Developments in Identity Theft and in the Protection of Personal Confidential Data and their Impact on IFA Practice and IFA Standards.

Research Project for Emerging Issues/Advanced Topics Course

Master of Forensic Accounting (MFAcc) Program

University of Toronto

Prepared by Anna Gubin

June 18, 2021

For Professor Leonard Brooks

Table of Contents

Table of Contents ii

Executive Summary vi

List of Abbreviations ix

Documents Reviewed/Relied Upon x

Acknowledgements xi

Introduction 112

Section I: Developments in Identity Theft 14

1.1 How Personal or Business Identities Are Obtained 14

Through information systems or databases 15

Through financial scams/fraud 16

Through business/organization vulnerabilities 222

In-house theft 222

Outsourcing 23

1.2 How Personal Identities Can Be Used by Thieves or Fraudsters 24

As an avenue to other crimes 24

As a business opportunity 26

Through repeat victimization 26

Through vulnerable “identities” 27

1.3 Business Identity Theft 29

Through business-number theft 30

Profiting from stolen business numbers or stolen business identities 32

1.4 Tax Schemes Related to Identity Theft 37

Income tax preparation 37

Working Income Tax Benefit (WITB) scheme 38

Wages-to-loan tax scheme 39
1.5 Offenders and Victims 40
Low-frequency offenders 40
Opportunity takers 41
High frequency offenders 41
Most common justifications given by identity thieves 42
Problems experienced by victims of identity theft 43
Victims may not report identity theft 46
Financial institutions may not report identity theft 48
1.7 Increased Identity Theft Because of COVID-19 50
Case 1: “Stimulus Programs Draw a Flood of Scammers 50
Case 2: “Canadians have lost more than $1.2 million to COVID-19 scams” 51
Case 3: Krebs on Security, “How Cybercriminals are Weathering COVID-19” 52
Section II: Recent Developments in Protection of Personal Confidential Data 52
2.1 What Individuals Can Do to Reduce Identity Theft 53
2.2 What Businesses Can Do to Reduce Identity Theft 56
2.3 Steps to Take by Victims of Identity Theft 59
Section III: Principal Roles of IFAs Against Identity Theft 61
3.1 IFA Expertise 61
3.2 IFA Role of External Investigator/Consultant 62
In fraud risk prevention 63
In educating employees 63
In designing procedures to prevent fraud 65
In fraud risk detection 66
In fraud investigation and corrective action 66

3.3 IFA Role of Internal Investigator 67
In fraud risk governance 67
In fraud risk assessment 68
Fraud risk identification 69
Fraud risk likelihood 70
Fraud risk response 70
3.4 IFA Roles With the Courts 70
Litigation consultant 70
Expert witness 71
3.4 Other IFA Roles 71
Anti-money laundering 72
Certification – Sarbanes Oxley Act 2002 (SOX) 73
Cybersecurity 73
Internal audit 74
Whistleblower reporting solutions 74
Section IV: IFA Standards Relevant to Identity Theft 75
4.1 Legal Standards 75
4.2 Professional Standards 76
4.3 Ethical Standards 76
4.4 Engagement Standards 77
Section V: Challenges 78
In Designing Controls and Procedures 79
In Fighting Identity Theft 80
The Impact of Identity Theft on the Economy and the Consumer 80
Section VI: Conclusions 81

Section VII: Bibliography 84
Appendix I: Interviews 90
Interview #1 90
Interview #2 92
Interview #3 94
Interview #4 96
Interview #5 99

Executive Summary

> *"Reports that say that something hasn't happened are always interesting to me, because as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say, we know there are some things we do not know. But there are also unknown unknowns — the ones we don't know we don't know…."*[1]

Identity theft is a crime committed by those obtaining personal identifying information from another person or group for wrongful purposes such as fraud or deception, which usually results in some personal gain.[2]

The introduction of personal computers, smartphones, iPads and the introduction of the Internet have changed the way data can be gathered, analyzed, and shared. Constant use of technology has become so integrated with our way of life that the exchange of information, and in many cases personal and sensitive information, has become almost commonplace.

People put more and more personal and sensitive data about themselves on the Internet through social media platforms or by using free, unsecured Wi-Fi to access their private accounts. These data can end up in the hands of the thieves.

Identity theft causes financial damage to consumers, creditors, retailers, and the economy[3] and challenges to policy- and law makers.

---

[1] (https://en.wikipedia.org/wiki/There_are_known_knowns).

[2] ACFE, Association of Certified Fraud Examiners, available at (https://www.acfe.com/fraud-101.aspx), last visited June 2, 2021.

[3] Hoofnagle Chris Jay, Fall 2007. "Identity Theft: Making the Known Unknowns Known", Harvard Journal of Law & Technology, (https://jolt.law.harvard.edu/articles/pdf/v21/21HarvJLTech097.pdf).

This paper examines developments in identity theft, how we as individuals can protect ourselves against identity thieves, and how we, as future Investigative Forensic Accountants (IFAs) can assist in the fight against identity thieves.

Section I describes identity theft in many forms and how it is adversely affects people in society. In particular, methods range from simple theft of electronic devices containing passwords, shoulder surfing and dumpster-diving, to sophisticated online- and telephone methods of acquiring personal and business information. This section discusses typical scams used by identity thieves to persuade consumers to divulge their personal data. It examines offenders and victims and why identity theft may not be reported. Sample media coverage shows how COVID-19 has increased fraud and identity theft.

Section II describes recent developments in protecting personal information and what individuals and businesses can do to reduce identity theft.

Section III discusses the roles IFAs can play to protect people and companies against fraud and identity theft, as investigators, consultants, educators, procedure designers, fraud risk assessors, and expert witnesses. **Section IV** looks at IFA practice standards particularly relevant to identity theft.

Findings

My research suggests that individuals and organizations are not doing enough to protect their personal data, especially as fraudsters become more sophisticated, organized, and convincing.

Victims of identity theft may lose confidence in e-commerce and may lose their financial reputations because of an identity thief's misuse of financial assets.

Identity theft causes economic losses to businesses due to liability issues, fines, and loss of clientele if security measures are not adequate. It causes price increases, because identity theft drives up the costs of doing business, and these costs are passed onto consumers.

Harsh penalties should be in place for identity thieves, but governments are behind in creating laws that are effective in protecting information (e.g., preventing the selling of confidential information or requiring disclosure that it might be sold, and requiring increased website privacy and security). Identity theft is under-reported because victims are embarrassed by it and institutions are afraid of liability. Law enforcement is not very effective in the fight against the identity theft crimes, because they do not have enough resources.

Fraud cannot be eliminated completely, but can be reduced. IFAs must become more cognizant of the fraud landscape against which they operate. Creativity, professional skepticism, investigative problem-solving skills, knowledge of the legal process, and curiosity are characteristics that IFAs must possess to help address issues that identity theft can present to an engagement.

IFAs have many roles in the fight against identity theft. They have special expertise and can work with industry as external investigators/consultants, internal investigators, or with the courts. They can play an increasing role in fraud risk detection, investigation, and corrective action.

List of Abbreviations

Term	Definition
ACFE	Association of Certified Fraud Examiners
AML	Anti-Money Laundering
ATM	Automated Teller Machine
BIG 4	When people mention BIG 4, they mean 4 large accounting companies in Canada: KPMG, Deloitte, Ernst, and Yonge and PriceWaterhouseCoopers.
CERB	Canada Emergency Response Benefit
CPA	Chartered Professional Accountant
CRA	Canada Revenue Agency
CVV	Card Verification Value (on the back of a credit card)
DOB	Date of Birth
HST	Harmonized Sales Tax
ICGN	International Corporate Governance Network
IFA	Investigative Forensic Accountant/Accounting
IRS	Internal Revenue Service (U.S.)
IT	Information Technology
ITA	Income Tax Act
NOA	Notice of assessment for Canadian personal and corporate returns
PIN	Personal Identification Number
PIPEDA	Personal Information Protection and Electronic Documents Act
RCMP	Royal Canadian Mounted Police
SIN	Social Security Number
SRED	Scientific Research and Experimental Development
Stimulus Program	This program is used in the U.S. to pay people that lost jobs due to COVID-19. In Canada people receive the Canada Emergency Response Benefit (CERB).
WITB	Working Income Tax Benefits

Documents Reviewed/Relied Upon

The bibliography includes various sources examined during my research. Where applicable, the research paper contains express references to the sources that support the views expressed therein. Listed in the bibliography, the documents reviewed in this paper include journals, textbooks, research papers, reports, and academic presentations. Also, please note that I used University of Toronto Library to access articles and reports. In the biography I listed articles and the websites, where these articles can be found, but some of them can be accessed for a fee.

When performing my research, I interviewed various individuals working in different industries (Appendix 1, Interviews 1-3), as well as individuals working directly in fields related to identity theft (Appendix 1, Interviews 4-5). Individuals working in different industries have the responsibility of safeguarding personal information within their organization and that was a reason for conducting interviews. The objective of the interviews was to gather knowledge from different people on the issue of identity theft and how personal information in different organizations is handled and protected.

Finally, the comments expressed herein are my own, and should not be regarded as being necessarily shared by any professional firm or organization with whom the writer is associated. Views and interpretations presented in this research paper should not be considered legal advice and are solely those of the author. The ideas and suggestions presented here are for discussion purposes only.

Acknowledgements

I wish to acknowledge the guidance and feedback made by my mentor Caroline Dixon during the research for this report. Thank you for all your support and always encouraging me to look at things from a different angle and for encouraging me to perform more research and gather additional information. Your guidance aided in my growth as an MFAcc student. Your knowledge, professionalism, and dedication are truly assets to the field of forensic accounting.

I wish to acknowledge Nadia Zyeva, Shulamit Finkelstein, Khaled Shoeb, Dwyne King, and Caroline Dixon for allowing me to interview them and for providing me the answers to my interview questions.

I wish to acknowledge Professor Brooks and MFAcc faculty for providing guidance and for giving me the opportunity to write this research paper. This was a great work experience for me.

Introduction

It is almost too easy to get money from people through business impersonation or personal identity theft. For example, because of many peoples' lack of understanding of digital identities and their failure to take online security seriously, combined with too much trust in strangers or fear of authority (e.g., the Canada Revenue Agency (CRA)), criminals use their better understanding to take money from people.

In recent years, phone scammers tell people that they owe taxes and must pay if they do not want to be prosecuted. Many people become victims of such scams, even if they do not owe any money to CRA or other government organizations. Newcomers are particularly vulnerable, but we are all vulnerable. Scammers can be tough and convincing, even to me, the author, a chartered professional accountant (CPA), who knows that I do not owe any money to the CRA and that the police cannot come and arrest me.

In other cases, people give away information about themselves in full and for free, without even realizing it,[4] either to phone scammers pretending to be from a research group conducting interviews or through posting information about themselves on social media sites (e.g., Facebook). People reveal their daily habits, where they work, names and pictures of themselves and their family, etc. Not everyone makes their information private, for "friends" only. Even if they do, many people accept new friends without

[4] Research Note: During the author's research, much information was found on social media sites without any privacy protection or restrictions for use.

doing a background check to confirm they know them. So, we can say that victims also help to gather information about themselves because of their behaviour online.

Understanding how identities are stolen and the motives behind the actions of the criminals may not eliminate identity theft, but might make it harder for criminals to steal someone's identity if action is taken.

Through examples and personal experience, the aim of this research paper is to enhance the reader's understanding of:

- recent developments in identity theft: how personal or business information is obtained and used by criminals.
- who the perpetrators and victims are.
- how to protect personal and business information and the steps victims must take to recover from identity theft.
- what roles investigative forensic accountants (IFAs) can play to protect people and companies against fraud and identity theft and which IFA standards of practice are particularly relevant.
- continuing challenges in fighting identity theft and its impact on the economy.

Section I: Developments in Identity Theft

Let us answer the questions: What happens in identity theft cases? Why is it happening?

Identity theft includes not only stealing personal information, it includes the stealing of company identities (See section 1.3 Business Identity Theft), since a corporation is considered an individual under the Income Tax Act (ITA).[5] [6]

For perpetrators, knowing in advance that there likely will be no consequences when a financial crime is committed under a false identity is a strong incentive to commit that crime. With financial crimes, unlike murder investigations, fingerprints and other forensic evidence are not easily collectable. This section looks at how identities can be obtained, how they can be used, and who are the perpetrators and victims of identity theft and fraud. Also, I would like to refer to interviews #4 and #5 in which individuals working as Forensic Accountants confirmed that in many cases it is hard and almost impossible to bring identity thieves to justice.

1.1 How Personal or Business Identities Are Obtained[7]

Techniques used by identity thieves can be divided into two categories: those used to obtain an identity and those used to convert stolen identities into cash.[8] Identities are

[5] Income Tax Act (RSC, 1985, c 1. (5th Supp.)). (https://laws-lois.justice.gc.ca/eng/acts/i-3.3/page-33.html)

[6] Research Note: In this research paper, only corporations are covered, not partnerships or joint ventures.

