500

Action Fraud. Not all member states in the E.U have the same processes for rectifying identity theft. The Centre for Strategy & Evaluation Services notes that the United Kingdom has an online portal for identity-related crime victims and a robust public awareness campaign. Specifically, the online portal is called Action Fraud[55]. United Kingdom residents can report the incidence of identity-related crime online, and this information may result in an investigation by law enforcement and the National Fraud Intelligence Bureau. The National Fraud Intelligence Bureau can take down bank accounts, websites, and phone numbers used by fraudsters when identified. They recommend contacting the bank and credit card company first then contacting ActionFraud which will help an individual to regain their identity.

[54] Ciccio 2014

[55] Action Fraud 2020

Protective Registration. Cifas provides a "Protective Registration," which is a service where when a financial product is applied to receive credit, the application is delayed and reviewed[56]. Protective Registration service works by adding a flag beside the name of the individual in their National Fraud Database, companies and organizations can sign up and will see the flag and can take extra steps when giving out credit. This service costs 25 pounds for two years. This service can be taken advantage of after a company notifies you that your information has been improperly accessed in a database breach.

4.3. United States

4.3.1. Database Breach Scale and Impact

In 2016 there had been a reported 1,091 database breaches. This grew to 1,579 in 2017. There are an estimated 14.2 million credit card numbers that had been exposed as well as nearly 158 million Social Security Numbers. Most of the 158 million were from the large-scale breach of Equifax, which also impacted 19,000 Canadians. Roughly half of the United States population was impacted by database breaches in 2017 alone[57]. Regularly, there are reports of large-scale database breaches on companies with little to no legislative response.

4.3.2. Database Breach Initiatives

In terms of the policy, the FTC asks that a company's data security measures are reasonable depending on the size of the company. Other than state-specific regulation regarding database breach notifications, there is no federal requirement on all companies[58]. Fifty states have some reporting requirement to impacted individuals, in cases where individuals live in multiple states, many laws need to be followed. Some states have specific kinds of personal information that triggers mandatory notifications to individuals, and they are usually expected to report it within a 30–60-day time frame.

[56] Cifas 2020

[57] Tatham 2018

[58] McNicholas and Angle 2020

There are no fines for those who violate reporting or suffer a database breach due to lack of security unless it involved a company that deals with medical information.

The United States federally does not have mandatory or legislatively enforced data and cybersecurity provisions. There are the expectations of reasonable security in individual states; for example, the state of New York passed the *SHIELD Act*, which requires reasonable security for personal information, specifying specific measures to meet these requirements, and database breach notifications. The notification should be given without delay. However, the content of the notification is dependent on the scale of impact on residents of New York. If 5,000 or more people in New York are impacted by the breach, then the notification needs to include the "timing, content, and distribution of the notices to the number of people affected.[59]" If the company's impact had customers or employees that include New York residents, then the company needs to inform the state attorney general. Under this legislation, if a company were to fail to notify individuals the residents are eligible to sue for their actual financial damages with an upper limit of $250,000.

California, as of January 1, 2020, has the *California Consumer Privacy Act* (CCPA) in effect. This legislation exists because of the lack of federal legislation and is the strongest data protection legislation in the U.S. The CCPA applies if there are annual gross revenues of USD$25 million, derives 50% or more of its annual revenues from selling the personal information of consumers, or a company that buys, receives, sells, or shares the personal information of 50,000 or more consumers[60]. This legislation affords data protection rights to Californian consumers. For example, Californians can opt-out of a company selling their data. In terms of database breaches, there are no specific security requirements other than giving the ability for individuals to sue companies if they can prove that there was a lack of cybersecurity.

4.3.3. Identity Theft Impact Reduction Initiatives

In 2017, there were a reported 344,000 incidents of identity theft. This does not include cases where identity theft is not reported or cases where the theft is not identified. Of the 344,000 reported incidents of identity theft, 133,000 reported credit

[59] "New York SHIELD Act: The Latest Amendment to NY State's Cybersecurity Law" 2019

[60] State of California - Department of Justice - Office of the Attorney General 2019

card fraud, 82,000 reported tax fraud, 55,000 reported telecom fraud, and 50,000 reported bank fraud. The reported total losses from fraud in 2017 saw a 21.6% increase from the previous year and a total of $905 million lost. There has been a steady rise in the number of people impacted by identity-related crime so much so that the United States expects that $50.9 billion will be spent on fraud detection and prevention software from 2017 to 2022[61]. On an annual basis, around 1% of the population is impacted by identity-related crime.

Credit Freezes and Alerts. U.S citizens can place freezes or fraud alerts on credit reports[62]. A credit freeze places a stop at all credit applications, and it does not allow credit to be taken out under a name. If the individual notices that they are impacted by identity theft, then they can place the credit freeze at no cost. The freeze can be lifted or temporarily lifted to have a credit application go through. A freeze prevents companies from accessing credit reports. This would not allow telecoms, banks, credit card issuers, and potential employers to look at credit. This option previously had a cost until the government intervened to give the option of having a credit freeze at no cost. A fraud alert needs to be placed individually at the three credit bureaus in the United States, which are Experian, Equifax, and TransUnion. It will not cut off access to credit reports like a freeze, and it will notify the company that is conducting the credit check to be wary of potential identity fraud.

4.4. Australia

4.4.1. Database Breach Scale and Impact

As a part of the National Identity Security Strategy, the framework is the inclusion of the reported number of database breaches as an indicator that captures the acquisition of identities. In Australia, they have found that there is limited reliable data on the true extent of data breaches. Regardless, they state that database breaches "present significant opportunities for obtaining personal information that is used in identity crime." The targeting of database breaches is vital to Australia because, on

[61] Tatham 2018

[62] FTC Consumer Information 2018

average, there is one data breach every week in Australia with an average of 20,000 records lost per incident[63].

Although there are guidelines set by the Australian government to have secure information systems, organizations are not required by law to report data breaches. The authors state that the lack of mandatory reporting results in a lower number of data breaches reported than what occurs and that citizens would not be able to take the appropriate actions The Ponemon Institute examined 22 database breaches from 2009 to 2012 and the loss to companies due to the impact of the database breach from ensuing identity theft or fraud was between $123 - $145 on average[64].

4.4.2. Database Breach Initiatives

The Australian Government provides a step-by-step process on companies how to respond to database breaches online. When a database breach occurs, the government suggests that the company contain the breach, assess the harm, notify the government and potentially individuals, and review. The theft of the record for fraud is a crime. There is a gap which is the lack of any government legislation that would provide compensation to the victims. Organizations are not obligated to provide any post-breach support, and due to the frequent occurrence of database breaches, it is not financially viable to provide it to everyone impacted. There are no special protections offered to victims of a database breach.

National Identity Security Strategy. In April 2007, the Council of Australian Governments developed a National Identity Security Strategy to protect the identity of Australians[65]. The impetus for this action comes from the high rates of identity theft in Australia. All states and territories were called on to enhance the security and verification processes of individuals to combat crime. This led to the creation of an Identity Matching Service, which uses biometric data to confirm the identity[66]. This service creates an information-sharing network between the states and territories and allows authorized private sector organizations to access the service to confirm identity. This strategy

---

[63] Equifax Australia 2019

[64] Commonwealth of Australia 2014

[65] Ibid

[66] Council of Australian Governments 2017

recognized the need to quantify the scale to which identity theft impacts citizens. To do this, the Government of Australia created an identity crime and misuse measurement framework to access the effectiveness of policy and practice throughout Australia[67]. This framework includes the need to report every year about the current state of identity crime and misuse.

National Identity Crime Measurement Framework. This framework provides a comprehensive picture of identity crime and a means of understanding how identity crime changes. This framework is an incredibly comprehensive and quantitatively measurable set of performance measures that can be used by any country to capture the state and the effectiveness of identity theft protection and legislative action. Figure 1 captures how this framework is conceptualized. This model is used for an annual report created in Australia to describe the state of identity theft and identity-related crime. This can be adapted for Canadian use where a research group can release an annual report on the state of identity theft and can be tasked to collect and disseminate this data. In Australia, the Australian Institute of Criminology is charged with creating a report based on this conceptual model. A detailed description is in Appendix C.