[7] Newman Graeme, McNally Megan M., (July 2005). "Identity Theft Literature Review", (https://www.ojp.gov/pdffiles1/nij/grants/210459.pdf)

[8] Research note. These lists of techniques are derived or taken mostly from Internet sources of different kinds, e.g., newspapers, magazines, reports, interviews with different law enforcement agents and research articles.

obtained through information systems, financial scams, and through business vulnerabilities, among others.

Through information systems or databases

Identity thieves may gain access to the personal information of others by using the weaknesses of some information systems or by breaking into databases. This will give access to different sorts of information, depending on what kind of database is compromised and if actual data inside the database was secured or not.

Credit card fraud resulting from the compromising of a retailer's database is a good example. (See inset example).

> ***Example: When Retailers Databases Are Compromised: Credit Card Fraud***
>
> When the database of a retailer is compromised, information on many customers will be compromised: for example, addresses (if goods were shipped), first and last name, date of birth (if the retailer sends birthday messages), credit card number with the expiration date and sometimes the Card Verification Value (CVV) code (on the back of the card).
>
> Fraudsters could make purchases on a credit card account or make a new credit card. All purchases made go on the victim's credit card statement. Later, the credit card company will ask the victim of credit card fraud to pay for goods that were never purchased.
>
> Since credit card companies provide insurance, most likely the amount of harm done to the cardholder will be minimal, beyond the time spend to obtain a new credit card and to stop use of the old one.
>
> Credit card fraud provides entry into the system that will get fraudsters goods and services without the serious possibility of getting caught.

Depending on what kind of personal information is stored in the compromised electronic database, offenders might access bank accounts of the victims, open telephone or utility accounts, or obtain a driver license in the victim's name. Identities can also be sold to criminals who commit further crimes. New identities with clean records can be created

from stolen information, and these can be sold to hide the real identities of illegal immigrants or criminals. (For more information, see Section 1.2.)

Through financial scams/fraud

Financial scams, for the most part, are old scams adapted to new technologies in order to obtain victims' identities. Getting the information to carry out scams or fraud range from simple to sophisticated, as the following examples show:

- **Simple theft:** Thieves may steal paper documents from household or business garbage or mail. (See inset example.)

> ***Example: Dumpster Diving and Mail Theft Can Pay Off***
>
> Information from a business's dumpster, people's home garbage, or a mailbox can be valuable to thieves.
>
> With found financial information (e.g., credit card statements, bank statements), utility bills, and other account information, fraudsters could, at a minimum, change the victim's address to another and receive the victim's financial and other information directly.
>
> The solution? Business and personal records should be shredded before discarding. Individuals can request that all statements be in electronic format. Individuals could login to view and print statements when they need them.[9] Home mail should not be left in the mailbox for long periods of time, and locks should be installed. [10]

- **Telephone or telemarketing fraud:** Fraudsters/scammers request personal details while pretending, for example, to do a security check or collect money for a charity. **Solution:** To prevent this, people should not give any personal

[9] CIMIP, Center for Identity Management and Information Protection, (https://www.utica.edu/academic/institutes/cimip/idcrimes/schemes.cfm).

[10] CIMIP, Center for Identity Management and Information Protection, (https://www.utica.edu/academic/institutes/cimip/idcrimes/schemes.cfm).

information to people that do not need to know it. If someone calls and asks for personal information, people should tell the caller that they will call them back.[11]

- **Scam centres:** Scam centres are a form of organized crime for telephone fraud. The scams work, because the "fraudsters…strike a lot of fear" in their targets." [12] For many years, scammers have identified themselves as CRA representatives claiming that there is a tax balance to be paid, and if it is not paid, police will make an arrest. Another scam is called the "bank investigator scheme…[see inset example] now one of the most prolific, with the Canadian Anti-Fraud Centre[13] reporting a least $3 million stolen from Canadians in an already dark 2020." [14]

[11] CIMIP, Center for Identity Management and Information Protection, (https://www.utica.edu/academic/institutes/cimip/idcrimes/schemes.cfm).

[12] Miller, Harry, March 20, 2021, "As COVID surged, Indian police shut down scam centres targeting Canadians. Now, they're back – CBC.ca," *Canada News Media* (https://canadanewsmedia.ca/as-covid-surged-indian-police-shut-down-scam-centres-targeting-canadians-now-theyre-back-cbc-ca/).

[13] See Canadian Anti-Fraud Centre, Services and information, alphabetical list of scams at (https://www.antifraudcentre-centreantifraude.ca/index-eng.htm).

[14] Miller, Harry, March 20, 2021, "As COVID surged, Indian police shut down scam centres targeting Canadians. Now, they're back – CBC.ca," *Canada News Media* (https://canadanewsmedia.ca/as-covid-surged-indian-police-shut-down-scam-centres-targeting-canadians-now-theyre-back-cbc-ca/).

Example: The Bank Investigator Scheme: A Common Scam-Centre Call

Under the *Bank Investigator Scheme*, phone scammers pose as bank investigators looking for people's help and money.[15] The Canadian Anti-Fraud Centre lists many scams[16] and describes many story variations.[17]

People could be told that officials from their banks are under investigation, and higher up/police/other financial institution or officers of business bureau of Canada [different calls have different version of who imposters represent] need their help to catch those individuals before they disappear with people's money.

The scammers direct targets "…to purchase gift cards, which…would be tied to the purported thieves, and thus help to track who they are."

To be convincing, scammers claim to have a target's "…name, home number, address and some bank information…that is often obtained from contact lists gathered sometimes by legitimate businesses (e.g., data brokers[18]) that scammers buy for pennies per name."

Scammers "…get paid a percentage of the steal."

"The fraudsters…strike a lot of fear" in their targets."[19] They try to prevent targets from hanging up, and start with the lines like, "If you hang up, nothing can be done to help you, and your credit will be ruined, and/or your money lost out of

[15] Quotations taken from Miller, Harry, March 20, 2021, "As COVID surged, Indian police shut down scam centres targeting Canadians. Now, they're back – CBC.ca," *Canada News Media*, (https://www.cbc.ca/news/marketplace/marketplace-india-scam-centres-1.5947798).

[16] See Canadian Anti-Fraud Centre, Services and information, alphabetical list of scams at (https://www.antifraudcentre-centreantifraude.ca/index-eng.htm).

[17] See Canadian Anti-Fraud Centre, "Bank investigator," at (https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/b-investigator-enqueteur-eng.htm).

[18] Melendez Steven and Pasternack Alex, March 2, 2019. "Here are the data brokers quietly buying and selling your personal information", Fast Company Journal, (https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information).

[19] Quotations taken from Miller, Harry, March 20, 2021, "As COVID surged, Indian police shut down scam centres targeting Canadians. Now, they're back – CBC.ca," *Canada News Media*, (https://www.cbc.ca/news/marketplace/marketplace-india-scam-centres-1.5947798).

bank accounts." or "This is a last warning, before matter will appear before her majesty in the court of law."[20]

- **Bribery or extortion:** Fraudsters could also commit crimes like extortion and bribery to access financial and personal databases or records of businesses and other agencies. For example, employees could be threatened or bribed to provide passwords or access to an employer's buildings or records. **Solution:** Many organizations try to prevent this by giving employees access to only the customer data they need. However, if two or more employees collude, they can pool information on an individual. Finding out who sold/leaked the information will be difficult since, officially, employees should have limited access. Another measure that companies have put in place to prevent stealing of customer information is to allow employees access only when they are serving the customer. (See inset example.)

Example: Limiting Employee Access to Customer Information

In April 2020, I (the author) called Rogers regarding a personal issue with the Internet and was told to stay on the call, since Rogers employees cannot do work on my account if the call is ended.

To prevent agents from browsing through customer accounts, internal auditors verify, on a random basis, that the time an employee spends on a customer's account agrees to the time the same customer is on the phone with an agent.[21]

At first glance this seems like a good control. But what prevents an employee from taking a screenshot or photo with a personal phone of the page of customer details, especially now

[20] The author received phone calls with such messages and was asked to press 1 to continue and to get help.

[21] This example is the author's personal experience. When told about staying on the phone, I started to ask questions. I was told about this control in place at the Rogers calling centre in Mississauga.

(spring 2021) when, because of the pandemic, people have been working from home for more than a year?

I asked my spouse, who has almost 30 years of experience as a computer engineer, about this issue. He told me that it is almost impossible for an employer to monitor each computer, especially when people are working from home. Monitoring is possible in a controlled environment, like an office, but not at people's houses. Employees can go "offline" and no one at the organization can see what they are doing. Employees could be selling some or part of the information they see.

There is no control over employees saving information on their own personal devices. Company compilers may not have the option to save any information from a laptop. Even if an employee's company e-mail is monitored, personal e-mail is not.

- **Shoulder surfing**: A would-be thief attempts to get close enough to a victim at an automated teller machine (ATM) machine to see the personal identification number (PIN) when entered. More sophisticated thieves install small cameras at ATM machines or gas stations to view people entering their PIN codes. **Solution:** To avoid this, people need to be aware of their surroundings, and shield passwords and PINs when entering them.[22]
- **Skimming:** Criminals use electronic devices that will read and record information on the magnetic strip of a credit card. This enables criminals to use the information to create another credit card, linked to victim's account, to make unauthorized purchases. **Solution:** To prevent this, people should not let other people use their cards (e.g., in a restaurant, when a waiter takes a client card to a

[22] CIMIP, Center for Identity Management and Information Protection, (https://www.utica.edu/academic/institutes/cimip/idcrimes/schemes.cfm).

terminal) and they should check their credit card statements for unauthorized purchases.[23]

- **Phishing:** Phishing schemes are the most common types of computer identity theft.[24] A phishing e-mail is sent to legitimately or illegitimately acquired email addresses, often looking as though it comes from a legitimate-looking organization. For example, an email might say it comes from a financial institution. It might say that the client's bank account was compromised and will be closed if the client does not contact the bank. In the e-mail, a link is provided for the client to click. Clicking on the link might take the client to a real-looking website and the client will be asked to login. The login information will be copied, and thieves will login into the actual account. In addition, spyware could be installed on the victim's computer to monitor activity and to copy passwords for different websites. **Solution:** To prevent this, the receiver of such e-mails should not click on any links but delete the e-mail. If they are still concerned, they can call their financial institutions directly to discuss the status of their account.[25]
- **Social engineering:** Social engineering is the practice of pretending to be someone else over the phone, Internet, or in person[26]. Usually, social engineers know some information that leads a person to believe they are legitimate and give

[23] CIMIP, Center for Identity Management and Information Protection, (https://www.utica.edu/academic/institutes/cimip/idcrimes/schemes.cfm).

[24] Author note: As part of my job I must attend different cyber/computer security courses. Instructors at Deloitte were referencing to phishing schemes as most common type of computer identity theft.

[25] CIMIP, Center for Identity Management and Information Protection, (https://www.utica.edu/academic/institutes/cimip/idcrimes/schemes.cfm).

[26] CIMIP, Center for Identity Management and Information Protection, (https://www.utica.edu/academic/institutes/cimip/idcrimes/schemes.cfm).

the information requested. **Solution:** To prevent this, people should not give any personal information to people that do not need to know it. If someone calls and asks for personal information, people should tell the caller that they will call them back.[27]

Through business/organization vulnerabilities

In-house theft

Client/customer records may be vulnerable to theft or copying by people working for a business or organization, as the following examples show.

- **Employees:** Employees may have access to large amounts of sensitive client data.[28] The author, for example, working as a manager in one of the Big 4 accounting companies, has access to very sensitive client data, such as social insurance number (SIN), date of birth (DOB), CRA access and CRA representation for the client, current and prior addresses, and employer or business information. We may also have access to data related to the clients' children and relatives, since in many cases the client will pay us for preparing tax returns for them.

[27] CIMIP, Center for Identity Management and Information Protection, (https://www.utica.edu/academic/institutes/cimip/idcrimes/schemes.cfm).

[28] Weisburd David, Waring Elin, June 2009. "White Collar Crime and Criminal Careers", Cambridge Studies in Criminology, (https://www.cambridge.org/core/books/whitecollar-crime-and-criminal-careers/6D3DC88DCFCF9FEA7C8D9D9508CDD8E8). The Book can be downloaded from this website.

- **Employees working from home:** Employees working from home may pose additional risks to company data. (See inset example, *Limiting Employee Access to Customer Information*, above).
- **Organized theft:** In many organizations,[29] duties and assets are segregated so that one employee cannot access all information about a client. In addition, some information is restricted, accessible only with a senior manager's/partner's/owner's approval, even for employees with a high clearance/access level. These restrictions are in place so that employees will not be tempted to sell or alter client information. Unfortunately, these restrictions can be by-passed when employees with different access levels collude and bring together the information on an individual.
- **Unethical businesses:** Business information is exposed in many ways. As an example, many people who are not registered professionals or CPAs prepare personal and corporate tax returns in their homes. No engagement/ confidentiality letters may be signed with the client. What if they sell information or use it fraudulently? [30]

Outsourcing

Outsourcing work can make client/customer records vulnerable to theft or copying. (See inset example.) Even in Big 4 companies, it is not always clear from engagement letters that work could be outsourced to other countries; for example, companies receiving

[29] This information comes from author's personal work experience as an auditor for last 11 years. During this time the author performed many audits. One of the first things the author asked clients, to help understand the entity and its environment, was about segregation of duties and safeguard of assets.

[30] Research note: The author knows people that prepare tax returns in their homes without being professional accountants and without providing a contract regarding confidentiality.

outsourced work might be given uninformative names like "USI group."[31] At other times, clients may overlook long engagement letter details that indicate that work can be outsourced overseas.

Example: Could Outsourcing of Work Contribute to Identity Theft?

To save labour costs, many big companies outsource administrative work[32] to countries where employees are paid less than in Canada.

In my experience, at a Big 4 company, outsourced work has consisted mostly of printing and finalizing financial statements and tax returns. But in doing that work, workers have access to clients' sensitive information, such as SIN, DOB, address(es), tax history, and more.

If this information were taken and later sold (by in-house or outsource workers), it would be extremely difficult to trace and to determine at what stage of tax preparation it was stolen.

1.2 How Personal Identities Can Be Used by Thieves or Fraudsters[33]

As with obtaining personal information, the use of stolen identities can be simple or sophisticated as the following examples show.

As an avenue to other crimes

Identity theft can be a motive to commit other crimes because, today, identity thieves recognize the monetary value of personal information. Offenders may commit traditional theft-related crimes, but the main goal is to collect personal information. (See inset example.)

[31] This information comes from the author's work experience in a Big 4 organization.

[32] Research note: this information is the author's experience, through working as an auditor and working in big companies.

[33] Newman Graeme, McNally Megan M., (July 2005). "Identity Theft Literature Review", (https://www.ojp.gov/pdffiles1/nij/grants/210459.pdf)

Example: Identity Thieves Recognize the Value of Personal Information

When I lived in Richmond Hill, Ontario in spring/summer 2020, local papers reported that thieves entered residences under false pretenses and took, by force, cell phones and other electronic devices (e.g., tablets and laptops).

Why would thieves take these devices if jewellery, cash, or other valuable items could be stolen instead?

One reason could be to extract personal information from them.

I talked to several people (including family, friends, co-workers) unofficially about this subject. I learned that many save all of their passwords on their devices and click "save" for new passwords when they open new accounts. But using this shortcut to avoid entering passwords every time they access their accounts could turn them into victims of identity theft if their devices are stolen.

For example, with stolen laptops, tablets, or smart phones, thieves may be able to access passwords saved on the devices to enter bank accounts, e-commerce sites, e-mail messages, and apps to reset passwords. They could move money to other accounts through e-mail transfers, make purchases, and retrieve personal and even business-related information (e.g., pay stubs, employer information) before victims regain access to their accounts. Some information might be sold on the "dark web"[34] or "underground."[35]

To commit a crime under the identity of someone else is an attractive proposition since it reduces the risk both in commission of the crime and in getting caught after the crime. For example, renting a car with a stolen identity seems less risky than stealing one.

[34] Dark web: the part of the World Wide Web that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable, (https://en.wikipedia.org/wiki/Dark_web).

[35] Underground: economic activity that takes place outside government sanctioned channels. Underground transactions usually occur "under the table" to avoid government price or taxes, (https://www.investopedia.com/terms/u/underground-economy.asp).

As a business opportunity

To facilitate other crimes, an identity thief could obtain a couple of major pieces of information (e.g., a birth date and SIN) and use this information to "breed" (develop) additional documents. (See inset example.)

Example: Document "Breeding"

If identity thieves obtain a couple of major pieces of information (e.g., a birth date and SIN) they can use this information to "breed" (develop) additional documents.

For example, using this information might allow an apartment to be rented. This will give scammer an address, so that utility bills can be obtained. With utility bills a library account can be opened and that could provide a scammer with a quasi-government-issued identity document (ID). That additional information might allow a bank account to be opened and credit card applications to be filled out. A driver's license might be issued based on the information obtained by the scammers.

Breeding identity documents creates a "business opportunity" for fraudsters. They can put together fake document packages to sell underground or through the dark web.

Counterfeit identity documents could start with the identity's young age, include bank accounts, and even filed tax returns, so when fraudsters sell these packages, purchasers will gain the background and current life of someone else.

Counterfeit identity documents are attractive for undocumented workers or people that have committed or plan to commit crimes and are trying to escape jail or punishment. Committing offences in another person's name means that police will look for that person, not the true offender.

Through repeat victimization

Repeat victimization refers to repeated attempts by a fraudster to use an individual's identity until its ability to generate money and opportunities for additional crimes is exhausted. (See inset example.)

Example: Crime Doesn't Stop with the Theft of a Wallet

When victims of identity theft discover that their identity has been compromised, they will not likely know the extent of the compromise.

For example, after theft of a wallet, the victim will stop all activities on bank accounts and credit cards. New credit and bank cards will be sent to the victim, and the victim will think that the episode is over.

But the thief might sell the victim's driver license and other documents on the street or to people that specialize in document breeding. After the initial theft of the wallet, the victim will suffer more consequences if the driver license is used to open new bank- or credit card accounts, or to take a loan in the victim's name: repeat victimization.

Through vulnerable "identities"

Deceased people's information has been used by identity thieves to get car loans, cell phones and phone plans that cannot be traced to the offender[36].

Offenders have continued to receive pensions and benefits or have claimed the deceased as a dependent on tax returns in order to obtain personal tax credits[37].

In recent years, the CRA found a way to ensure deceased people are not "collecting" CPP, old security, and other benefits by requiring funeral directors to file death certificates with the CRA. When the certificate is filed, all payments are stopped.[38] But this is only for the CRA.

---

[36] Newman Graeme, McNally Megan M., (July 2005). "Identity Theft Literature Review", (https://www.ojp.gov/pdffiles1/nij/grants/210459.pdf)

[37] Newman Graeme, McNally Megan M., (July 2005). "Identity Theft Literature Review", (https://www.ojp.gov/pdffiles1/nij/grants/210459.pdf)

[38] The following information was received during author's experience in performing audits and reviews in funeral homes. Since deceased people and benefits after death are not topics of this research paper, no further work was performed on the topic of deceased persons' benefits. The practice described is for Ontario and may be different in other provinces.

Banks and other financial institutions do not receive this information automatically, so for them and for the purposes of offenders, new accounts can be opened in the deceased person's name and offenders can apply for overdraft protection, take the overdraft, and never repay it[39]. New credit card accounts can be opened, be "maxed out" and never repaid. Completely "new" identities can be created using information about the deceased found in obituaries, or illegally acquired (e.g., purchased from employees) from funeral homes or retirement homes[40].

Elderly people often become targets of identity thieves, for several reasons. They may:

- not be technologically educated and are not likely to keep up with all the latest developments.
- view credit card transactions monthly, instead of in real time, as for many younger people, and will not see a fraudulent transaction until statements are received.
- have difficulty transitioning to online services (especially because of COVID-19), setting up numerous accounts, and remembering different passwords. They may not know about or be able to set up identity verification tools and smart phones, let alone about how to update apps on computers or phones to ensure that the latest updates are all installed.

[39] Newman Graeme, McNally Megan M., (July 2005). "Identity Theft Literature Review", (https://www.ojp.gov/pdffiles1/nij/grants/210459.pdf)

[40] Newman Graeme, McNally Megan M., (July 2005). "Identity Theft Literature Review", (https://www.ojp.gov/pdffiles1/nij/grants/210459.pdf)

- rely on “professionals” to help them navigate online, who could take advantage of their vulnerability. If fraud is discovered, pointing to anyone will be difficult since, usually, time has passed.

Newcomers to Canada can also be easy targets for criminals, particularly if they are not fluent in English and are intimidated by authority. In many countries, the police are corrupt, and it is quite common for police to come and arrest people if they owe money.[41] Also, because, in some countries, brutality by the authorities is common, newcomers to Canada might easily be fooled by a person phoning and claiming that to be from the police or the CRA. They might be willing to pay the fraudsters, so they and their family will be left alone. They do not know Canadian laws, have not dealt with the CRA or police on a regular basis, and-do not know that the CRA never demands payments over the phone, especially by prepaid cards. Also, many of them do not know to whom to turn. They do not have lawyers or accounts that they can ask and may be afraid to call police.

1.3 Business Identity Theft

Identity theft is not just about stealing information about an individual; it can also include businesses. In the identity theft of a business, a stolen business number and business address are the main pieces of information used to steal the business identity and to take over the business.

Anyone who knows how the system of corporate tax returns works, and how HST, payroll, and revenue recognition work, knows there is room for manipulation. Identity

[41] The author was born in Soviet Union and lived in Ukraine and Russia after Soviet Union collapsed. Brutality and bribery are common in dealing with authorities. Unfortunately, there is no such thing as a “right” in such countries.

theft of a business will include some of the same "gains" as for personal identity theft but can include false billing or applying for different grants available only to businesses and claiming different refunds from the CRA.[42]

Through business-number theft

Stealing a company's business number and business address may be easy to do in Canada, because information is publicly available and is easily accessed by people who know where to look and because the business number remains the same for the following types of accounts: Corporate Account (for this account only letters "RC" are being added after the 9-digit number); for HST account (RT) letters are added and for Payroll account (RP) letters are added[43].

For example:

- **Exploiting supplier information:** Information on a company's suppliers may not be as highly secured as that of customers. By accessing a supplier's invoice, an employee could obtain information including the name of the company, address, phone number, e-mail address, contact information, and HST number. (See inset example.)

[42] Research note. The author uses her knowledge as a CPA, with many years of experience in industry and public practice and uses her knowledge about identity theft in a business.

[43] Research note. The author uses her knowledge as a CPA, with many years of experience in industry and public practice and uses her knowledge about identity theft in a business.

Example: Business Identity Theft: The Business Number is Key

The HST number is the company's business number followed by an alpha-numeric code beginning with "RT." The alpha-numeric for payroll begins with "RP," and for corporate account with "RC" By convention, only two letters, the same for all of Canada, will differ between them.[44]

This information could be:

- **sold, or a similar entity could be created**, with a name that is like a supplier. On the street, this information could be used by fraudsters to make invoices using the correct HST number and send it to entity, the legitimate supplier is doing business with. Address on the invoice can be changed and cheque will be sent to the thieves address. Please note, that this fraud would require inside knowledge, like when suppler is usually paid and for what services.
- **used to file for government grants/financial support** such as COVID related CEBA in the amount of $60,000[45] or loans from financial institutions and credit cards in the stolen company's name. For other examples (See Sections 1.3, 1.4 and 1.7).
- **used to claim different refunds** from the CRA.[46] HST refund can be claimed on non existing expenses. To prepare and claim refund, HST report needs to be prepared and filed with CRA. Fraudster would be claiming fake expenses to claim Income Tax Credit (ITC) on such expenses and after report will be filed with CRA, will wait to cheque to arrive.

- **Opening a fake business.** It is not difficult to open a business account, and one can be opened online. The only information needed is a valid address and the name of a shareholder. It can be any name, since the CRA does not verify the

[44] Research note. Author is working with different business accounts for many years. All information about different kinds of business accounts can be obtained on CRA official website. (https://www.canada.ca/en/revenue-agency/services/tax/businesses/topics/registering-your-business/you-need-a-business-number-a-program-account.html).

[45] Government of Canada website, (https://www.canada.ca/en/services/benefits/covid19-emergency-benefits.html).

[46] Research note. Author uses her knowledge as a CPA, with many years of experience in industry and public practice and uses her knowledge about identity theft in a business.

name of the shareholder and does not check agreement of the name to the driver license, etc.[47]

- **Using a dormant business's information.** Fraudsters could use the number of a dormant business for illegitimate purposes. There are a lot of business accounts that are dormant. So, there are two ways to claim the identity of a business. Either create a new, fake one online (see above) or through taking the identity of an existing business that has been dormant for years.

  Information on dormant businesses can be:

  - found online
  - purchased from employees working in archives, or people working for companies that prepare tax returns (see *Unethical businesses* in Section 1.1, above).[48]

- **Exploiting public information.** Business numbers of any business are public knowledge and can be found on the CRA website. There is an option to search for an HST number to verify its validity. By learning the HST number a thief will know the business and payroll numbers, etc., as explained above.

Profiting from stolen business numbers or stolen business identities

Let us look at the most common ways for offenders to profit from stolen business numbers or stolen business identities of, for example, dormant businesses.