[67] Commonwealth of Australia 2014

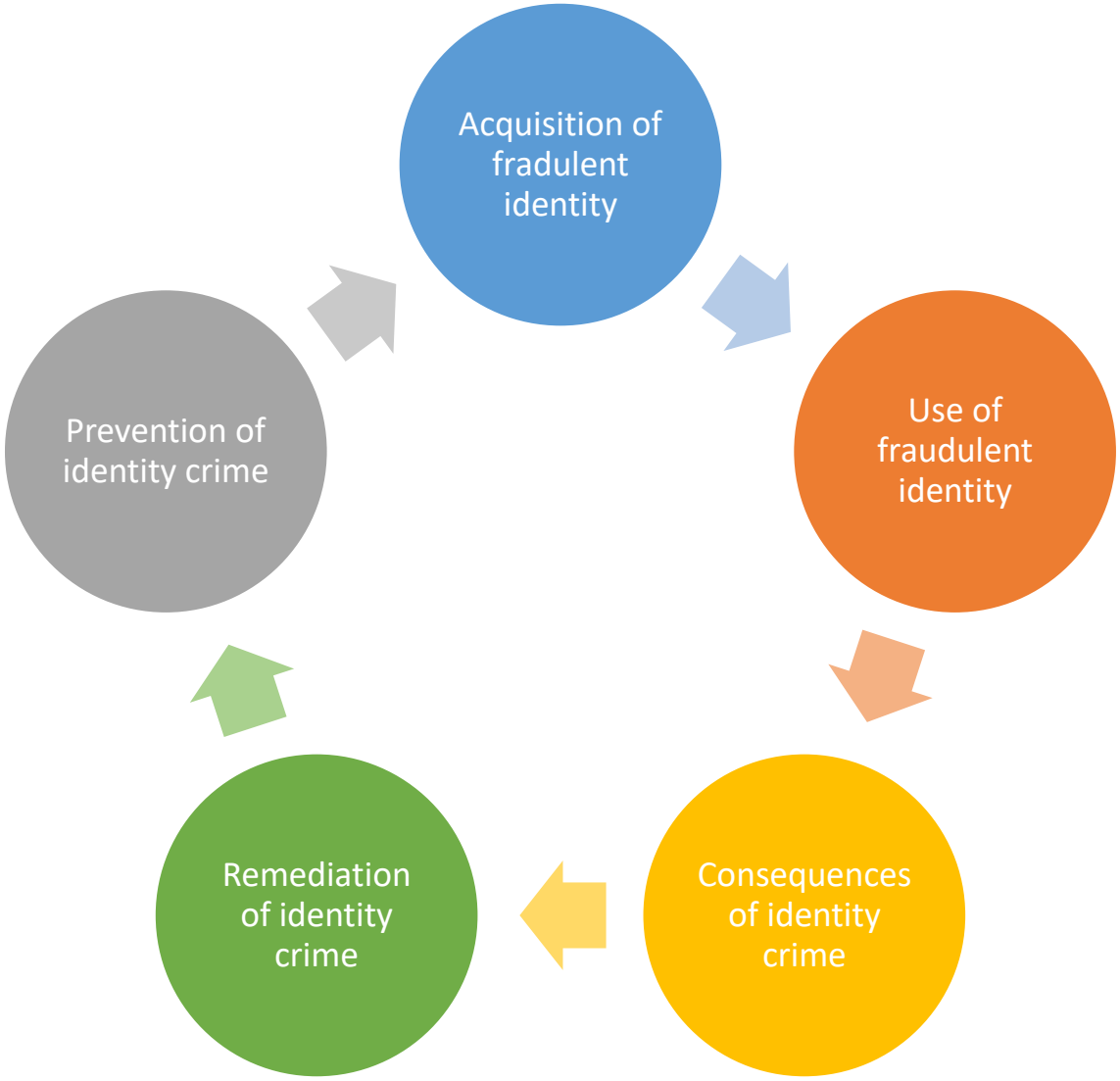

Figure 2: Adapted Conceptual Model to Measure Identity Crime in Australia[68]

4.4.3. Identity Theft Impact Reduction Initiatives

The Australian Bureau of Statistics (ABS) estimates the cost of identity-related crime costs $2.65 billion per year, with the majority lost by individuals through credit card fraud, identity theft and scams[69]. The costs include costs to individuals, governments, the justice system, and the private sector. Identity theft impacted 1 in 4 Australian's surveyed stating that they have been impacted by identity-related crime, and 13% reported that their identity had been misused in 2016.

---

[68] Ibid

[69] Goldsmid, Gannoni, and Smith 2017

Identity Matching Services. The Identity Matching Services is a government-backed service that can be provided through private companies that offer crucial matching document data with a government record[70]. Identity Matching Services include a document verification service, a face verification service, a face identification service, a One Person One License Service, a Facial Recognition Analysis Utility Service, and an Identity Data Sharing Service.

Document Verification Services. The Document Verification Service aims explicitly to work at all levels of government and can verify drivers' licenses, Australian passports, international passport visas, Medicare cards, Australian citizenship certificates, immigrations cards, registration by descent certificates, birth certificates, marriage certificates, change of name certificates, facial image template, and biometric data. This service provides access to instant verification of the validity of identity documents, decreases the incidence of identity theft, and allows some government agencies and private sector organizations to identify individuals through identity document data. Some government agencies can use Facial Recognition through identity documents and other documents in the system to identify people. All Australian residents and visa holders are connected to this service, and there is no way to remove identity documents from the system.

Although this service provides an easy way to rectify identity theft, the scale to which privacy can be compromised by law enforcement services and the private sector is worrying. Like all large databases, this system is also susceptible to hacks. Those who work with this system should follow the principles of privacy by design, best practice security, data providers to maintain access controls, have data quality, identity resolution by users, protect legally assumed identities, and robust accountability[71].

Commonwealth Victims' Certificates. The Western Australian Government and the Commonwealth Attorney-General's Department have made provisions for victims of identity crimes to be granted an Identity Crime Certificate[72]. This certificate records the name of the victim and describes the nature of the theft. Australians can then use the

[70] IDMATCH 2020

[71] Council of Australian Governments 2017

[72] Government of Australia 2020

certificates to prove to credit issuers that they have been the victim of identity theft. This can make the process of rectifying identity theft easier. The individual will need to go to the Magistrate in person and prove their identity with documents. At times, this action can be recommended by the courts when a Commonwealth identity crime is proven.

Identity Recovery. iDcare is a not-for-profit that receives donations from private sector partners to provide advice on how to respond to data breaches, scams, identity theft and cybersecurity concerns[73]. iDcare provides support services for organizations and individuals. Individuals receive a tailored response plan given the circumstances, and a dedicated case manager to help individuals through the process. iDCare provides a base level service for free that helps victims repair the damage to their reputation, credit history, and identity information. They are one of the few not-for-profits that offer Identity & Cyber Security counsellors. Australia, in June 2019, transitioned the Australian Cybercrime Online Reporting Network (ACORN) to ReportCyber. ReportCyber is an online reporting tool that enables victims of identity theft to report to relevant federal, state, or law enforcement agency who will then review. There are a variety of methods available online to citizens to report and track and receive help on how to correct the impacts of identity theft and related crimes.

Credit Monitoring Services. Other than iDCare, private companies like the credit bureaus that operate in Australia offer credit monitoring services that provide insurance when there is identity theft. Experian offers this service for as low as AU$5 a month up to AU$15 a month and can monitor some personal information as well as provide identity theft insurance[74]. Along with this, Experian and other credit bureaus offer a credit report ban that will prevent creditors from access to the credit report for a credit check. The Credit Report Ban is like a credit freeze; however, the length of the ban is 21 days, and it can be extended.

[73] IDCARE 2019

[74] Equifax AU 2020

4.5. Summary of Case-Study Analysis

Figure 3: Summary of Case-Study Analysis

	Canada	United Kingdom	United States	Australia
Database Breach Scale and Impact	- Voluntary baseline cybersecurity standards - Has database breach notification requirements, -Fines will not exceed $100,000	-The fines up to 4% of global revenues. -Increased reporting of database breaches and have helped the collection of better data. -A minimum level of cybersecurity	-New York state specifies that it requires reasonable security for personal information and specifies measures to meet that standard. -In California, Americans must sue for compensation	-National Identity Security Strategy framework. -Australia has initiatives where database breaches need to be reported, and there can be financial penalties for remediation.
Database Breach Initiatives	-No mandated post-breach supports. -It is up to the individual to seek reprisal in court.	-Private organizations offer Custom ID protection and repair responses to those impacted by a breach. -The government suggests post-breach supports. -It is up to the individual to seek reprisal in court.	-New York and California have in law what would need to be proven to claim damages. -In California, victims would need to prove the company does not have enough cybersecurity practices.	-No requirement for post-breach supports of victims. -No incentive to provide these supports
Identity Theft Impact Reduction Initiatives	-Between 2017 and 2018 there was a 12% increase. -Financial losses accounted for 21.2 million dollars in 2018. -Victims responsible for reporting and contacting identity crime - Credit monitoring and fraud alert services.	174,000 incidents in 2017 and 189,000 incidents in 2018 -The government-run online portal to report and manage identity crime for victims. -One-stop-shop to report and manage identity crime. -Protective registration which is an alternative to credit monitoring provides loss prevention supports so credit issuers can ads	-344,000 incidents of identity theft in 2017. Of the 344,000 incidents, the most common type of fraud was a credit card fraud. -A government-run online reporting portal will walk the individual through recovery steps, update plans, and pre-fill forms to submit to credit issuers. - Credit freezes to ensure that their credit cannot be accessed at all. -Fraud alerts and credit monitoring services.	Identity-related crime has impacted 1 in 4 Australian citizens -National Identity Security Strategy -Identity Matching Database that captures biometric data, government-issued identity documents to verify the validity of documents -Commonwealth Victims' Certificates obtain a certificate to prove identity -IDCARE, a not for profit, offers a free service that repairs damage to reputation, credit history, and identity information. -Cheap credit monitoring services

Chapter 5.

Interview Findings

In this section, there is a discussion on the key findings of 4 semi-structured interviews. There were two key topics discussed which include both cybersecurity and identity theft. These conversations brought out some key themes which include the idea that breaches are inevitable, the cost of doing business, compliance, information from a database breach, and protecting victims.

5.1. Database Breach Prevention

5.1.1. The Inevitability of a Breach

Database breaches are inevitable. An interviewee stated breaches will always happen and hackers will innovate and find novel ways to hack into systems. Canada can adopt policies meant to prevent the incidences of database breaches; however, hackers will adapt, and they will find a way to breach databases. The solution to this issue has had mixed opinions from experts. Interviewees believe that all Canada can do now is focus on rapid response, breach detection, and containing a breach. Others say Canada needs to implement a baseline cybersecurity policy in the event of a breach. When baseline cybersecurity policies are implemented the stolen data cannot be easily used.

5.1.2. Cost of Doing Business

Some interviewees expressed concerns about how large companies do not take the proper precautions to prevent a database breach. This concern comes from the belief that the benefits of being reactive outweigh the costs of being proactive. For individuals, this would mean their personal information would be at risk in the event of a breach. The costs of a breach will be the “cost of doing business” as companies will see more value in responding to a breach than preventing a breach. An interviewee notes that “stakeholders aren’t too concerned about [major breaches], and they happen, so […] there is this idea that the market can take care of it.” There are almost no consequences for having a database breach occur since companies currently can have

policies that cover the damages caused by a breach. Other interviewees state that companies that are impacted by a database breach look to be proactive that “seeks to minimize accountability and downplay the impact on victims.” Many companies understand that action is necessary to improve security practices. However, as other interviewees pointed out, the correct incentives are not available. One interviewee mentions that a stronger regulator can provide this information and can guide businesses on a better path to stronger cybersecurity measures.