[47] Research note. Author helped many clients to open bank accounts and is aware of the documents that are needed to open a new business.
[48] Research note. The author knows people that prepare tax returns in their homes without being professional accountants and without providing a contract regarding confidentiality.

Examples follow of common ways for offenders to profit from business number theft, or by assuming the identity of a dormant business. They can:

- **Make false financial statements and apply for loans and credit cards in the company's name**. Under this scenario, a new business will be opened under a fake owner's identity. Since, now, businesses can be opened online and corporate numbers will be e-mailed, any name can be used to open a corporation. Fake financial statements and even fake federal returns will be prepared and filed with the CRA because, in order for the business to get a loan, many lenders will ask for at least two years' Notice of Assessment (NOA) issued by the CRA. Credit card companies also ask for financial statements and NOAs when opening accounts for new businesses. These financial statements would be prepared as a Notice to Reader, without review or audit provided by CPAs[49]. After loans and credit cards are provided, the thieves will disappear with the money or goods they obtain.

  At first glance, the scheme looks like too much trouble for thieves to go through, but if multiple companies are opened at the same time—especially in different provinces under different owners' names, so that connections are difficult to find—and multiple companies apply for loans with different banks and credit card companies, the proceeds could be significant.

  To prepare financial statements and tax returns, minimal accounting knowledge is required. Also, many un-licensed, non-CPA businesses prepare tax returns based

[49] Research Note. In author's line of work banks and credit card companies were asking for Financial Statements that were not reviewed or audited to open a new bank account, provide loan or issue a credit card in business name.

on information given to them, with few questions asked. (See *Unethical businesses* in Section 1.1).

- **Put fake people on payroll and claim a Scientific Research and Experimental Development (SRED) credit.**[50] When a business pays salaries that are part of an innovation project, the business is eligible to claim a SRED credit and receive as a pay-back part of the salaries. Fraudsters could prepare a SRED claim based on false payroll expenses.[51] In most cases, the CRA will not audit SRED expenses when filed, and the SRED refund will be paid out. If, later, the CRA decides to revisit the SRED claim and ask for additional documentation, the offenders will have disappeared. Since the company was opened under false-owner information, there will not be much that the CRA can do.
- **Purchase inventory or equipment on account.** Another common scheme for "one day companies" [52] is to purchase inventory or equipment on account and disappear with the goods. Even though the business has no credit history, it may develop a very attractive website, and post reviews from many "satisfied customers." It may even lease a room in an office building with an attractive address, so viewers think the business is well-established. This business could apply for credit with suppliers and use friends as references, who claim the company is legitimate. Offenders would open as many credit accounts as possible,

[50] https://www.scientificresearch.ca/about-sred

[51] Research note: This information is from author's experience, working in accounting industry and having experience with preparation of SRED claims.

[52] Research note: "One day businesses" are companies that exist for short period of times.

to gain as much as they can. They could even pay some suppliers for a couple of months to establish trust before disappearing with goods and unpaid accounts.

The business, in most cases, will face no consequences, since it will be long gone, and there is no one to go after them. It would probably cost a supplier more to hire a lawyer and try to locate the business owners than to just write off their accounts receivable and claim bad debt expenses on the unpaid accounts.

- **Claim HST refunds.** When an HST account is newly opened, or re-activated after many years, it is understandable that the associated newly opened, or re-activated business will need to buy machinery, office equipment, computers, autos, and other necessary items for the business to operate, even before revenue starts. Offenders can take advantage of this fact and "purchase" many items with high dollar amounts, and then claim a refund for the HST supposedly paid on these items. Offenders could also add many personal expenses to the HST filing. Usually, the CRA does not audit the first HST return.[53] It may audit subsequent HST returns, particularly when they all show high refund balances, have no review, and show no HST collected from customers.[54] However, by the time the CRA sends review letters, requesting the business to submit documentation for invoices claimed, the offenders will be long gone. The CRA could put a hold on the bank account of the business, but with such businesses, the bank account balance is usually nil. If the business number was new and the business was

[53] Research note: This information comes from the author working with HST auditors, while working in industry.

[54] Research note: This information comes from the author working with HST auditors, while working in industry.

incorporated under a stolen identity, there is nothing much CRA can do. With a legitimate business, the shareholders would be liable to the CRA for the money.

- **Apply for a Canada Emergency Business Account (CEBA).** When COVID-19 started, the Canadian government made monetary payments of $60K as interest-free loans to help businesses through the tough times[55]. There were only two requirements for businesses to receive this support: a bank account and a payroll account that paid salaries of $20K to employees in the prior year. Since this support was paid from April 2020 to December 31, 2022, companies were opened under fictitious names, bank and payroll accounts were opened, and payroll (T4 slips) were filed to fictitious SIN numbers. To file payroll, only T4 slips (renumeration slips) need be e-filed with CRA.
- **Make a cycle of fake business activities, pay salary to the owner, and apply for mortgage or bank loan.** In this scenario, offenders could open businesses, file fake revenue and expenses with the CRA, pay themselves salaries, report salaries, and purchase houses based on that information. This would be a very secure scheme, since the CRA never asks where money comes from[56]. CRA reviews expenses, but not income. Such statements will not go through review or audit. Just the fact that an individual had a corporation that paid him/her a salary reported to the CRA, and the CRA has provided a Notice of Assessment (NOA) makes a bank more willing to provide mortgage- or car financing. Under this scenario, the offender would have everything in her/his name and her/his

[55] https://ceba-cuec.ca/

[56] Research note. In over 20 years of working experience in accounting, I never saw/heard of the request to provide support for revenue received.

mortgage would be paid. The offence would be the posting of fake entries for the corporation.

1.4 Tax Schemes Related to Identity Theft

Tax schemes "attempt to deceive taxpayers by convincing people to pay less than what they owe." [57] They might have these common elements: [58]

- Tax schemes are advertised.
- Tax savings are promised, which often include large returns on small investments.
- A portion of the tax refund is taken by the promoters to cover their fees.
- They are too good to be true.

When related to identity theft, fraudsters might provide tax preparation services to vulnerable people, but collect the benefits. For example:

Income tax preparation

- **Scheme 1: Tax return for vulnerable people.** Consider sick or disabled or elderly individuals in long-term care facilities. Often, such people cannot take care of their finances and may need assistance. Their low income will make them eligible for different benefits and credits, such as the HST credit and low-income assistance. By learning the person's social security number (SIN)

[57] Government of Canada, (https://www.canada.ca/en/revenue-agency/campaigns/tax-schemes.html).

[58] Government of Canada,(https://www.canada.ca/en/revenue-agency/campaigns/tax-schemes.html).

number and DOB, a fraudster could file tax returns on behalf of the person, but provide their own bank account, where benefits will be deposited[59].

Working Income Tax Benefit (WITB) scheme

- **Scheme 2: Working Income Tax Benefit (WITB[60]) scheme:** Promoters of the WITB scheme claim "they can get a tax refund for participants from the working income tax benefit (WITB) even if they have no work income." [61] The WITB is a refundable tax credit intended to give tax relief to eligible low-income individuals and families who are currently in the workforce. An individual that was not employed during the calendar year is not eligible for this benefit. An individual can only claim the WITB if s/he is a Canadian tax resident and is earning income from working in Canada.[62] Under this type of scheme, a fraudster will prepare a T4 slip for the ineligible claimant (a T4 slip is an annual form given to each employee in Canada to record earnings and deductions) from a business that s/he never worked for. The business will be able to deduct the amount listed on the T4 as an expense and, in this way, reduce income taxes, and the individual will be able to receive WITB. The maximum basic amount is $1,381 for single individual. The amount is gradually reduced if an individual's adjusted net income is more than $13,064.

[59] Research note: This information is from author's experience working on personal tax returns and witnessing different schemes.
[60] Research note: In most recent personal tax returns the name was changed to "Low – Income Workers Tax Credit".
[61] Government of Canada, (https://www.canada.ca/en/revenue-agency/news/newsroom/alerts/alerts-2018/warning-working-income-tax-benefit-tax-scheme.html).

[62] Government of Canada,(https://www.canada.ca/en/revenue-agency/news/newsroom/alerts/alerts-2018/warning-working-income-tax-benefit-tax-scheme.html).

Under this scenario two types of fraud are happening. First, a business will deduct salary expenses for the salaries that were never paid and as a result will pay less/or sometimes even no taxes to CRA. Second, the person that never worked will received a T4 slip showing income that will make him eligible to receive WITB credit from CRA. Promoters of the scheme can ask receiver of WITB for some % as their commission.

Wages-to-loan tax scheme

- **Wages-to-loan tax scheme.** [63] Under this tax scheme, promoters/sellers of the scheme tell participants that no tax will be deducted from their salaries if, instead of being paid through payroll with a T4 issued at the end of the year, they are paid with what they are told are non-taxable loans, but what they are told is not true. The target groups for this type of schemes are usually new Canadians since their knowledge of Canadian tax system is limited. (In many European countries, as well as in the former Soviet Union and the Middle East, there are no such things as tax returns, so new immigrants may lack knowledge about tax returns, as well penalties for tax evasion). Also, seniors and students are targets for such schemes. Students are lured in with the promise of being able to "pay down debt by freeing up cash" [64] that usually would otherwise be withheld from their pay cheque and submitted to the CRA. Under this scheme, the promoter will lease a person's services to an

[63] Government of Canada,(https://www.canada.ca/en/revenue-agency/news/newsroom/alerts/alerts-2017/warning-wages-loan-tax-scheme.html).

[64] Government of Canada,(https://www.canada.ca/en/revenue-agency/news/newsroom/alerts/alerts-2017/warning-wages-loan-tax-scheme.html).

employer and employer will pay the promoter what person/worker earned, and the promoter will give worker wages as a tax-free loan less percentage of their fee. [65] These actions will result in tax evasion since promoter will have to deduct all payroll taxes and submit to CRA. Workers are also liable to pay their portion of payroll taxes and withholding and are committing tax evasion.

1.5 Offenders and Victims

This section looks at different kinds of offenders and victims.

Low-frequency offenders[66]

Usually, these are one-time offenders that commit fraud/identity theft in emergency situations. For example, a low-frequency offender could be a parent who opens a utility account in her/his child's name because they have ruined their own credit. These types of offenders are referred to as "crisis responders" since they appear to engage in criminality in response to some type of perceived crisis.[67]

[65] MacMillan Estate Planning Team, (https://www.macmillanestate.com/the-strongroom-blog/are-wages-to-loan-as-good-as-they-sound).

[66] Newman Graeme, McNally Megan M., (July 2005). "Identity Theft Literature Review", (https://www.ojp.gov/pdffiles1/nij/grants/210459.pdf)

[67] Engdahl Oskar, March 18, 2011. "White Collar Crime and Informal Social Control: The Case of "Crisis Responders" in the Swedish Banking and Finance Sector", Scientific Research, (https://www.researchgate.net/publication/228424880_White_Collar_Crime_and_Informal_Social_Control_The_Case_of_Crisis_Responders_in_the_Swedish_Banking_and_Finance_Sector).

Opportunity takers

"Opportunity takers,"[68] as the name suggests, do not consider engaging in criminality day to day, but if or when an opportunity comes up, they will take it. This group would include a cashier who notices a customer leave a credit card and then uses the card to make an unauthorized purchase. Another example would be a person who has a facial but makes a benefit claim for a more expensive massage instead, from a practitioner who is a registered massagist therapist and facial specialist. More examples would be company insiders, including professionals working as employees and managers, or companies receiving outsourced work, who have access to large amounts of sensitive client data. [69] (See section 1.1, *In-house theft,* and *Outsourcing*.)

High frequency offenders

High frequency offenders can be divided into two subgroups: "opportunity seekers" and "stereotypical criminals" [70] Opportunity seekers will try to create a situation in which they can commit an offence. They might initiate calls to potential victims and claim to represent the police, CRA, or other authority, with the goal of extracting money.

[68]Weisburd David, Waring Elin, June 2009. "White Collar Crime and Criminal Careers", Cambridge Studies in Criminology, (https://www.cambridge.org/core/books/whitecollar-crime-and-criminal-careers/6D3DC88DCFCF9FEA7C8D9D9508CDD8E8). The Book can be downloaded from this website.

[69] Weisburd David, Waring Elin, June 2009. "White Collar Crime and Criminal Careers", Cambridge Studies in Criminology, (https://www.cambridge.org/core/books/whitecollar-crime-and-criminal-careers/6D3DC88DCFCF9FEA7C8D9D9508CDD8E8). The Book can be downloaded from this website.

[70] Weisburd David, Waring Elin, June 2009. "White Collar Crime and Criminal Careers", Cambridge Studies in Criminology, (https://www.cambridge.org/core/books/whitecollar-crime-and-criminal-careers/6D3DC88DCFCF9FEA7C8D9D9508CDD8E8). The Book can be downloaded from this website.

Stereotypical criminals would be offenders that frequently commit identity theft, and their activity is not situationally dependent.

Organized crime groups, like scam centres, would fall under this category. (See Section 1.1, *Through financial scams/fraud*.) Now, with COVID-19 lockdowns, some of the scam centres that target Canadians, many in India, have moved into residential apartments, making them virtually impossible to detect or stop.[71]

Most common justifications given by identity thieves[72]

The most common excuses given by identity thieves, when they are caught, are explained below. They are: denial of injury, appeal to higher loyalties, justification by comparison, sad stories, and denial of victim.

- **Denial of injury.** Under this justification, thieves claim that no actual harm/injury was experienced by victims. Thieves take the approach that an identity was not stolen, but some part of it was borrowed.
- **Appeal to higher loyalties.** Thieves claim that crimes were committed to help others and that is why they are justifiable. They shift the blame away from themselves to bad circumstances, saying they had no choice but to commit the crime to help their family or others.

[71] Miller, Harry, March 20, 2021, "As COVID surged, Indian police shut down scam centres targeting Canadians. Now, they're back – CBC.ca," *Canada News Media* (https://canadanewsmedia.ca/as-covid-surged-indian-police-shut-down-scam-centres-targeting-canadians-now-theyre-back-cbc-ca/).

[72] Copes Heith, Vieraitis Lynne M., Septembre 2009. "Understanding Identity Theft Offenders' Accounts of Their Lives and Crimes", Criminal Justice Review Volume 34 Number 3, (https://journals.sagepub.com/doi/10.1177/0734016808330589). Please note I accessed this document through University of Toronto Library.

- **Justification by comparison.** Under this justification, thieves claim that their crimes are not as bad as other crimes, so they should not be punished in the same way as, e.g., sex offenders or murderers. Also, they would ask why they are being punished for stealing, say, $5K, while a corrupt politician can escape justice after stealing or giving out grants or contracts worth $5M.
- **Sad tale.** Under this justification, thieves try to explain that they are good and honest people, but something bad happened to them, and they had no other choice, except to commit crimes to improve their situation. The stories can vary from losing jobs and having no money to paying their mortgage to someone to being ill and needing expensive drugs.
- **Denial of victim:** Under this scenario, thieves claim that there is no actual victim since people were reimbursed by insurance or credit card companies.

Problems experienced by victims of identity theft[73]

Victims of identity theft may experience several problems and issues. For example:

- **Time and monetary costs.** Recovery from all of the issues identity theft creates can take time, starting with filing a police report, calling banks and locking accounts, closing/blocking credit cards, notifying credit agencies and trying to remove accounts from the credit report that scammers may have opened in the victim's name. The amount of time spent can range from hours for calling credit card companies to many months, if loans or mortgages were

[73]Newman Graeme, McNally Megan M., (July 2005). "Identity Theft Literature Review", (https://www.ojp.gov/pdffiles1/nij/grants/210459.pdf)

taken in the victim's name or if another identity was created by using some of the victim's information. Victims of identity theft will incur additional costs if, for example, they need to hire a lawyer, accountant or other professional to deal with the consequences of identity theft.

There is no single, comprehensive written guidance on the steps required if a person becomes a victim of identity theft, but Section 2.3 outlines steps to take.

- **Opportunity costs.** Victims may not be able to obtain a job or purchase a house or car, and can even lose a job, if some clearance is required but, because of the identity theft, this clearance cannot be given. For many positions, especially in financial institutions, a financial check is required. Having issues with collection agencies, even if someone else opened a loan in the victim's name, can create problems that could prevent the victim from getting a job. Because credit scores decrease when new loans carry high unpaid balances, victims cannot apply for additional loans and must wait until their scores are repaired again. That can take some time, since some financial institutions are not eager to write off losses and close accounts.
- **Requirement to prove fraud**[74] by some of the financial institutions can lead to additional delays and can lead to more theft and losses to victims.

[74] Wright Rosalind, March 1, 2002. "The Hiding of Wealth: The Implications for the Prevention and Control of Crime and the Protection of Economic Stability", Journal of Financial Crime Volume 9 Issue 3, (https://www.emerald.com/insight/content/doi/10.1108/eb026022/full/html). Please note that this is a link to the article, but article for research was downloaded from University of Toronto Library.

Normally, financial institutions will have to absorb losses associated with identity theft, but to avoid them, a "requirement to prove fraud"[75] requires victims to prove that fraud was committed and that losses were suffered because of it, not because the victim was careless with their PINs and other personal information, for example, by choosing a simple PIN or sharing a password with family or friends.

- **Communication issues.** For some victims of identity theft, a big issue is finding a "live" person to communicate with, not just an answering machine. When identity theft occurs, the victim needs to contact all financial institutions, where s/he has accounts, to contact credit bureaus, and each institution has their own forms and processes to be followed when identity theft occurs. Some victims report difficulty in finding out about and getting help with filling out the correct forms, and a lack of support from the organizations.
- **Agency-inflicted suffering.** Harassment by collectors, rejection for a loan or insurance policy, having utilities cut off, having a lawsuit filed against them, having a criminal investigation started or a warrant issued for their arrest, may be suffered by victims in severe identity theft cases, for example, when another person assumes their identity for some time. Collection agencies will try to collect the money from the person whose name they have, even if it is not the same person who took out the loan/mortgage in the first place. Victims

[75] Vail Brian, July 2018, Case Summary: Du v. Jameson Bank, (https://www.fieldlaw.com/News-Views-Events/133814/Case-Summary-Du-v-Jameson-Bank).

can be forced to go to court—sometimes in a different province or state—to have some of the claims against them withdrawn or to clear their records.

Victims may not report identity theft

The publicly available data on identity theft comes mainly from survey research, due to following reasons. One is that some of the crimes that fall under identity theft are treated differently by victims and law enforcement than other crimes. For example:

- **Victims do not always go to the police.** In the case of credit card fraud, charges are reversed, so no damages can be reported.
- **Victims often discover the theft long after it occurred.** Nowadays, with transactions visible in real time, victims of credit card fraud should find out about it quickly. But if victims rely on monthly statements and/or do not review them, or if other accounts or loans are opened in a victim's name, learning about the fraud could take a long time, perhaps only when the mortgage is in default, the bank account has a negative balance, credit cards have high balances, or collection agents are calling. By that time, offenders are long gone, and victims are left to deal with the consequences of restoring their credit history and credit accounts.
- **People are ashamed to admit to identity theft.** We often hear news about scammers and scams. Scammers can be tough and convincing, even to me, the author, a CPA, who knows that I do not owe any money to CRA and that police cannot come and arrest me. So, people who still fall victim to scammers are ashamed to admit it.

- **Under the damage threshold.** To start an investigation, damages should be over $5,000. Some of the scammers deal below that amount to avoid being charged.[76]
- **Chances of finding offenders/getting funds returned are low.** Filing a police report takes a long time, and the chances of finding offenders and getting money returned are almost zero. (Please see interview #4 with Dwayne King, former Police Officer). Many offenders call/work outside Canada, outside the jurisdiction of Canadian police. (See inset example.)

Example: A Trans-national Fraud

At my (the author's) previous place of employment, one of our accounting clients, instead of calling us to verify what he was told, was scared into transferring his tax balance in the form of prepaid (virtual) Apple cards (along with the PINs) to offenders pretending to be "the CRA."

This client tried to make us reimburse his loss, since he claimed that we did not let him know about the taxes owing. After we (accountants) discovered the fraud and tried to take the Apple cards back for the client, the balance was nil on all cards.

We also called the CRA and confirmed that no taxes had been owed. He had been scammed.

[76] Research note: Some of the author's company's clients reported that they were turned away by police when they reported lower amounts in damages. They were told to file the claim with their financial institutions and opening a case was refused.

Financial institutions may not report identity theft

Many financial institutions and other companies that handle personal information may not report identity theft for several reasons:[77]

- **Some companies are in business of collecting and selling information on individuals.** In Canada, there is Personal Information Protection and Electronic Documents Act (PIPEDA), that governs how private-sector companies can collect, use, and disclose personal information.[78] But there are many loopholes that companies can use to sell personal information.

  When working on this research paper, the author could not confirm that this or another law in Canada would prohibit a company from selling personal information or would require a company to disclose that it might be sold to another company. (See inset example.)

Example: Could Simple Questions Lead to Complex Problems?

When people go to a builder's office to check for new houses, or go to realtors' open houses, they are asked to provide their name, address, type of home they are looking for, and other personal information.

They do not consider what might happen with the information, and they do not sign a confidentiality agreement.

Could this information on potential new home buyers be sold to other realtors or builders?

[77] Melendez Steven and Pasternack Alex, March 2, 2019. "Here are the data brokers quietly buying and selling your personal information", Fast Company Journal, (https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information).

[78] Office of the Privacy Commissioner of Canada, (https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/).

The author could not confirm that a law in Canada (even the Personal Information Protection and Electronic Documents Act) would prohibit selling of this information or require a company to disclose that it might be sold.

Companies that collect information claim they need it for marketing purposes. If such companies were to report identity theft, or report any data loss, they would open themselves to lawsuits. That is why nothing is reported.

- **Stockpiled consumer information.** Massive databases are maintained by credit agencies, telecommunications companies, and others, for targeted advertising and sharing arrangements among companies. These companies are not required to inform individual consumers when their information is sold or stolen. In many cases, individual consumers, employees, or others are blamed for their own victimization, but the systems or the industries that make them such easy targets are seldom re-evaluated.[79]
- **Require redesign, not fines**. Fines do not address the problem of data stockpiling and exchange among companies. Instead of fines, redesign of information architectures, to ensure anonymity and confidentiality at every step of data generation and circulation, should be required.

[79] Melendez Steven and Pasternack Alex, March 2, 2019. "Here are the data brokers quietly buying and selling your personal information", Fast Company Journal, (https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information).

- **Costs are concealed.** Financial institutions report costs associated with identity theft and other frauds under costs of goods sold (COGS) and these costs are treated as part of doing business. One of the reasons it is done, is that financial institutions do not want shareholders and anyone else to see, that entity had/has any association with identity theft. This will be bad for business and reputation[80].

1.7 Increased Identity Theft Because of COVID-19

This section provides sample media coverage showing how the pandemic has affected identity theft.

Case 1: "Stimulus Programs Draw a Flood of Scammers[81]

This case took place in U.S. but is relevant to Canada since identity thieves steal people's information to receive payments from governments (either Canadian or American). These payments became available as part of stimulus packages when the COVID-19 epidemic started.

This article is about trillions of dollars in stimulus funds that created a rush among criminals to take the money from those who needed it the most. In this case, a scammer had claimed a family's $3,400 stimulus cheque. When the victim went to the Internal Revenue Service (IRS) website to check on the status of her family's stimulus funds, she learned that someone else had filed taxes on her husband's behalf and had used his identity to obtain their $3,400 payment. COVID-19 has made it even easier for fraudsters

[80] Research note: When working as auditor author observed expenses related to identity theft and other frauds being reported as either cost of goods sold or being part of administrative expenses.
[81] New York Times, September 15, 2020, (https://www.nytimes.com/2020/04/22/technology/stimulus-checks-hackers-coronavirus.html).

to get information. Many are bombarding Canadians and Americans with e-mails and phone calls that use the uncertainty around the virus to distribute malware and to get people to divulge their bank information and other data,[82] which can then be used to defraud the same people. Google reported it intercepted 18 million such emails in early April, 2020.[83]

Case 2: "Canadians Have Lost More Than $1.2 Million to COVID-19 Scams"[84]

Con artists from all around the world are preying on the anxious. "Hundreds of Canadians have received text messages and e-mails from scammers trying to cash in on the COVID-19 pandemic…[and] Canadians have lost more than $1.2million in recent weeks to scammers taking advantage of the COVID-19 pandemic,"[85] CBC News reported.

The article continued, saying that "Jeff Thomson of the Canadian Anti-Fraud Centre said the centre has received 739 reports since March 6 [2020] of attempts to defraud Canadians with scams related to the pandemic. He said 178 of those attempts succeeded."

Scammers are using pandemic to infect victim's computers with malware. "…[V]ictims …receive messages telling them they have been exposed to someone who has tested

[82] Dilanian Ken and Saliba Emmanuelle, March 12, 2020, "Coronavirus scammers are seeking to profit off the deadly virus", NBC News, (https://www.nbcnews.com/news/us-news/coronavirus-scammers-are-seeking-profit-deadly-virus-n1156126).

[83] Tidy Joe, 17 April 2020. "Google blocking 18m coronavirus scam emails every day, BBC News Magazine, (https://www.bbc.com/news/technology-52319093).

[84] Thompson Elizabeth, Nicholson Katie and Ho Jason, May 1, 2020, CBC News, (https://www.cbc.ca/news/politics/covid-scams-fraud-crime-1.5551294).