As of now, an interviewee mentions that “companies … [manage] the risk by buying insurance” so that the costs of fixing the issue are cheaper than preventing the issue. For example, policies such as larger fines, stronger regulators, or minimum cybersecurity standards do not have high compliance among companies.

5.1.3. Compliance

Some interviewees focus on compliance issues with large companies adopting stronger cybersecurity measures. An interviewee stated “the government has failed to create…the right incentives…for the private sector” suggesting that there is more the government can do to ensure compliance. One interviewee is a strong supporter of a strong regulator enforcing compliance. The interviewee states that as of now there is a “wrong balance between the big banks and the consumer” The interviewee is referring to how Canadians are not able to do much in the event of theft because of a “lack of effective regulation in Canada.” This interviewee advocates for stronger fines coupled with a strong regulator as a necessary component of having a real impact on the personal information leaked in database breaches.

5.2. Identity Theft and Victimization

5.2.1. Information Used in Identity Theft

One interviewee noted that identity theft is the “single most important challenge since it touches everything”. There are eight categories of personal information that can be used to commit identity fraud. One of the interviewees shared what they call a TRICK Matrix. The eight categories are personal information; private details; assigned unique identifiers; self-selected unique identifiers; financial details; location information;

biological identifiers; and behavioural and communications. Database breaches, which impacts companies of all kinds, expose this information to hackers. The more breaches there are, the more likely it is that one or more of the personal information categories are collected. This can be used by hackers to put together a profile of an individual to commit identity fraud.

After identity theft, interviewees note that “I [need] to prove who I am… that’s time, that’s effort, that’s a hassle, [and] that’s a headache.” This interviewee is exploring the idea that in the event of a breach, unlike other victims, the victims are responsible for dealing with the impacts of a breach. The fact that it is on the victims, means that there are financial, time, and mental health costs that are not rectified.

5.2.2. Corporate Responsibility

Companies do not take responsibility for identity theft that occurs after a database breach. One interviewee stated, “Look at the value of shares [after a database breach] the rule is that nothing happens.” This interview is bringing up the point that larger fines would potentially impact the bottom line of some companies which would spur action. Interviewees mentioned the Life Labs breach as the best example. Life Labs as far as the Canadian public knows did not do the basic cybersecurity protocol of encrypting their data. Up to 5 million people may have their medical information compromised. This information could be collected and sold and used to conduct fraud in the future. There is no recourse for victims other than a class-action lawsuit. However, the interviewees mentioned that settlement money mostly goes to lawyers. One interviewee mentions the solution of both a strong regulator and stronger fines. The company most of the time would know which individuals have their information compromised. Policies like credit freezes, cheap credit monitoring, and policies that prevent identity theft after a breach are all good and will be effective.

Chapter 6.

Summary of Findings

6.1. Database Breaches Initiatives

Legislation focused on data security and database breach prevention is strongest in the U.K due to the jurisdiction of the GDPR. The GDPR is a strong regulation with the highest limit for fines. Regulators can fine companies upward of 4% of their global revenues. In practice, for companies like British Airways, a minimum of 4% of global revenues can mean fines as large as $880 million for an incident. Interviewees suggested that the GDPR is a great first step for data protection, reducing the likelihood of a database breach, and consumer protections. California is entering this database breach prevention following the framework of the GDPR. The existing initiatives are new, their true impact is not yet felt. Through the GDPR large companies are being fined for putting personal information at risk and the government knows sooner if a breach occurs. As the interviewees mention, the biggest issue with policies that target companies is compliance, large companies have insurance policies ready to payout.

As of now, the GDPR has shown the effectiveness of breach notification regulations where companies are required to report a breach within 72 hours to the government and notify consumers without delay. Victims of database breaches do not have much offered to them. Interviewees noted that companies can provide credit monitoring to prevent identity theft and identity fraud out of goodwill or as a part of their insurance package. The U.S required individuals to sue the company and prove that the company had lax cybersecurity practices. This is not equitable due to the costs of the legal system and the onus placed on the victim of a breach. Australia has a comprehensive identity theft framework which includes measures for database breaches as a measure of risk. There is a gap in that database breaches will occur, and victims will be impacted. However, as the interviewees agreed that hackers will find new and innovative ways to breach a database, so reactionary measures are the most effective in preventing harm. One interviewee mentions all Canada can do is have minimum standards and take action to reduce the impacts after a breach occurs.

6.2. Identity Theft Reduction Initiatives

Australia is a leader in identity theft focused legislation. They created the National Identity Strategy and the National Identity Crime Measurement Framework where there are annual reports of the impact and scale of identity crime. Everything is measured and everything is reported. The concern with this framework in the Canadian setting is that this framework encroaches on facial recognition techniques that could be used by companies in the future. The National Identity Crime Measurement Framework is something that would be an impactful next step for Canada. The U.K has multiple pieces of legislation that cover the criminal aspect of identity theft. Legislatively there is not much in terms of prevention other than educational programs. The U.S does not have a broad policy or strategy to reduce identity theft other than existing legislation.

The U.K has a program called Action Fraud that is an online portal where users can report the incidence of identity theft online, and this information can result in an investigation. They also have something called protective registration. This is a free service that provides identity monitoring support and delays credit applications to ensure that there is not identity fraud occurring. This can give an alert to the individual if their credit is being used without their knowledge. The U.S has a comprehensive online reporting system which includes contact information required for major banks to report identity theft. This includes a plan for recovery in the event of a breach. Citizens also have access to a free credit freeze where they can put a hold on anyone who pulls their credit information. This could be useful in the event of a database breach to limit the immediate identity fraud that may happen within the year. Australians have other options including a Commonwealth Victims' Certificate, Identity Recovery Services, and Cheap Credit Monitoring Services. All these options can help rectify the damage from identity theft or reduce the risk of being the victim of identity fraud after a database breach.

Chapter 7.

Policy Objectives, Criteria, and Options

This paper aims to limit the loss of information through database breaches, limiting the number of identity-related crimes, and protecting victims of identity theft by providing options when a breach occurs. This section will draw from the information gained in the background, case study analysis, and interviews to propose potential policy options that will be evaluated using criteria and measures. A policy needs to address and limit the impact of identity-related crime from database breaches. The options will target the limiting of the loss of information through database breaches which will then impact the identity-related crime and protecting victims of identity theft by providing options.

7.1. Evaluation Criteria

The criteria are used to evaluate the policy options to see which of the options would best tackle the issue of database breaches, the identity theft that follows, and its impacts. The criteria include security/protection, efficiency, cost, compliance issues, and stakeholder acceptance. The key objective of the policy is to ensure that either there is less risk of being impacted by identity theft due to a database breach or that those impacted by identity theft have more options to ensure that their wellbeing is maximized after a theft. The other extremely important objective of any policy is compliance. As identified in the interviews, compliance on behalf of the large companies involved is the key issue. The criteria, definition, measure, and scale that will be used to evaluate policy options are described in Table 3. The scale for this is High, Medium, and Low. High represents significant positive impacts, Medium represents moderate impacts, and low represents little to no impact. Impacts are evaluated using information from the case study analysis and the interviews. Low means that there are little to no impacts from adopting the policy, Medium represents an anticipated moderate impact, while High represents an anticipated significant positive impact from adoption in Canada.

Table 3: Criteria and Measures

	Criteria	Definition	Measure	Criteria
Security/Protection	Impact of identity theft	Does this policy decrease the risk of a database breach?	A reduction of those impacted by identity-related crime annually High. There is a significant decrease in the risk of personal information being used for identity theft Medium. There is a moderate decrease in the risk of personal information being used for identity theft Low. There is little or no decrease in the risk of personal information being used for identity theft	High, Medium, Low
	Wellbeing of victims	How will this policy better either the outcomes or the rectification process for victims of identity theft?	Number of available options for those impacted by identity theft or the ease of rectifying identity theft High. There is a significant decreased in the risk of harm that could be caused to a victim of identity theft Medium. There is a moderate decrease in the risk of harm that could be caused to a victim of identity theft Low. There is little or no decrease in the risk of harm that could be caused to a victim of identity theft	High, Medium, Low
Compliance Issues	Number of actors who can follow and implement the policy requirements	The difficulty of all actors in complying with a policy?	Percentage of companies expected to follow the legislation easily High. There is a significant likeness that companies will comply with the policy Medium. There is a moderate likeness that companies will comply with the policy Low. There is little or no change in the likeness that companies will comply with the policy	High, Medium, Low

	Criteria	Definition	Measure	Criteria
Efficiency	Efficiency to the economy	Does this policy decrease the loss to society from identity theft?	Change in the loss in dollars due to the implementing of a specific policy High. There is a significant decrease in the losses to victims of identity theft and companies as a result of this policy Medium. There is a moderate decrease in the losses to victims of identity theft and companies as a result of this policy Low. There is little to no decrease in the losses to victims of identity theft and companies as a result of this policy	High, Medium, Low
Cost	Impact on the budget	How much does this policy cost the federal government to implement?	Cost in dollars to the government High. There is a little to no increase in the costs to the government with this policy option Medium. There is a moderate increase in the costs to the government with this policy option Low. There is a significant increase in costs to the government with this policy option	High, Medium, Low
Stakeholder Acceptance	Stakeholder support	How will this policy be accepted by the banks, credit bureaus, and other credit issuers?	Expected support/opposition High. There will be significant support among stakeholders Medium. There is moderate support among stakeholders Low. There is little to support among stakeholders	High, Medium, Low
		How will victims respond to this policy option?	Expected support/opposition High. There will be significant support among stakeholders Medium. There is moderate support among stakeholders Low. There is little to support among stakeholders	High, Medium, Low

7.1.1. Security/Protection

The key policy objective of any policy would be the protection and remediation options for victims of identity theft. Protecting Canadians from the risk of harm from their personal information being accessed by a third party is paramount. Security & Protection is the key policy objective so it will be weighted higher. Security and Protection is the primary policy objective for policies that can impact identity-related crime, which is that there are either fewer victims of identity theft in the future, and the damage is lessened as well. The scale for this will go from Low, Medium, and High. High represents significant positive impacts.