[85] Thompson Elizabeth, Nicholson Katie and Ho Jason, May 1, 2020, CBC News, (https://www.cbc.ca/news/politics/covid-scams-fraud-crime-1.5551294).

positive for COVID-19 and [asks] them to fill out what looks like an Excel form." When this form is open, "…it infects user's computer with Trojan downloader that installs malicious files…"[86]

Case 3: Krebs on Security, "How Cybercriminals are Weathering COVID-19"[87]

This article describes in how many ways the COVID-19 pandemic has been a boon to cybercriminals.[88] People working from home present a target: a rich environment for cybercriminals because of vulnerabilities that accompany remote work. Home networks are easy to target compared to the high-end network infrastructures at workplaces. Because employees' home networks are being attacked, confidential information that belong to organizations is being leaked.

Section II: Recent Developments in Protection of Personal Confidential Data

> *Let us answer the question, what is being done to protect against identity theft?*

Given the latest and more sophisticated schemes, people and organizations need to protect themselves against identity theft. Some may think that protection measures are

[86] Thompson Elizabeth, Nicholson Katie and Ho Jason, May 1, 2020, CBC News, "Canadians have lost more than $1.2 million to COVID-19 scams",(https://www.cbc.ca/news/politics/covid-scams-fraud-crime-1.5551294).

[87] Clerix Kristof, April 30, 2020, Krebs on Security In Depth security news and investigation, (https://krebsonsecurity.com/2020/04/how-cybercriminals-are-weathering-covid-19/).

[88] Shomiron Das Gupta, April 30, 2020, "Coronavirus pandemic A boon for cybercriminals", (https://www.moneycontrol.com/news/technology/coronavirus-pandemic-a-boon-for-cybercriminals-5123001.html).

too costly, and some do not take identity theft seriously enough. But the price of not taking steps to protect against identity theft can be even higher.

As with other crimes, identity theft might be impossible to eliminate. With the increased use of the Internet for day-to-day banking, working from home, posting stories on the social media websites, and sharing information through e-mail, etc., thieves will find ways to steal this information, because of the low chance of being caught and prosecuted. Given these facts, individuals and organizations need to find ways to reduce the chance of identity theft happening to them. This section explores different methods that individuals and organizations can use to decrease identity theft. [89]

2.1 What Individuals Can Do to Reduce Identity Theft

- **Increase the effort the offender must make to commit identity theft.** Some of the crimes are committed because people do not take security and Internet security seriously. Security is not just about expensive firewalls on personal computers, but simple efforts to protect passwords. For example, make passwords/PINs more challenging to guess (e.g., no obvious names or dates), and protect them (e.g., no sticky notes next to computers; or allowing devices to remember them). Only send personal information through e-mail in password-protected PDFs, and shred important documents or request that all bank and other statements be in electronic format.

[89] Newman Graeme, McNally Megan M., (July 2005). "Identity Theft Literature Review", (https://www.ojp.gov/pdffiles1/nij/grants/210459.pdf)

- **Reduce temptation.** Many identity theft crimes happen because people provoke thieves by putting their wealth on public display. There is a Russian saying, "People ask to be robbed."[90] Used mostly when talking about house break-ins, this saying can be used today in relation to peoples' online and offline behaviour. People like to show how well-off they are, even if it is not true. This behaviour attracts ordinary and online criminals. To prevent this attention, people should not provoke thieves by showing their wealth.
- **Do not use Visa Debit or Debit Mastercard linked to line-of-credit accounts online.** People without credit cards can use Visa Debit or Debit Mastercard cards to make purchases on the Internet. Sometimes these cards are linked to line-of-credit- or savings accounts with high balances. The difference between these cards and regular credit cards is that if thieves make a purchase using a stolen credit card, the purchase can be disputed, and money will likely be returned to the credit-card holder, or the transaction will be cancelled. When purchases are made through Visa Debit or Debit Mastercard, money is immediately taken from the linked account, and banks are not very willing to reimburse it. Credit card companies are insured, so the insurance company will pay the amount of the fraudulent transaction. Purchases made with Visa Debit or Debit Mastercard are not insured, and the bank will argue that purchaser did not protect her/his debit card information properly.[91] If these cards are used, they should be linked to an

[90] Researchers Note: Author was born in Soviet Union, and in 1990, this was a famous saying.

[91] Researcher Note: We had a client that was a victim of $11,000 purchase using his debit Visa card. The card was linked to his line of credit account and bank never repaid money on this transaction, arguing the victim's PIN was easy to guess and the card information was not properly protected.

account with a limited amount of money and only the daily limit should be used on the card.

- **Reduce online presence.** People share too much personal information online through the social media websites. A thief can easily collect information and duplicate the identity of an individual. People's online presence should be reduced to prevent this from happening.

- **Be careful to whom personal information is provided.** Personal information should not be provided over the phone. First, if someone calls from a known organization, they should have the information they are asking to verify. Second, if there is a doubt that the caller is from the organization, then hang up, dial the organization, and talk to customer service.

- **Clear devices before discarding.** Before disposing of old laptops, cell phones and other electronic gadgets, hard drives must be cleared or reformatted, so that information cannot be reproduced by a knowledgeable IT specialist.

- **Check government websites periodically.** Check CRA personal/business accounts periodically to make sure nothing was filed by someone else and that personal information on file has not been changed.

- **Monitor credit scores regularly.** Regularly check the websites or subscribe to credit monitoring services (e.g., offered by Equifax[92] and TransUnion). By subscribing, individuals will be notified immediately if a credit score request is made on their account or if a new account is opened in their name. By getting this

[92] Equifax Website, (https://www.equifax.com/personal/).

information sooner than later, individuals may be able to prevent fraud from happening.[93]

- Install security software. E-mail filtering, anti-virus, and anti-spyware software will scan a computer and report suspicious activity. For this software to effective, the latest updated versions must be installed.[94]

2.2 What Businesses Can Do to Reduce Identity Theft

- **Banks should adopt protocols to detect the signs of a scam.** Banks in Canada need to adopt protocols and employ staff that are specially trained to detect the warning signs of a scam (e.g., unusual withdrawals). They need to contact customers to warn them that they are potential victims, and direct them to call police or the bank itself. Such a banking protocol has been successful in the U.K.,[95] so Canada would benefit from a similar approach.[96]
- **Financial institutions should report identity theft.**[97] To improve awareness and protection measures, financial institutions should collect statistics on the:

---

[93] Steinberg Scott, February 27, 2020, CNBC, (https://www.cnbc.com/2020/02/27/these-are-the-latest-ways-identity-thieves-are-targeting-you.html).

[94]Steinberg Scott, February 27, 2020, CNBC, "There are the latest ways identity thieves are targeting you", (https://www.cnbc.com/2020/02/27/these-are-the-latest-ways-identity-thieves-are-targeting-you.html).

[95] Miller Harry, March 20, 2021, CBC News, "As COVID surged, Indian police shut down scan centres targeted Canadians. Now, they're back",(https://canadanewsmedia.ca/as-covid-surged-indian-police-shut-down-scam-centres-targeting-canadians-now-theyre-back-cbc-ca/).

[96] Miller Harry, March 20, 2021, CBC News, "As COVID surged, Indian police shut down scan centres targeted Canadians. Now, they're back",(https://canadanewsmedia.ca/as-covid-surged-indian-police-shut-down-scam-centres-targeting-canadians-now-theyre-back-cbc-ca/).

[97] Hoofnagle Chris Jay, Fall 2007. "Identity Theft: Making the Known Unknowns Known", Harvard Journal of Law & Technology, (https://jolt.law.harvard.edu/articles/pdf/v21/21HarvJLTech097.pdf).

- **Number** of identity theft incidents suffered and avoided and steps that could be taken to avoid/reduce/eliminate such incidents.
- **Forms** of identity theft attempted, and the financial products targeted, in order to better protect these products.
- **Losses** suffered or avoided.

Such reporting would improve general understanding of identity theft and enable financial institutions and policymakers to tailor preventive measures to reduce severity and methods of the crime.[98] Such reporting could create a market for identity theft prevention, since financial institutions would then have incentives to offer the safest products.

- **Deal with identity theft in the workplace.** Organizations should establish protocols and procedures to handle allegations of identity theft in the workplace. When misconduct is reported, the management team must investigate and report its findings, and internal processes need to be developed/improved based on the findings.[99] Senior management and other officers at the top of the organization are responsible for communicating and upholding the message that all employees will be required to act within the company's ethical code of conduct. To deter fraud,[100]

[98]Hoofnagle Chris Jay, Fall 2007. "Identity Theft: Making the Known Unknowns Known", Harvard Journal of Law & Technology, (https://jolt.law.harvard.edu/articles/pdf/v21/21HarvJLTech097.pdf).

[99] Association of Certified Fraud Examiners, "How management can prevent fraud in the workplace",(https://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/tone-at-the-top-research.pdf).

[100] Code of business Conduct and Ethics, (https://www.sec.gov/Archives/edgar/data/1094007/000119312504044901/dex14.htm).

they must be clear in communicating that identity theft and other crimes will not be tolerated, and offenders will be reported to police.

- **Safeguard information.** [101] Information of employees and customers should be encrypted so that, even in the case of a security breach, no information will be lost. Only limited information should be accessible by any employee. This way, employees will have less motivation to obtain or sell information. To protect taxpayers, for example, CRA employees cannot see full information on an individual, just pieces that cannot be used alone to identify or compromise an identity.[102] All paper documents that contain sensitive information about the customers should be shredded, not just thrown away in a recycling bin.
- **Make work from home more secure.** During the COVID-19 pandemic, many employees worked from home, and many organizations may continue to allow employees to work from home, after stay-at-home orders end.[103] These employees have access to a variety of sensitive information. It is the responsibility of the organization to protect this information and to ensure that stiff penalties and termination will follow if employees share it. Also, organizations need to invest in IT security and to give all employees company laptops and mandatory access to a virtual private network (VPN). A VPN allows an individual "…to create a secure [encrypted] connection to another network over the Internet. VPNs can be used to

[101] Newman Graeme, McNally Megan M., (July 2005). "Identity Theft Literature Review", (https://www.ojp.gov/pdffiles1/nij/grants/210459.pdf), p 70.

[102] Researcher Note: The author calls the CRA on the daily basis and is aware of this process.

[103] Research note: Information is taken from the articles in magazines and from Deloitte (where the author works), which will allow employees to continue working from home, as long as they work in Canada.

access region-restricted websites, shield…browsing activity from prying eyes on public Wi-Fi, and more."[104] By providing company laptops, and disallowing personal ones organizations will reduce the risk of employees accidentally or purposely sharing company information.

- **Increase the risk of getting caught.**[105] When employees in an organization or thieves outside an organization know that their online activities can be monitored, and the organization's security team can find their location and identity, they will not try and steal from that organization, because their risk of being caught will increase. Small companies without a budget to maintain their own security department could outsource to a reputable security agency, which could monitor Internet activities on the company's behalf.
    - **Educate customers and employees.** Organizations could provide customer and/or employee training and increase awareness[106] of online identity theft, financial fraud, the need for online security, and ways to safeguard information.

[104] Hoffman Chris, October 15, 2020, "What is VPN, and Why Would I Need One?", How to Geek Newsletter. (https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/)

[105]Newman Graeme, McNally Megan M., (July 2005). "Identity Theft Literature Review", (https://www.ojp.gov/pdffiles1/nij/grants/210459.pdf), p70.

[106] Ruchika Jha, 'Identity theft: Is it a modern crime?' (*Law Times Journal*, 14 March 2020) (http://lawtimesjournal.in/identity-theft-is-it-a-modern-crime/).

2.3 Steps to Take by Victims of Identity Theft

While there is no single, comprehensive written guidance on the steps required if a person becomes a victim of identity theft, Internet sources are easy to find. One source[107] advises taking these steps:

- **Obtain a credit report.** Check for unauthorized inquiries and unauthorized new accounts. Call financial institutions to remove these new accounts.
- **File an identity theft report with police.** This report is one of the first steps toward credit recovery. It is required (as proof that identity theft occurred) in dealing with financial institutions to have them remove unauthorized new accounts discovered in the credit report (above).
- **File police report (above) with all creditors.**
- **Put a fraud alert on credit reports.** A fraud alert notifies companies that the victim's identity was stolen. It requires businesses to verify the person's identity before a new credit is issued, to prevent fraudulent activity. This alert lasts for up to seven years, depending on the credit agency/bureau and length of alert chosen. Canada has two credit bureaus, TransUnion and Equifax[108].
- **List fraudulent activities.** Compare credit reports from different credit bureaus. Compile a list of new unauthorized accounts and forward it to each credit bureau.

---

[107] Steinberg Scott, February 27, 2020, CNBC, "There are the latest ways identity thieves are targeting you", (https://www.cnbc.com/2020/02/27/these-are-the-latest-ways-identity-thieves-are-targeting-you.html).

[108] Rennie, Lisa and Wood, Caitlin., "What is a Credit Bureau?" *Loans Canada [blog]* ((https://loanscanada.ca/credit/what-is-a-credit-bureau/).