7.1.2. Compliance Issues

The policy needs to be followed by companies, and the companies should be easily able to comply with the requirements of the policy. As identified in the interviews, other than the primary objective which is to protect Canadians from being impacted by identity theft, having large companies complying with substantive policies is the greatest hurdle. Currently, in the E.U, many businesses are struggling to comply with the database breach prevention and reporting requirements. The database breach prevention methods are aimed at reducing the personal information available to third parties, which would impact the number of identity-related crime incidents. Database breach reporting requirements give consumers the ability to lock down and protect their credit. There should be mechanisms in place to examine how easy it would be for firms to comply.

7.1.3. Efficiency

There is a loss to the economy in both the damage to consumers and businesses from the impact of database breaches and the identity theft that can follow[75]. Efficiency means that the policy would decrease the loss to society. Database breaches and their impacts, in general, have large impacts on companies so mitigation policies are efficient[76]. As a part of the overall losses for the business, loss of customer trust is a

[75] IBM Security and Ponemon Institute 2019

[76] Ibid

large portion of the costs. This would consider the value proposition between investing in cybersecurity infrastructure and the costs of dealing with a database breach.

7.1.4. Cost

Cost by the government to implement any program or policy needs to be considered. There may be a preference such that the degree of investment by taxpayers should be proportionate to the scale of the issue. The measure for this criterion is the cost to the government from implementing a policy.

7.1.5. Stakeholder Acceptance

The stakeholders in this policy would be the credit bureaus, the banks, credit issuers, businesses, and any Canadian. Any change to the systems may impact their bottom line and may impede their business. Policy options would need to prevent or ameliorate harm businesses while protecting the Canadians that can be impacted by identity theft. The extent to which stakeholders believe that the policies implemented would have a real impact on this important issue and the extent to which industry players would be willing to accept changes in policy is considered to impact the scoring.

7.2. Policy Options

There are four policy options considered to address the impacts of database breaches. These options come from the literature, case studies, and interviews. The options are stronger regulator and fines, baseline cybersecurity standards, comprehensive identity theft reporting and data collection, and identity theft protection services. These options aim to reduce the impact of database breaches or protect the wellbeing of victims of identity theft the options to introduce a stronger regulator or baseline cybersecurity policies focus on the impact of database breaches. While the options of comprehensive database breach reporting and identity theft protection services focus on the victims of a database breach.

There are some policies I did not evaluate such as a full adoption of Australia’s framework due to privacy concerns. The scale of data collection in Australia includes the

privacy challenges of facial recognition. This would be incredibly difficult to implement and would not be welcomed by stakeholders.

7.2.1. Policy Option 1: Stronger Regulation, Fines, and Support

Policy option 1 is to implement regulations like the GDPR with a strong regulator, implement large fines, and provide compliance tools to companies. Regulations including the existing framework offered by the PIPEA would be expanded to be tougher on data security. The aim is to limit the data that would be compromised which will decrease the occurrence of identity theft. Canada can adopt policies similar to the GDPR including a stronger requirement where the firm needs to report a database breach within 72 hours of becoming aware of it to the government, while individuals need to be notified without undue delay if steps have not been already completed to limit significant harm, mandating stronger cybersecurity requirements, where the lack of enough data security is met with fines, and there are limits to the kinds of data that can be collected. Data regulators are the bodies that enforce these rules. The U.K and France have regulators that engage in similar functions. This regulator could have the ability to conduct studies like those conducted through Australia's Identity Theft Measurement Framework.

Under the PIPEDA companies can be charged anywhere from $10,000 – $100,000 for non-compliance. This policy would impose a larger fine on companies who both fail to report a database breach on a timely basis and companies who suffer a database breach due to weak cybersecurity measures. This policy option includes amending existing legislation to have similar teeth as the GDPR. These fines can mirror the 4% global revenue to ensure that the promotion of cybersecurity and data protection is more than the "cost of doing business." When introducing strong regulations interviewees state strongly that it should be followed with a strong regulator who has as its mandate the application of strong data protection regulations. One interviewee stated, "[Canada] need[s] a clear regulatory framework here that will obligate them to participate in such initiatives." This interviewee believes large corporations only take actions that will maximize profits and minimize costs. Database breaches are a common occurrence that does not impact their bottom line as much as it should because of the insurance which allows it to be cheaper to respond to a breach rather than prevent a breach.

Interviewees believe that if it is cheaper to be subject to a breach than to prevent it, companies will not act.

What is necessary for this strong regulator to consider is that it would need to provide the carrot to its stick. The government supports companies, with information and incidence response. When probed the interviewee suggested that the government should provide resources, knowledge, technical support, and information on what to do in the event of a breach especially for SMBs. Another interviewee states that “the federal privacy commissioner must get enforcement powers, the PIPEDA must be prescriptive about what companies need to do and by when” This role can be filled by a strong regulator who could be an empowered privacy commissioner.

7.2.2. Policy Option 2: Baseline Cybersecurity Standards

The PIPEDA does ask that companies adopt cybersecurity policies. However, these policies are not defined. Mandating baseline cybersecurity standards would introduce some baseline cybersecurity standards for companies. Baseline cybersecurity standards can begin from existing government recommendations[77]. For example, baseline policies should include “encrypted identity data” where “every identity element from address to phone number needs to be properly encrypted.” Baseline cybersecurity standards would ensure that in the case of a breach, Canada can reduce the impact. Impacts will be reduced because personal information will be harder to use due to encryption. Also, interviewees noted that baseline cybersecurity standards should include the creation of breach detection and response plans that should be mandatory. As of now, Canada does provide a recommendation for a baseline cybersecurity standard for SMBs. These recommendations can be adopted by SMBs if they would like under the CyberSecure program. In this program, companies can be audited and can adopt internal policies as per recommendation to achieve an acceptable level of security. This can be expanded to cover the intricacies of large companies and can be added to existing legislation. Baseline cybersecurity standards would include a breach response plan to ensure that there are measures in place to limit the risk to personal information in the event of a breach.

[77] Canadian Centre for CyberSecurity 2019

This policy would be a useful first step in moving to stronger policies. Policy Option 1 would be a much stronger version of this option and could reasonably be the next step from this policy option. As of now, the Canadian government asks that companies take cybersecurity practices seriously but does not define what they should look like. Once companies can adapt to a baseline minimum, then these companies would have an easier time adopting strict standards since they would have the initial infrastructure in place.

7.2.3. Policy Option 3: Comprehensive Identity Theft Reporting and Data Collection

A policy to implement a comprehensive identity theft reporting and data collection includes an expansion of online reporting methods to a one-stop-shop style reporting system. As of now, Canadians need to contact their banks, both credit bureaus, the police, the Canadian Anti-Fraud Centre, and their credit card issuers. Although the Anti-Fraud Centre provides an online reporting tool, expanding that with personalized next steps will allow Canadians to know what to do next when struggling with the theft. This option is reactive. This option also includes the creation of documents and studies like Australia to capture the extent, scale, and usefulness of policies when identity theft is measured. Australia has seen much success and clarification about the scope of the issue.

The case studies show that the United States and the United Kingdom have a comprehensive online identity theft reporting system. The United States uses a website called identiytheft.gov. This website asks for information about the theft, sends this to the appropriate agencies, provides a recovery plan, and helps the victim put that plan into action. Canada does have an online reporting system that collects information for law enforcement but does not offer personalized support. This policy option would make it easier for those impacted by identity theft to report the theft and reduce the impact of said theft. This option does not limit the information being leaked in the first place, but it will reduce the potential damage so long as Canadians know it exists. On top of this, the reporting system will allow Canada to collect data useful in determining the size and scope of identify theft. Collecting this data would allow Canada to understand the scale of the impacts of a database breach, who is more likely to be impacted, and what remedies they can implement protect Canadians.

7.2.4. Policy Option 4: Identity Theft Protection Services

The case studies showed that there is a difference in available measures for victims of identity theft to limit the damage. Policy option 4 is to implement stronger identity theft protection services so that after a Canadian is notified of a breach, they can take the proper precautions. The United States has something called a credit freeze. With the new legislation, it is now free for Americans[78]. A freeze is offered by credit bureaus, and it stops credit issuers from accessing credit for as long as the freeze is in place. This can give the individual enough time to have their information in order and contact all firms that they interact with. The freeze can be taken off or temporarily unfrozen for a short time at any time and can last a few years. Australia's credit bureaus offer a credit ban, which is effectively a credit freeze that lasts 21 days and can be extended as deemed necessary. This allows individuals to protect their credit for as long as necessary so that when identity theft is noticed, individuals can act to limit the damage. Other than the United Kingdom, where there is a non-profit which offers credit monitoring at a low or no cost, other jurisdictions charge for credit monitoring and identity theft insurance. In Canada, paid credit monitoring services are offered for $19.95 on average. In comparison credit bureaus in Australia offer this service for as low as AU$5. This option focuses on empowering victims of database breaches by giving them the option to be proactive while preventing identity fraud.

During the interviews, several options for those impacted by a database breach and those impacted by identity theft from that information were considered. These options include identity theft protection, credit monitoring, credit freezes, and fraud alerts. All the interviewees admit that there is some positive impact of these services to victims of database breaches. Regarding credit monitoring or freezes they admit that this would need some sort of legislation or reputational pressure. Even if offered the impact of this would be low since, as one interviewee explains, "the bad guys can wait a year or two before they exploit." Especially when companies only offer one or two years of protection in the event of a breach.

[78] FTC Consumer Information 2018

Chapter 8.

Evaluation of Policy Options

Policies will be evaluated according to Table 4: Criteria and Measures and will be shown in Table 5: Policy Matrix. The scale for this is High, Medium, and Low. High represents significant positive impacts, Medium represents moderate impacts, and low represents little to no impact. In terms of weighting, the objective of security and protection is weighted higher than the other objectives.

8.1. Evaluation of Option 1: Stronger Regulation, Fines, and Support

When a database breach occurs, and personal information is compromised, identity thieves can commit identity-related crimes easier. This policy would not do too much to reduce the number of data breaches since as mentioned earlier breaches are difficult to stop. What it will do is reduce the impact of breaches and ensure that companies keep their internal cybersecurity levels at a high standard. This would add efficiency to the economy in that the amount of money lost by consumers and businesses when businesses are better able to protect their data. As mentioned earlier, the government has instituted breach notification requirements, which have brought costs to the firm but have allowed individuals to know that they need to act to secure their information. Stronger requirements can offset some breach notification and the costs of dealing with a database breach. The GDPR also mandates that reporting to the government needs to happen within 72 hours of a database breach. In terms of compliance issues, this would be difficult for some firms because many of the small firms may not have the systems in place. The policy would need to address this. The GDPR has large fines, for example, Marriott International was fined $170 million by the U.K for failing to undertake due diligence leading to a breach. This breach impacted 339 million records. These fines can be then used to fund government programs that could include data security or identity theft protection. The solution is related to its regulations and is tied to a strong regulator.

There are some caveats with adopting this policy option. The most important being the difficulty in enforcing this type of legislation due to the scale and impact this would have on all aspects of the economy.

Interviewees had different opinions on the impacts of the fines themselves. In general, interviewees believe that large fines can deter companies from being lax and can be used to ensure that companies strengthen their cybersecurity levels. As of now, interviewees identified that large companies have insurance policies that pay for the cost of dealing with a breach, giving consumers credit monitoring, and dealing with fines. The issue is that personally identifying information will still be leaked and can be used by other parties to commit identity theft. GDPR like fines would be high enough to ensure that the costs to businesses would be high enough to ensure companies are proactive with their cybersecurity. Some interviewees believe reputational impacts after a database breach would be enough to ensure that these companies will take better actions in the future. This expert believed that the risk of reputational damage is enough for them to change their behaviour. This option would be impactful, but difficult to implement in Canada successfully.

8.1.1. Security and Protection

This will have a great impact on the risk of being impacted by identity theft. There will be a reduction in those impacted by identity theft in the long term. As Cifas suggests, limiting data collection like the GDPR limits the risk of personal information being leaked. So long as the protections are rolled out in a way where small business and large companies can adapt. Although it is the case that small businesses will deal with the costs of bringing their cybersecurity levels to an adequate state, the impact on the security of personal data will increase. There will be a moderate impact on the wellbeing of victims in that it can better outcomes **(Medium)**. This policy aims to limit the risk of personal information being compromised in the first place. This will have no impact on victim outcomes or the rectification process. **(High)**

8.1.2. Compliance Issues

The GDPR has had a rocky adoption period. But both large companies and small businesses struggle to catch up to the legislation. The biggest hurdle is notifying the

government within 72 hours when a breach is discovered[79]. In general, almost half of the businesses say that their business is far from compliance or will never comply[80]. 27% of businesses say that they have not started the implementation phase as of 2019[81]There will be a negative impact on small businesses from a monetary perspective. From a business perspective that is a compliance issue. I expect similar challenges in Canada, especially because many of our businesses are SMBs. **(Low)**.

8.1.3. Efficiency

The GDPR has impacted the rate at which mergers and acquisitions occur due to compliance concerns and a large portion of businesses believe that the requirements impact innovation[82]. **(Low)**

8.1.4. Cost

This policy would need to creation of a regulator who can administer stronger GDPR like database protection requirements. This would inevitably come with the costs of dealing with this sort of policy. For example, the U.K's data regulator estimates that they would need a 70% increase in their budget to meet the demands of the GDPR[83]. In real terms in the 2017/2018 fiscal their budget was £24m in the 2018/2019 fiscal after the GDPR it needed to be £38m[84]. **(Low)**

8.1.5. Stakeholder Acceptance

Victims of identity theft from database breaches would likely support this policy **(High)**. In the event of a breach, caused by negligence then the companies involved would have to pay a fine. Companies would not like this at all, as it would create an administrative burden to meet data protection policies. **(Low)**

---

[79] Chivot and Castro 2019

[80] Ibid

[81] OPC blogger 2019

[82] Chivot and Castro 2019

[83] Information Commissioner's Office 2017

[84] Ashford 2018

8.2. Evaluation of Option 2: Baseline Cybersecurity Standards

This policy option entails a strengthening of the PIPEDA to increase and set minimum requirements for data security and the prevention of database breaches. The PIPEDA outlines that measures appropriate to the data contained in the database and that companies need to protect this information. However, there is no outlining of necessary safeguards. This is the case while the federal government engages in a program CyberSecure, which targets small businesses to strengthen their data protection to a minimum level that they have decided upon already.

There is some debate on what baseline cybersecurity policies would entail. The GDPR has regulations that can be adopted into what the baseline standards could look like. This includes pseudonymization, encryption of personal data, the ability to ensure confidentiality. Pseudonymization refers to the de-identification of some data in a database. Interviewees mentioned encryption where personal information could be hidden in a string of characters. These could be some baseline measures that could be implemented after more research. In terms of baseline standards, there was a mix in the interviews. One interviewee was pessimistic about minimum standards for cybersecurity in large companies stating, “standards are a business opportunity for companies.” Meaning that the topic of standards is used more so that consultants can come in and make money. Another interviewee mentioned that the idea of minimum standards is not something that would be useful because hackers figure out new and innovative ways of breaking into databases regularly. What this would mean is that whatever standards are implemented would eventually become useless as hackers find their way around them.

8.2.1. Security and Protection

Baseline cybersecurity standards would reduce the impact of database breaches on SMBs, but it would also ensure that large companies do not put a lot of consumer data at risk at one time. It would decrease slightly the impact of easy database breaches and reduce the risk of personal information being compromised **(Medium).** This policy does not target the impact on the wellbeing of victims **(Low)**. The target is the protection of compromised personal information that can reduce the chance of identity theft occurring.

8.2.2. Compliance Issues

In terms of compliance, there an existing recommendation called “CyberSecure Canada,” where there is an accreditation process where companies are encouraged to enhance their cybersecurity processes, after which they will be evaluated and given a certification if firms so choose to participate. With the CyberSecure program, there needs to be some sort of transfer to ensure that small businesses can add baseline policies if it is legislated. Large companies will have an easier time adopting and complying with the policy. **(Medium)**

8.2.3. Efficiency

Since the overall costs to businesses will be less than the GDPR style of strong regulations, there would be an increase in the efficiency of the economy due to saved dollars in dealing with a breach and the saved dollars in the reduction of identity theft. The impact on efficiency is moderate. **(Medium)**

8.2.4. Cost

There will be an impact on the budget since, to promote compliance, the government may need to provide financial supports. **(Medium)**

8.2.5. Stakeholder Acceptance

Stakeholders such as the banks, credit bureaus, and credit issuers deal with identity fraud and theft regularly, and it is difficult for these credit issuers to deal with the impacts of identity theft. Larger companies are implementing cybersecurity protections **(Medium)**. The acceptance by the public to this policy will be positive, but some may believe that this does not go far enough. **(Medium)**

8.3. Evaluation of Option 3: Comprehensive Identity Theft Reporting and Data Collection

Canada currently has implemented an online reporting system for identity theft. This reporting system does not contain information that can help individuals through the

process of dealing with identity theft. The implementation of a better and easily accessible reporting system would allow victims of identity theft to connect with the government. This reporting system does not assist individuals with contacting the other agencies. The FTC in the United States provides a reporting system that assists the user with all aspects of identity theft. The primary objective is security and protection, and better mechanisms to report identity theft would not decrease the number of people impacted by theft. To put this differently, it would be a better process for those impacted by identity theft. This would increase efficiency in the economy because quick reporting to government and all players can limit the damage to financial wellbeing. There will be the cost to the government, insofar that they need to build a better and user-friendly system that can be managed easily like the FTC's reporting system in the U.S. There needs to be an effort in rebranding the system and having it appear more often in online searches. Compliance issues would arise regarding how easily the website can connect to the most prominent players in identity theft, which are the credit bureaus in Canada: Equifax and TransUnion. This policy would be accepted and supported by stakeholders. The benefits of these policies result in more people being able to report and manage the process of identity recovery.

8.3.1. Security and Protection

This policy will not decrease the risk of personal information being used for identity theft **(Low)**. What this policy will do is provide options for Canadians to better the outcomes and promote the rectification process in the event of a theft. The options for victims are moderate. There will not be a significant change, but it will provide some guidance to victims so that they do not need to deal with the impacts without much help. A roadmap with the tools necessary to contact everyone that needs to be contacted will help victims. **(Medium)**

8.3.2. Compliance Issues

This policy does not need compliance as it will not impact companies other than having easily accessible channels that the government can link to. **(High)**

8.3.3. Efficiency

This option would limit the costs of identity theft because it allows quicker reporting to the authorities and helps Canadians secure their accounts. **(Medium)**

8.3.4. Cost

There will be a moderate cost to the government in the development, testing, implementation, and promotion of this website **(Medium)**.