- **Call creditors.** Speak with fraud departments of creditors to make them aware of any fraudulent application(s) and to stop all new, unauthorized applications from being processed. Send police report and contacts to each fraud department.
- **Be patient.** After taking those steps, allow some time to pass to repair the damage. Recovery from identity theft can take weeks or even months.

Section III: Principal Roles of IFAs Against Identity Theft

Let us answer the question: What can an IFA do to assist in the fight against identity theft?

IFAs have many roles in the fight against identity theft. They have special expertise and can work with industry as external investigators/consultants, internal investigators, or with the courts.

3.1 IFA Expertise

Management and those charged with governance[109] have the responsibility for oversight and setting objectives for targeted activities and the entity as a whole.[110] Objectives are

[109] 'Those charged with governance' is a term used for officers of an organization responsible for ensuring the achievement of objectives and held to account for the organization's activities.

[110] U.S. Government Accountability Office (U.S. GAO). "Standards for Internal Control in the Federal Government",.(http://www.gao.gov/assets/670/665712.pdf). Page 41

set by management before designing the internal control system,[111] and this is where IFAs come in. As an old saying goes, "failing to plan is planning to fail."[112] IFAs are encouraged to ensure that their work is adequately planned.[113]

IFAs are specialists in managing fraud risks, and they do so differently from an internal auditor: the IFA is skilled in assessing risks, concerns, or allegations of fraud or other illegal or unethical conduct.[114] Furthermore, as allies, IFAs can provide expertise to audit committees and financial statement audit teams,[115] and can advise companies on how to avoid the risk of being associated with fraudulent activity.[116]

3.2 IFA Role of External Investigator/Consultant

When working on fraud engagements as an external investigator or consultant,[117] IFAs can develop a set of procedures that can help with fraud risk prevention, detection, investigation, and corrective action.

---

[111] Ibid.

[112] Variously attributed to many authors, including Benjamin Franklin.

[113] The Canadian Institute of Chartered Accountants (CICA). (2006, November). Standard Practices For Investigative and Forensic Accounting Engagements.

[114] The Canadian Institute of Chartered Accountants (CICA). (2006, November). Standard Practices For Investigative and Forensic Accounting Engagements. Page 2.

[115] AICPA Forensic and Litigation Services Committee and Fraud Task Force. (2004). FORENSIC SERVICES, AUDITS, AND CORPORATE GOVERNANCE: BRIDGING THE GAP.

[116] Marron, K. (2002, July 22). "Forensic accounting steps into limelight". Retrieved from The Globe and Mail, (https://www.theglobeandmail.com/report-on-business/forensic-accounting-steps-into-limelight/article25301452/).

[117] Richards David A., Melancon Barry C., Ratley James D., "Managing the Business Risk of Fraud: A Practical Guide", Institute of Internal Auditors, (https://na.theiia.org/standards-guidance/Public%20Documents/fraud%20paper.pdf).

In fraud risk prevention

IFAs use their knowledge, experience, and education to

- develop a plan to combat identity theft in an organization, and
- interpret the impact and efficiency of the plan on an organization.

This is done by reviewing existing incidents of identity theft and designing recommendations and procedures that decrease/eliminate future incidents. To justify recommendations, IFAs can present a clear picture of financial impacts and potential savings, which are the most convincing arguments for organizations to change their current practices.

What follows is how IFAs educate employees and design procedures to prevent fraud.

In educating employees[118]

Materials, training, and seminars could be prepared by IFAs. Materials should emphasize employees' obligations to make honest use of corporate information; that is, by using it only for work-related purposes and to serve clients. They should state that stealing, selling, and providing client information to anyone outside the organization can result in termination of employment and may constitute a criminal offence. Employee communication materials should include clear references to the impact of fraudulent activities on the reputation and cost of doing business in the organization. (See inset example.)

[118] Richards David A., Melancon Barry C., Ratley James D., "Managing the Business Risk of Fraud: A Practical Guide", Institute of Internal Auditors, (https://na.theiia.org/standards-guidance/Public%20Documents/fraud%20paper.pdf).

Example: What Employees Need to Know About Identity Theft

Nowadays, since everything is interconnected, and information posted on one side of the globe appears on the opposite side in a matter of seconds, employees need to understand the impact of their actions on their organization.

Employees need to understand the problem of identity theft and its impact on

- reputation of the organization
- monetary loss due to fraudsters stealing money by using another identity, and
- potential lawsuits from clients.

Materials, training, and seminars could be prepared by IFAs, but communication of the whole picture should come from the top leader of the organization, so that employees understand how their work protocols and following the rules can impact the organization they work for.

In addition, a whistleblowing telephone line and email address to report internal fraud/misappropriation of information should be present and working in every organization. Whistleblowing presents another way of preventing fraud and abuse of information by employees. (For more information, see Section 3.4.)

In designing procedures to prevent fraud

Reducing the vulnerability of an organization to possible fraud and selling of the organization's data to others requires a plan to re-design some procedures. For example, an IFA can work together with an IT team (if the organization is too small for its own IT team, IT security can be outsourced) to design procedures that employees and customers need to follow to safeguard information. The organization's website should be designed so that it does not remember customers' credit cards after a transaction is completed. This way, even in case of a security breach, credit card information cannot be stolen. By modifying information storage, it is possible to protect the integrity and security of the information.

An IFA can also help to design the internal IT system and incorporate segregation of duties. For example, employees will have access only to the information that they need to perform their work and clients' personal information should not be visible, just the client's name, or client number. In this way, personal information cannot be sold to marketing- or contact-list companies, and clients will not become targets of advertising campaigns or fraud. (See Sections 1.1 and 2.2.)

Challenges for Plan Design & Implementation

The plan and procedures will work if they are implemented properly and the organization follows them, rather than just recording the existence of a plan in meeting minutes to appease shareholders.

The tone at the top is especially important, as well. Corporate officers must lead by example and follow the plan themselves, so employees will continue to implement and follow the plan[119].

[119] Association of Certified Fraud Examiners, "How management can prevent fraud in the workplace", (https://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/tone-at-the-top-research.pdf)

In fraud risk detection

Fraud within the company and abuse of clients' personal information happens in a variety of ways, and schemes are constantly evolving. A prevention strategy is mandatory for organizations to avoid loss of reputation and lawsuits. To develop the strategy, the IFA uses effective mechanisms and procedures for detecting and intercepting fraudulent activities, based on an adequate risk analysis. The credibility brought by the presence of a forensic accountant is valuable in convincing employees not to go ahead with their fraudulent schemes. The investigation of fraud, especially cases where collusion is involved, requires the IFA to show a great deal of creativity in the methods used to prove the scheme and to prevent it from occurring in the future. By correctly identifying areas at risk, the IFA can target the organization's usually very limited investigative resources to those areas.

In fraud investigation and corrective action

When fraud takes place in an organization, IFAs can use their knowledge and experience to investigate fraud, find guilty parties and collect evidence against them. After documentation is gathered and evidence is obtained, the IFA performs interviews with employees to gain added support for findings. IFAs will report on findings, perform root cause analysis with relevant stakeholders and process owners, update controls and policies, and liaise with relevant departments to communicate changes. For example, if fraud risks are found in human resources (HR) processes, changes can be documented in HR policies and communicated during employee orientation programs. Corrective actions would usually be taken by the employer or police.

3.3 IFA Role of Internal Investigator[120]

When working as an internal investigator, as part of an organization, an IFA can develop a set of procedures that can assist in fraud risk governance, assessment, and prevention.

In fraud risk governance[121]

Prepare the fraud risk management program to include the expectations of those charged with governance, the organization's ethical culture and values, as well as best regulatory practices or codes. A multidisciplinary approach is recommended in addressing fraud risks by having many departments/personnel within an organization participate (see Table 1).

[120] Richards David A., Melancon Barry C., Ratley James D., "Managing the Business Risk of Fraud: A Practical Guide", Institute of Internal Auditors (https://www.acfe.com/uploadedfiles/acfe_website/content/documents/managing-business-risk.pdf).

[121] Richards David A., Melancon Barry C., Ratley James D., "Managing the Business Risk of Fraud: A Practical Guide", Institute of Internal Auditors, (https://na.theiia.org/standards-guidance/Public%20Documents/fraud%20paper.pdf).

Table 1: A Multidisciplinary Approach to Addressing Fraud Risks[122]

Department Personnel to Include	*Why Necessary to Include*
Accounting and finance personnel	To leverage their familiarity with accounting processes and control.
Non-financial business units and operations personnel	To leverage their knowledge of day-to-day operations, customer and vendor interactions, and issues within the industry.
Risk management personnel	To ensure that the fraud risk assessment process integrates with the organization's risk management program.
Legal and compliance personnel	To identify risks associated with potential criminal and civil liabilities if fraud occurs.
Internal auditors	To leverage their intimate familiarity with controls and monitoring functions.
Internal expertise or external consultants	To include expertise in standards, key risk indicators, anti-fraud methodology, control activities, and detection procedures.
Management including senior management, business unit leaders, and appropriate others	To include those ultimately responsible for the effectiveness of the organization's fraud risk management efforts.

In fraud risk assessment

"To protect itself and its shareholders…from fraud, an organization should understand fraud risk and specific risks that…apply to it.[123] An IFA can help to structure fraud risk assessment that will be tailored to the organization's size, complexity, and goals. This assessment should be performed and updated periodically. This fraud assessment can be

[122] The info is from The Institute of Internal Auditors, AICPA, and ACFE, [n.d.], "Managing the Risk of Fraud: A Practical Guide", (https://na.theiia.org/standards-guidance/Public%20Documents/fraud%20paper.pdf), p. 22.

[123] The Institute of Internal Auditors, AICPA, and ACFE, [n.d.], "Managing the Risk of Fraud: A Practical Guide", (https://na.theiia.org/standards-guidance/Public%20Documents/fraud%20paper.pdf or https://www.acfe.com/uploadedfiles/acfe_website/content/documents/managing-business-risk.pdf), p. 8.

integrated with overall organizational risk assessments or can be performed separately, but should include risk identification, risk likelihood and risk response.[124]

Fraud risk identification

This should include an assessment of the incentives, pressures, and opportunities to commit fraud. Employees can be involved in different schemes (see inset example). When working as internal investigator, the IFA will be able to help prevent these schemes/frauds from occurring.[125]

Example: Employee Schemes that an IFA Can Help Prevent

Employees can be involved in different schemes that an IFA can help prevent:

- **Asset misappropriation.**[126] Employees steal the organization's resources, such as cash, electronics, and other assets. The IFA can help assess organization vulnerability and make stealing hard/impossible.
- **Billing schemes.** [127] Employees present fake bills to the organization for payment. The IFA can help in assessing controls that should be in place to prevent billing schemes.
- **Corruption.** [128] Employees use their position in the organization for personal gain. The IFA can help assess transactions that require personal influence to be completed (e.g., real estate purchases or building approvals) and can help propose ways to limit employees' influence.

[124] The Institute of Internal Auditors, AICPA, and ACFE, [n.d.], Managing the Risk of Fraud: A Practical Guide (https://na.theiia.org/standards-guidance/Public%20Documents/fraud%20paper.pdf or https://www.acfe.com/uploadedfiles/acfe_website/content/documents/managing-business-risk.pdf), p. 8.

[125] Report to the nations, 2020 Global Study on Occupational Fraud and Abuse,(https://acfepublic.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf).

[126] Gordon Daphne, October 10, 2019. "Understanding the 3 types of occupational fraud", CPA Canada Website, (https://www.cpacanada.ca/en/news/atwork/2019-01-10-types-of-occupational-fraud).

[127] AGA Website was visited for the information on different types of schemes. (https://www.agacgfm.org/Tools-Resources/intergov/Fraud-Prevention/Tools-by-Fraud-Type/Billing-Schemes.aspx).

[128] Association of Certified Fraud Examiners, Modul 13, "Corruption", (https://www.acfe.com/risk-assessment-m13.aspx).

Fraud risk likelihood

An IFA can review "…employee incentive programs and the metrics on which they are based [and will be able to] provide a map to where fraud is most likely to occur."[129] The IFA's "[f]raud risk assessment should consider the potential override of controls by management as well as areas where controls are weak or there is a lack of segregation of duties."[130]

Fraud risk response

The IFA can assist in preparing procedures in response to fraud risk, such as termination of employees and management, bringing legal actions against guilty parties, and communicating the message to management and employees that fraudulent behaviours will be uncovered and punished.

3.4 IFA Roles with the Courts[131]

There are two alternatives for the use of IFA services in pending litigation: as a litigation consultant and as an expert witness. An IFA should not accept an engagement to perform both services, because litigation consulting could taint the IFA's independence as an expert witness and remove the benefit of privilege. The two roles can be summarized as follows:

Litigation consultant

As a litigation consultant, the IFA can:

[129] The Institute of Internal Auditors, Ibid., p. 8.