8.3.5. Stakeholder Acceptance

Stakeholder acceptance for large companies will be high. There is no direct impact on them. Participation in an initiative to reduce identity theft impact protects large companies such as banks **(High)**. There will be support among the victims of identity theft. They will not feel as if the government is not doing as much as it can to help them through the process of rectifying the theft **(High).**

8.4. Evaluation of Option 4: Identity Theft Protection Services

The case studies showed that there is a difference in available measures for victims of identity theft to limit the damage. The United States has something called a credit freeze. With the new legislation, it is now free for Americans. A freeze is offered by credit bureaus, and it stops credit issuers from accessing credit for as long as the freeze is in place. This can give the individual enough time to have their information in order and contact all firms that they interact with. The freeze can be taken off or temporarily unfrozen for a short time at any time and will last a few years. Australia's credit bureaus offer a credit ban, which is effectively a credit freeze that lasts 21 days and can be extended. This allows individuals to protect their credit for as long as necessary so that when identity theft is noticed, individuals can act to limit the damage. Other than the United Kingdom, where there is a non-profit which offers credit monitoring at a low or no cost, other jurisdictions charge for credit monitoring and identity theft insurance. However, compared to Canada, where each credit bureau charges $19.95 for credit monitoring. Bureaus in Australia offer this service for as low as AU$5.

During the interviews, several options for those impacted by a database breach and those impacted by identity theft from that information were considered. These options include identity theft protection, credit monitoring, credit freezes, and fraud alerts. All the interviewees admit that there is some positive impact on victims of database breaches if they receive this from the company who have had their information accessed by a third party. Regarding credit monitoring or freezes they admit that this would need some sort of legislation or reputational pressure. Even if offered the impact of this would be low since, as one interviewee explains, “the bad guys can wait a year or two before they exploit.” Especially when companies only offer one or two years of protection in the event of a breach.

8.4.1. Security and Protection

There will be a moderate direct impact on the number of those impacted by a database breach or identity theft. It will provide options to victims of database breaches to proactively protect and monitor their credit history **(Low)**. There will be significant outcomes for victims or the rectification process of identity theft than the current system. **(High)**

8.4.2. Compliance Issues

There will be some compliance issues from companies including credit bureaus since they will be asked to provide services that they provide elsewhere for free or a reduced cost. **(Medium)**

8.4.3. Efficiency

This policy will have a moderate impact on the losses to victims of identity theft and companies. Usually, identity theft prevention measures are reactive. When notified about a breach, the individual can be proactive and place credit monitoring, a credit freeze, or similar initiative within the package. **(Medium)**

8.4.4. Cost

There can potentially be a cost to the government in how they would like to move with this policy. Either the government can legislate that the credit bureaus offer these options for free or the government can pay the credit bureaus to offer this service in Canada. **(Medium)**

8.4.5. Stakeholder Acceptance

This policy will have general acceptance by large companies since it would reduce the costs to companies in the event of a breach **(Medium)**. Victims of identity theft will support this policy as it provides more options for victims to reduce further fraud and have more information. **(High)**

Table 4: Policy Matrix

Criteria	Option 1: Stronger Regulation, Fines, and Support	Option 2: Baseline Cybersecurity Standards	Option 3: Identity Theft Reporting & Data Collection	Option 4: Identity Theft Protection Services
Security and Protection				
Impact of Database Breaches	High	Medium	Low	Medium
Wellbeing of Victims	Medium	Low	Medium	High
Compliance Issues				
Number of actors who can follow and implement the policy requirements	Low	Medium	High	Medium
Efficiency				
Efficiency to the Economy	Low	Medium	Medium	Medium
Cost				
Impact on the budget	Low	Medium	Medium	Medium
Stakeholder Acceptance				
Stakeholder Support of Large Companies	Low	Medium	High	Medium
Stakeholder support of the Public	High	Medium	Medium	High

Chapter 9.

Recommendation and Conclusion

The recommendation is based on how the policies rank on the scale from high; medium; and low scale and the overall objectives of this paper which is to mitigate the impact of database breaches on Canadians. The recommendation includes short-term and long-term policies to consider.

In the short term, the recommendation is to adopt and enforce baseline cybersecurity standards for all businesses with a focus on small business compliance and to adopt which is to pursue the adoption of identity theft protection services. In other words, adopt Option 2 and 4. In the short term, this policy does not have a significant impact on database breach consequences. However, baseline cybersecurity standards include a post-breach plan and other initiatives that are shown to reduce overall costs[85]. The adoption of baseline standards would need to be coupled with increasing the availability of identity theft protection services. The government would pursue include affordable credit monitoring, introducing credit freezes, and promoting non-profits who offer identity theft recovery options. The U.S and Australia have policies that work and can be adopted in Canada.

In the long term, the goal is to adopt Option 1 which is the stronger regulation, fines, and support which is a GDPR like solution. Option 1 is the best in terms of the overall objective of mitigating the impact of database breaches. However, the issue with this GDPR style option is feasibility and compliance issues. Small business in the E.U has seen losses from the introduction of strong policies since those businesses have difficulty meeting the needs of the regulation A solution that positively impacts compliance, efficiency, and the cost is to first implement the baseline cybersecurity measures on a mandatory basis. By bringing small businesses up to speed, it would be easier to avoid the issues seen in the U.K with compliance.

Option 3 was not selected because the reporting element occurs after identity theft and identity fraud has occurred. It would not have a great impact in the event of a

[85] IBM Security and Ponemon Institute 2019

breach and would not prevent the loss to victims more than the other options. However, the importance of data collection like Australia is not to be understated. Understanding the scale of the issue is an important step to determining what should be done to combat the issue.

This study has its limitations. First, this paper considers the opinion of four interviewees, more interviewees would be able to provide a better sense of the thinking around database breaches and identity theft. There is a lack of diverse opinions in the interviews as most of the interviewees were academics who work in the field of cybersecurity. Another limitation is the lack of data surrounding database breach mitigation policies and their efficacy. The jurisdictions in the case-study analysis have recently implemented these policies and it is difficult to gather information on the true impact.

Future research would benefit from more interviewees with different perspectives on the field of database breaches such as those who work in database breach response teams and potentially representatives from firms who deal with increasing the baseline cybersecurity standard in organizations. This would allow for a perspective on the policy options that could change the scoring and impact the recommendation.

This research aims to provide policy options that would be useful in addressing the issue of the impacts of database breaches. The primary impact considered is identity theft and the impacts on victims. The research has shown that there are few things policymakers can do to stop database breaches from occurring. What policymakers can do is address and limit the impacts of the breaches to being with. The options provided address with the issue from two fronts of both reducing the scale of personal information that could be leaked and helping victims of a breach by providing both preventative and post-identity theft options.

References

Action Fraud. 2020. “What Is Action Fraud?” 2020. https://www.actionfraud.police.uk/what-is-action-fraud.

Nadarajah, Murugan, Rob D’Ovidio, and Alexander Jenkins. 2013. “Safeguarding Consumers against Identity-Related Fraud: Examining Data Breach Notification Legislation through the Lens of Routine Activities Theory.” *International Data Privacy Law* 3 (1): 51–60. https://doi.org/10.1093/idpl/ips035.

Abedi, Maham. 2019. *LifeLabs hack: What Canadians need to know about the health data breach | Globalnews.ca.* https://globalnews.ca/news/6311853/lifelabs-data-hack-what-to-know/.

Ashford, Warwick. 2018. “Good Time to Be in Data Protection, Says Information Commissioner.” Computerweekly.Com. 2018. https://www.computerweekly.com/news/252439274/Good-time-to-be-in-data-protection-says-information-commissioner.

Borzykowski, Bryan. 2019. “4 Things You Need to Know about Identity Theft Right Now.” Chartered Professional Accountants of Canada. 2019. https://www.cpacanada.ca/en/news/canada/2019-03-14-identity-theft-101.

Canadian Anti-Fraud Centre. 2014. “Annual Statistical Report.” 2014. https://www.antifraudcentre-centreantifraude.ca/reports-rapports/2014/ann-ann-eng.htm.

Canadian Centre for CyberSecurity. 2019. “BASELINE CYBER SECURITY CONTROLS FOR SMALL AND MEDIUM ORGANIZATIONS V1.1.”

Canadian Internet Policy and Public Interest Clinic. 2007a. “Identity Theft: Introduction and Background.” https://cippic.ca/sites/default/files/bulletins/Introduction.pdf.

———. 2007b. “Techniques of Identity Theft.” No.2. ID Theft Series. Ottawa.

CBC News. 2019. “Equifax to Pay up to $700M in U.S. to Settle Data Breach, but Canada Is Not Included | CBC News,” 2019. https://www.cbc.ca/news/business/equifax-fine-1.5219957.

Chivot, Eline, and Daniel Castro. 2019. “What the Evidence Shows About the Impact of the GDPR After One Year – Center for Data Innovation.” Center for Data Innovation. 2019. https://www.datainnovation.org/2019/06/what-the-evidence-shows-about-the-impact-of-the-gdpr-after-one-year/.

Ciccio, Francesco di. 2014. “Comparison of Identity Theft in Different Countries.”

Cifas. 2020. “Fraud Prevention | Identity Fraud | Protective Registration | Cifas.” 2020. https://www.cifas.org.uk/.

Commonwealth of Australia. 2014. “Identity Crime and Misuse in Australia: Key Findings from the National Identity Crime and Misuse Measurement Framework Pilot.” www.itsanhonour.gov.au.

Council of Australian Governments. 2017. “INTERGOVERNMENTAL AGREEMENT ON IDENTITY MATCHING SERVICES.”

Desjardins. 2019. “Privacy Breach - An Update on the Police Investigation.” 2019. https://blogues.desjardins.com/press_release/2019/11/privacy-breach---an-update-on-the-police-investigation.php.

District m. 2018. “GDPR Data Protection Framework.”

DLA Piper. 2019. “DATA PROTECTION LAWS OF THE WORLD - National Data Protection Authority in France.” 2019. https://www.dlapiperdataprotection.com/index.html?t=authority&c=FR.

Dusseault, Pierre-Luc. 2015. “THE GROWING PROBLEM OF IDENTITY THEFT AND ITS ECONOMIC AND SOCIAL IMPACT.”

Equifax AU. 2020. “Credit Reports, Credit Scores, Credit Alerts.” 2020. https://www.equifax.com.au/personal/products/credit-and-identity-products.

Equifax Australia. 2019. “Data Breach Solutions.” 2019. https://www.equifax.com.au/business-enterprise/data-breach-solutions.

European Commission. 2019. “GDPR in Numbers.” https://ec.europa.eu/commission/sites/beta-political/files/190125_gdpr_infographics_v4.pdf?utm_medium=social&utm_source=linkedin&utm_campaign=postfity&utm_content=postfity05e1e.

FTC Consumer Information. 2018. “Free Credit Freezes Are Here.” 2018. https://www.consumer.ftc.gov/blog/2018/09/free-credit-freezes-are-here.

“General Data Protection Regulation (GDPR) – Official Legal Text.” 2019. 2019. https://gdpr-info.eu/.

Goldsmid, Susan, Alexandra Gannoni, and Russell G Smith. 2017. “Identity Crime and Misuse in Australia: Results of the 2017 Online Survey | Australian Institute of Criminology.” https://aic.gov.au/publications/sr/sr11.

Golladay, Katelyn, and Kristy Holtfreter. 2017. “The Consequences of Identity Theft Victimization: An Examination of Emotional and Physical Health Outcomes.” *Victims and Offenders* 12 (5): 741–60. https://doi.org/10.1080/15564886.2016.1177766.

Government of Australia. 2020. “Criminal Justice - Cybercrime and Identity Security.” 2020. https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime-identity-security/identity-security.

Government of British Columbia. 2020. “Personal Information Protection Act.” 2020. http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01.

IBM Security, and Ponemon Institute. 2019. “Cost of a Data Breach Report 2019.”

IDCARE. 2019. “About IDCARE.” 2019. https://www.idcare.org/about-idcare/what-is-idcare.

Identity Theft Resource Center. 2018. “2017 Data Breaches.” 2018. https://www.idtheftcenter.org/2017-data-breaches/.

Identity Theft Resource Centre. 2018. “AFTERMATH ®.”

IDMATCH. 2020. “Identity Matching Services Frequently Asked Questions.” Government of Australia. 2020. https://beta.idmatch.gov.au/faqs.

Information Commissioner’s Office. 2017. “Information Commissioner’s Annual Report and Financial Statements.”

Ligaya, Arminia. 2017. “Identity-Theft Protection Services Largely Not Worth the Fees, Experts Say - The Globe and Mail.” *The Globe and Mail*, 2017. https://www.theglobeandmail.com/globe-investor/personal-finance/household-finances/identity-theft-protection-services-largely-not-worth-the-fees-experts-say/article36504226/.

McNicholas, Edward, and Kevin Angle. 2020. “USA: Cybersecurity.” https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa.

“New York SHIELD Act: The Latest Amendment to NY State’s Cybersecurity Law.” 2019. Hashed Out by The SSL Store™. 2019. https://www.thesslstore.com/blog/new-york-shield-act-the-latest-amendment-to-ny-states-cybersecurity-law/.

Northcott, Melissa. 2012. “Identity-Related Crime: What Is It And How It Impacts Victims.” https://www.justice.gc.ca/eng/rp-pr/cj-jp/victim/rd5-rr5/index.html.

Northcott, Mellisa. 2018. “Identity-Related Crime: What It Is and How It Impacts Victims.” *Victims of Crime Research Digest*, no. 5. https://www.justice.gc.ca/eng/rp-pr/cj-jp/victim/rd5-rr5/p3.html#fn1.

Office of the Privacy Commissioner of Canada. 2020. “The Personal Information Protection and Electronic Documents Act (PIPEDA).” 2020. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/.

OPC blogger. 2019. “A Full Year of Mandatory Data Breach Reporting: What We’ve Learned and What Businesses Need to Know - Office of the Privacy Commissioner of Canada.” 2019. https://www.priv.gc.ca/en/blog/20191031/.

Richardson, Vernon J., Rodney E. Smith, and Marcia Weidenmier Watson. 2019. "Much ado about nothing: The (lack of) economic impact of data privacy breaches." *Journal of Information Systems* (American Accounting Association) 33 (3): 227-265.

Roberds, William, and Stacey L. Schreft. 2009. “Data Breaches and Identity Theft - Simon Fraser University.” 2009. https://sfu-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?adaptor=primo_central_multiple_fe&context=PC&docid=TN_crossref10.1016%2Fj.jmoneco.2009.09.003&facet=rtype,exact,articles&query=any,contains,database%20breaches%20and%20identity%20theft&search_scope=default_scope&tab=default_tab&vid=SFUL.

Schwartz, Mathew J. 2019. “GDPR: Europe Counts 65,000 Data Breach Notifications So Far.” Bankinfosecurity.Com. 2019. https://www.bankinfosecurity.com/gdpr-europe-counts-65000-data-breach-notifications-so-far-a-12489.

Shah, Maryam. 2019. “More than 28 Million Canadians Impacted by a Data Breach in Past 12 Months: Privacy Watchdog - National | Globalnews.Ca.” *Global News*, 2019. https://globalnews.ca/news/6116444/canadians-affected-by-data-breach-privacy-commissioner/.

Soloman, Howard. 2019. “Federal Government Launches Cybersecurity Certification Program for SMBs.” IT World Canada News. 2019. https://www.itworldcanada.com/article/federal-government-launches-cybersecurity-certification-program-for-smbs/420823.

State of California - Department of Justice - Office of the Attorney General. 2019. “California Consumer Privacy Act (CCPA).” 2019. https://oag.ca.gov/privacy/ccpa.

Statistics Canada. 2018. “Table 35-10-0177-01 Incident-Based Crime Statistics, by Detailed Violations, Canada, Provinces, Territories and Census Metropolitan Areas.” https://doi.org/https://doi.org/10.25318/3510017701-eng.

2019. “Police-Reported Crime Statistics in Canada, 2018.” 2019. https://www150.statcan.gc.ca/n1/pub/85-002-x/2019001/article/00013-eng.htm.

Tatham, Matt. 2018. “Identity Theft Statistics.” *Experian*. https://www.experian.com/blogs/ask-experian/identity-theft-statistics/.

Verizon. 2019. “2019 Data Breach Investigations Report.” http://veriscommunity.net/veris_webapp_min.html.

VictimsInfo. 2019. “Fraud and Identity Theft.” 2019. https://www.victimsinfo.ca/en/services/fraud-and-identity-theft.

Appendix A.

Canadian Policies

PIPEDA and Canada

The PIPEDA has pillars that underline this policy including accountability; identifying purposes; consent; limiting collection; limiting use, disclosure, and retention; accuracy; safeguards; openness; individual access; challenging compliance.

Accountability refers to the responsibilities of the businesses to follow the ten principles for companies to appoint someone to be responsible for the compliance, to protect all personal information held by the organization, and to develop and implement personal information policies and practices. Identifying Purposes refers to the responsibility of companies to identify and document your purposes for collecting personal information, tell customers why the information is needed at the time of collection, and to reaffirm consent if the purpose of the information changes. Consent refers to the procuring of meaningful consent when information is collected, and consent can be withdrawn at any time. Limiting collection refers to the responsibility on the part of the organization to explain the legitimate purpose of collection. Limiting use, disclosure, and retention refers to the fact that the organization may use or disclose personal information only for the identified purpose, the organization needs to know what personal information they have and what they are doing with it and obtain consent again if personal information is used for a new purpose. Accuracy refers to the responsibility of the organization or minimizes the possibility of using incorrect information when deciding about an individual or disclosing information to third parties.

Safeguards refer to a responsibility to protect all personal information appropriately and to protect against loss, theft, or any unauthorized access, disclosure, copying, use or modification. The PIPEDA does not offer particular security safeguards that must be used. The PIPEDA recommends that companies implement a security policy to protect personal information, including physical measures, up-to-date technological tools, and organizational controls.

Openness refers to the responsibility of companies to inform customers and employees that there are policies and practices for managing personal information and that these policies are easily understandable and available. Individual Access refers to the responsibilities of companies when asked to provide personal information about a person the company hold, including how that information was obtained. This would be done at a low or no cost. Challenging compliance refers to the responsibility of the organization to develop a single complaint handling and investigation procedure, to tell complainants about avenues of recourse, investigate all complaints, and improve any information-handling practice.

British Columbia

British Columbia currently has legislation called the *Personal Information Protection Act*[86] (PIPA), which exempts most organizations in BC from the PIPEDA. PIPA covers all private sector organizations that include people, corporations, partnerships, unincorporated associations, trade unions, trusts, and not-for-profit organizations. This is different from the PIPEDA slightly since the PIPEDA does not generally apply to not-for-profit, charity groups, political parties, and associations. PIPA requires organizations to obtain consent for the collection and use of information, be transparent about how this information will be used and can destroy or make anonymous personal information that the organization no longer needs.

Organizations are not allowed to refuse to supply you with a product or a service if you do not consent to the collection, use, or disclosure of personal information, and it does not allow the use or disclosure of your information for any purpose other than for what you have consented to. Consent is not necessary when the personal information is publicly available, when the collection benefits you, or when information is needed for an investigation. Issues with companies would be addressed with the company first and then the Office of the Information and Privacy Commissioner of B.C.

[86] Government of British Columbia 2020

Appendix B.

National Identity Crime Measurement Framework

Australia's National Identity Crime Measurement Framework is a comprehensive view of identity crime that needs constant review and studies to understand how the landscape changes. There are five components.

The first component is the acquisition of fraudulent identities. This has two indicators: one the price of the fraudulent identity credentials and the number of reported data breaches. The second component is the use of fraudulent identities which has indicators that include the number of identity crime and misuse incidents recorded, the number of prosecutions for identity crime offences, the number of people who self-report being victims, the number of people who perceive identity crime as a problem, and the types of personal information that may be more susceptible to identity theft. The third component is the consequences of identity crime, which has indicators that include direct costs of identity crime on government agencies, the direct costs of identity crime and misuse to business, direct financial losses to victims of identity crime and misuse the number of identity crime victims experiencing other non-financial consequences. The fourth component is the remediation of identity crime, the average time spent by a victim in recovering their identity, the number of inquiries to government agencies about recovering identity information, the number of applications for Victims' Certificates issued by the court. The fifth and final component of the framework is the prevention of identity crime, the indicators for this are connected to the identity verification processes which were introduced along with this framework, such as the Document Verification Service (DVS) and online security practices. The DVS captures the number of identity credentials verified by the DVS, the number of government agencies using the DVS, the number of private sector organizations using the DVS, and the number of DVS transactions.

In terms of online security practices, the Australian Government identified the proportion of individuals, businesses and government that adopt robust online security practices to protect personal information as an indicator that would limit the scale of identity theft.

Appendix C.

Interview Procedure and Participants

The interviews were semi-structured. Consent forms were received before the interviews began. Below are the questions that used information from the Case-Study analysis. Three interviews were conducted over the phone and one in person.

STAGE 1: INTRODUCTION

- Welcome, and thank you for taking the time out of your day for this interview
- Review the Purpose of the Interview
    - The purpose of the interview is to seek your perspectives on database breach and identity-related crime. Specifically, the aim is to gain perspectives on suggestions on what actions the government can take to reduce the impact of identity theft and identity-related crime.
    - Information obtained will be used to develop new policies for addressing challenges related to database breaches and identity theft.
- Interview Process
    - The interview will take around 30 – 45 minutes
    - The consent form I passed earlier outlines the ethical consideration, however, I will repeat it again
    - Participation in this research project is voluntary. You have the right not to participate in this study. If you decide to participate, you may choose to withdraw from the study at any time without consequences.
    - Your confidentiality will be respected. I will not release any information that discloses your identity without your consent.
    - I would like to record this conversation. It helps the quality of the analysis. If you consent to the recording of your voice, audio recordings will be destroyed after being transcribed
- Guidelines
    - Speak from your perspective
    - There are no right or wrong answers
    - Want your views; my opinions do not count.
- Do you have any questions before we begin?

STAGE 2: OPENING QUESTIONS

1. Starting more generally, what is your role in the field of identity theft, identity-related crime, or database breaches?
    a. Probe: How has your role changed with the landscape of database breaches and cybersecurity?
    b. (Expected Answer: They are an expert.)
2. What does the landscape of identity theft, identity-related crime, and database breaches look like in Canada?

STAGE 3: CORE

Identity Theft

3. Is the Canadian government doing enough to meet the issue of identity theft and identity-related crime in Canada?
    a. PROBE: What are some of the things the government of Canada can do about consumer protections, data, small business, banks, and credit bureaus
4. Is there something more that can be done by companies (large and small), banks, and the credit bureaus about identity-related crime.

Database Breaches

Government

5. Is there something that can be done by the government to motivate private companies to enhance their data protection?
    a. PROBE: Should legislation have stronger teeth with higher fines or requirements?
6. What are some challenges unique to Canada when considering options to combat identity theft from the database breaches?
    a. PROBE: How would the PIPEDA need to change to meet those challenges?

Companies

7. With what you know about massive database breaches, examples being Equifax, Capital One, Doordash, Lifelabs, is the government of Canada doing enough?

    a. PROBE: How are the impacted companies reacting?
8. What can be done by the government to protect those impacted by a database breach?
    a. PROBE: Should the government have stricter fines for not reporting it fast enough?
9. What do you think of standardized security practices and how can they prevent database breaches?
    a. PROBE: How can small businesses implement these practices?
    b. PROBE: Should companies who suffer database breaches from a lack of sufficient data protections offer some sort of compensation in the form of Credit Monitoring to those impacted?
10. With the new CyberSecure program for small businesses, should Canada bring those cybersecurity requirements to be mandatory or provide support for businesses for the level of security?
    a. PROBE: Which focus would be feasible considering the nature of database breaches?
    b. PROBE: Would this limit the number of database breaches?

Victims of Identity Theft

11. How easy is it for a victim of identity theft to report and recover from identity theft?
    a. PROBE: Is there something that can be done by Canada, or should we leave a private company to figure it out?
12. Other countries have credit freezes or cheaper credit monitoring services. Where do you see room for growth policy-wise to combat the prevalence of identity theft?
    a. PROBE: Who should be responsible for taking on this task

Potential Policy Options

13. What would happen if the Canadian government decided that everything that they are doing now, with the PIPEDA, and similar legislation is enough and did not act on it?
14. So, the GDPR, implemented in the E.U, is one of the strongest pieces of legislation on data protection and cybersecurity. Would adopting some of their protections impact either the incidence of data breaches or the impact of database breaches.
    a. The GDPR has fines up to 4% of global revenues. How difficult would it be to implement something like that in Canada?

15. The U.S has credit card freezes and a comprehensive online reporting system, which includes supports to contact banks and other initiations. How effective would something like that be for Canada?
16. In Australia and the E.U companies are required to report database breaches with legislation. But, the number of breaches keeps rising. What can be done to either decrease the number of breaches or the number of identities stolen because of that information?

STAGE 4: CONCLUSION

17. Is there anything you'd want to add about any of the topics we've discussed?

Appendix D.

Information Letter to Interviewees

SFU SIMON FRASER UNIVERSITY

Dear _____,

My name is Dennis Anthonipillai, and I am a Master of Public Policy Student from Simon Fraser University leading an independent research project on Identity Theft and Database breaches.

I am hoping to schedule a phone or in-person interview with you to discuss your expertise with respect to identity theft and database breaches. I would like to hear your opinions and to hear suggestions on what actions the government can take to reduce the impact of identity theft, identity-related crime, and database breaches. All responses will be kept confidential.

I am hoping to hold the interviews in December and January. Please let me know if you are available and would be interested in speaking with me.

Thank you very much for your time and consideration,

Appendix E.

Interview Consent Form

SFU SIMON FRASER UNIVERSITY

Protecting Canadians and Ameliorating the Impact of Identity Theft and Identity- Related Crime from Information Obtained from Database Breaches on Companies

Purpose of the study
The purpose of this thesis is to understand and recommend potential policy options for the government to boost identity theft protection and recovery for those impacted by identity theft in Canada.

Who is conducting the study?
Please note that this is an independent project led by Dennis Anthonipillai, a SFU Masters of Public Policy (MPP) student. The project is an educational exercise and students are not financially compensated. The information collected in this research will be published in the SFU Library and will be publicly available.

Principal Investigator:
Dennis Anthonipillai

Faculty Supervisor
Maureen Maloney

Why are you beings asked to take part in this study?
You are invited to take part in this thesis research because of your knowledge and expertise regarding cybersecurity or policies about identity theft and fraud.

Your participation is voluntary
Participation in this research project is voluntary. You have the right not to participate in this study. If you decide to participate, you may choose to withdraw from the study at any time without consequences.

What kind of information is being sought during the interview?
I will ask you 10-20 questions either in person or over the phone about your views on identity theft, Canadian banks, Canadians credit bureaus, and policies. This process is estimated to at most one hour of your time. I will be recording the interview audio with your consent

Could this study present risks to you?
I do not believe that this study will pose any physical or psychological risks to participants.

What are the benefits of participating?
I do not believe that participation in this study will provide any material benefits to participants.

Will you be paid for your time?
Participation in this study will not be remunerated.

How will your confidentiality be maintained?
Your confidentiality will be respected. The principal researcher will not release any information that discloses your identity without your consent. However, Telephone and email are not secure means of communication; therefore, confidentiality cannot be guaranteed. Audio recordings will be destroyed after being transcribed. Transcripts and all other data will be stored in SFU Vault on Canadian Servers and the researchers' password-protected laptop computer. Transcript data will be coded so that direct identifiers are removed from the materials and replaced with a code. Depending on the access to the code, it may be possible to re-identify specific individuals. However, the principal investigator retains a key that links the coded material with a specific individual if re-linkage is necessary within the three-year timeframe. All data will be permanently erased after three years.

What if I decide to withdraw my consent to participate?
You may withdraw from this study at any time without providing a reason. If you choose to withdraw, please contact the principal researcher and all data collected about you will be destroyed.

How will the results be shared?
The study findings will be discussed in a graduate thesis and may also be published in journal articles and books. The report will be publicly available in the Simon Fraser University Library.

Who can you contact if you have complaints or concerns about the study?
If you have any questions or concerns about your rights as a research participant and/or your experiences while a participating in this study, you may contact Dr. Jeffrey Toward, Director, Office of Research Ethics.

Consent for the use of your name and recording
Do you consent to the recording of the interview? The recording will be transcribed and then destroyed. You may withdraw consent at any time during the research process. After this, the recording and related transcription documents will be destroyed.
 Yes
 No

Do you consent to the potential use of your name in the final report? Selecting “No” will ensure that you will not be identified by name in the final report. You may withdraw consent and any time during the research process.

 Yes
 No

Consent Statement

Taking part in this study is entirely up to you. You are under no obligation to participated in this study. If you decide to participate, you may withdraw consent at any time.
Your signature below indicates that you consent to participate in this study.

_____	_____
Participant Signature	Date (yyyy/mm/dd)