[130] The Institute of Internal Auditors, Ibid., p. 8.

[131] This information was retrieved from the class, *IFA1907 Legal & Legal process Issues for Forensic Accountants*, in 2020. This is a summary of the information received during the course relating to the IFA's role in the court proceedings and how the IFA can assist courts and clients.

- **provide advice related to litigation** within her/his areas of expertise, such as critiquing the prosecution's forensic report.
- **communicate freely with counsel.** Documentation that supports the work is not subject to review by opposing counsel and is protected through litigation privilege, as the IFA will not be called as an expert witness.[132]
- **review testimony** of the expert witness hired by opposing counsel and advise counsel on any concerns relating to statements made.

Expert witness

As an expert witness, the IFA can:

- produce a forensic report that can be admitted into evidence.
- present work and opinions in court as a witness.
- provide in-depth investigation. This type of work can be expected to be time-consuming and therefore costly.

The most beneficial role for an IFA's services relates to litigation consulting. This will keep communications and work confidential while providing guidance in critical examination of forensic evidence.

3.4 Other IFA Roles

IFAs can also navigate a wide range of issues such as:[133]

[132] This information was retrieved from the class, *IFA1907 Legal & Legal process Issues for Forensic Accountants*, in 2020. This is a summary of the information received during the course relating to the IFA's role in the court proceedings and how the IFA can assist courts and clients.

[133] This information was retrieved from the Grant Thornton website on different services offered by forensic professionals. (https://www.grantthornton.ca/service/advisory/risk-and-forensics/).

Anti-money laundering

Money laundering[134] is the process by which "dirty" money (e.g., from drug selling or other illegal activities) is transferred through many layers of different bank accounts and other companies' accounts, so that it will appear to be "clean" money coming from legitimate business activities.

An IFA can help increase organizational defenses against becoming a source/victim of money laundering. It is critical for organizations to have anti-money laundering (AML) programs in place to prevent, detect, and respond to money laundering and terrorism financing. An IFA can ensure that an organization is complying with laws; can help to minimize threats; and provide assurance and security to clients. An IFA can handle compliance program review and testing;[135] risk assessment; program design and enhancements; investigations; enforcement actions; and remediation. When working on AML arrangements, the IFA can serve many categories of clients, including financial institutions, securities firms and dealers, foreign exchange providers, money remittance service providers, real estate brokers, government organizations, jewellery retailers, and precious metals dealers.[136]

---

[134] Government of Canada, Financial Transactions and Reports Analysis Centre of Canada, Definition of Money laudering, https://www.fintrac-canafe.gc.ca/fintrac-canafe/definitions/money-argent-eng

[135] This information was retrieved from the Grant Thornton website on different services offered by forensic professionals ,(https://www.grantthornton.ca/service/advisory/risk-and-forensics/anti-money-laundering/).

[136] ACAMS partners website for different training packages for employees, (https://www.acams.org/en/acams-for-organizations).

Certification – Sarbanes Oxley Act 2002 (SOX)[137]

SOX compliance refers to the annual audit in which a public company is obliged to provide proof of accurate, data-secured financial reporting.[138] [139] Using an experience- and risk-focused approach, an IFA can help an organization by reducing the burden of compliance and avoiding potential pitfalls. An IFA can help with setting internal controls, planning, scoping analysis, providing documentation, assessing inherent risk, providing walk-through and testing of existing controls, and evaluating potential control gaps.

Cybersecurity

Cybersecurity is the practice of defending computers, mobile devices, electronic systems, networks from malicious attacks.[140] In an organization without a sophisticated computer system, "…a cyber attack can damage investor and customer confidence, impact business operations and finances, and do long-term harm to the company's reputation."[141] An IFA specializing in cybersecurity can assess a company's vulnerability; establish or improve

[137] Website was visited to obtain more information on Sarbanes Oxley Act, (https://corporatefinanceinstitute.com/resources/knowledge/other/sarbanes-oxley-act/).

[138] Staff Contributor, May 28, 2019. "What is SOX Compliance",(https://www.dnsstuff.com/what-is-sox-compliance).

[139] Research note: Details of the SOX compliance are complex and are not covered in this research paper.

[140] Kaspersky website was visited to obtain more information on cyber security, (https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security).

[141]This information was retrieved from the Grant Thornton website on different services offered by forensic professionals, (https://www.grantthornton.ca/service/advisory/risk-and-forensics/cybersecurity/)

its IT security; identify and remediate vulnerability gaps and help to resolve breaches[142] or attacks.[143]

Internal audit

Internal audits evaluate a company's internal controls, including its corporate governance and accounting processes.[144] An IFA can assist in developing and implementing internal controls (or outsourcing of internal controls), preparing reports independent of management for the audit committee, and performing quality assurance reviews.

Whistleblower reporting solutions[145]

A whistleblower is anyone who has and reports insider knowledge of illegal activities occurring in an organization.[146] An IFA can assist in implementing a whistleblower program. Organizations benefit from having a whistleblower programs for many reasons, including: potential protection from negative publicity by dealing with issues internally; compliance with codes of good corporate governance; support of audit committee

---

[142] This information was retrieved from the Grant Thornton website on different services offered by forensic professionals, (https://www.grantthornton.ca/service/advisory/risk-and-forensics/cybersecurity/).

[143] This information was retrieved from the Ernst & Yonge website on different services offered by forensic professionals, (https://www.ey.com/en_ca/consulting/cybersecurity-risk-management#:~:text=EY%20Cybersecurity%20teams%20can%20help,invest%20in%20managing%20cyber%20risks).

[144] The Institute of Internal Auditors, (https://global.theiia.org/about/about-internal-auditing/pages/about-internal-auditing.aspx).

[145] This information was retrieved from the KPMG website on different services offered by forensic professionals, (https://home.kpmg/se/sv/home/tjanster/radgivning/Forensic/whistleblower-channel-kpmg.html).

[146]Kenton Will, March 30, 2020. Investoprdia Website, Law & Regulations, "What is a Whistleblower?", (https://www.investopedia.com/terms/w/whistleblower.asp#:~:text=A%20whistleblower%20is%20anyone%20who,aware%20of%20illegal%20business%20activities).

operations; support of the internal audit function; and identification of poor control processes and weak internal controls.[147]

Section IV: IFA Standards Relevant to Identity Theft

An IFA should consider relevant standard practices (standards) for engagements related to identity theft.[148] Here, the applicable standards are divided into the categories of legal, professional, ethical, and engagement-related standards.

4.1 Legal Standards

The following legal standards apply to an IFA testifying in court as an expert witness.[149]

The IFA should:

- provide independent assistance to the court by way of objective unbiased testimony for matters within their expertise.
- make it clear when a question or issue falls outside their expertise.
- never assume the role of an advocate.
- take responsible steps to provide the court with the information, assumptions on which their testimony is based, and any limitations that impact their testimony.

[147]This information was retrieved from the Grant Thornton website on different services offered by forensic professionals, (https://www.grantthornton.ca/service/advisory/risk-and-forensics/Whistle-blower-reporting-solutions/).

[148] CPA, Standard Practices for Investigative and Forensic Accounting Engagements (https://www.muskratfallsinquiry.ca/files/P-00244.pdf).

[149] This information was retrieved from the class, *IFA1907 Legal & Legal process Issues for Forensic Accountants*, in 2020. This is a summary of the information received during the course relating to the IFA's role in the court proceedings and how the IFA can assist courts and clients.

4.2 Professional Standards

The following professional standards apply to an IFA while testifying in court.[150] The IFA:

- should be independent in fact and in appearance.
- must have expertise.
- should be paid for services (e.g., for a completed report that has already been provided to a prosecutor) *before* a court hearing. Otherwise, this can indicate that fees may be (or appear to be) contingent on the outcome of the case. The opposing counsel can ask to see the engagement letter and review paragraphs that address fees.

4.3 Ethical Standards[151]

The IFA should show:

- **Confidentiality.** The IFA cannot discuss the case with anyone except the party that hired her/him.
- **Independence.** The IFA must be independent in fact and in appearance.
- **Reliability.** The IFA's findings must be reliable.

[150] This information was retrieved from the class, *IFA1907 Legal & Legal process Issues for Forensic Accountants*, in 2020. This is a summary of the information received during the course relating to the IFA's role in the court proceedings and how the IFA can assist courts and clients.

[151] This information was received in IFA1900 Forensic Accounting & Investigation, Fraud & Cybercrime in 2020 class. This is a summary of the information received during the course relating to IFA standards.

In addition, all work presented by the IFA must be her/his own, and the IFA should not take any information/evidence without authorization from the client or appropriate authority.

4.4 Engagement Standards

The IFA must ensure that:[152]

- the engagement can be performed objectively and verify that there are no conflicts of interest that could bias the engagement.
- there is enough time to prepare a report and to collect evidence.
- that all legal fees are paid before the trial starts, so that opposing counsel cannot say that the IFA's payment depends on the outcome of the trial.

Pre-engagement, the IFA must[153]:

- Verify there are no conflicts of interest that could bias the engagement.
- Verify that there are enough resources to effectively complete the engagement, such as competent and experienced staff and the ability to obtain relevant expertise, where required.
- Prepare an engagement letter outlining the parameters of the engagement.
- Understand the circumstances surrounding the engagement in order to plan the engagement and the procedures to be performed.

[152] This information was received in IFA1900 Forensic Accounting & Investigation, Fraud & Cybercrime in 2020 class. This is a summary of the information received during the course relating to IFA standards.

[153] This information was received in IFA1900 Forensic Accounting & Investigation, Fraud & Cybercrime in 2020 class. This is a summary of the information received during the course relating to IFA standards.

Engagement execution is the stage in which interviews and evidence gathering will be performed.

Reporting. Upon completion of the investigation, the IFA will provide a report outlining the scope and findings of the investigation in the format agreed upon within the engagement letter.

Section V: Challenges

This section reviews the challenges in fighting identity theft[154] and challenges that the IFA faces in successfully designing and helping to implement procedures that are aimed at reducing identity theft and the leaking of personal information in organizations.

In Designing Controls and Procedures

- **Budget.** Many organizations do not have a sufficient budget to develop, implement, and monitor plans to fight identity theft. For these organizations, the costs of identity theft perceived to be lower than the costs of hiring an IFA to perform these services. Small organizations that cannot afford to pay an IFA or fund a fraud managing department could outsource the work to firms that specialize in providing IT security to small organizations.
- **Business environment.** Corruption is normal in some areas/countries and institutions. Corruption is sometimes institutionalized, and organizations may design codes of ethics only to meet regulatory requirements. While a

[154]Zaidi Kamaal," Identity Theft and Consumer Protection: Finding Sensible Approaches to Safeguard Personal Data in the United States and Canada". (https://contacts.ucalgary.ca/info/ha/files/info/unitis/publications/1-9740597/Zaidi%2C%20ART%201.pdf).

multinational organization can attempt to invest in security design, the unspoken words and subtle practices of local society[155] can pose challenges to implementation.

- **Legal challenges.** The IFA can face legal challenges while designing and implementing procedures to reduce identity theft.
- **Not walking the talk.** Managers and C-suite executives may be fraud perpetrators who can override existing controls. [156] Such behaviours create barriers to IFAs in implementing controls and procedures.

In Fighting Identity Theft

- **Many websites do not have privacy and security.** The government needs to step in and make it mandatory for e-commerce websites to adopt secure, essential privacy and data protection for credit cards and personal information. If these websites are not secured, hacked information could be sold to identity thieves.
- **Review data protection laws.** Various governments and law enforcement agencies need to revisit their data protection laws and thoroughly inspect them, so that necessary changes can be made.
- **Collaboration is needed.** Collaboration between the governments and different law enforcement agencies is needed so that identity theft committed outside the domain of a country do not go unpunished. Arrangements and diplomatic

[155] Evill, R. (2019, December 30). "*5 Anti-Fraud Lessons From Southeast Asia"*. Retrieved from ACFE Insights: (https://www.acfeinsights.com/acfe-insights/5-anti-fraud-lessons-from-southeast-asia).

[156] Association of Certified Fraud Examiners. (2020). Report to The Nations - 2020 Global Study on Occupational Fraud and Abuse.

agreements must be made, so offenders outside of Canada can be prosecuted for the crimes committed within Canada.

- **Work with victims.** Governments and law enforcement agencies must work with identity theft victims to provide them with assistance and advice regarding the rights that are available to them. Currently there is no path provided by the government or police to victims of identity theft. Money is not being returned to them, and victims are left on their own to deal with collectors and clean their credit scores.
- **Convincing thieves.** Some perpetrators can con victims into giving them money by being very charming and convincing. People will trust these convincing thieves and will give money away. Convincing thieves will never go away, but increasing public awareness is a defense against them.

The Impact of Identity Theft on the Economy and the Consumer

Activities between buyers and sellers in the marketplace usually involve an exchange of information to complete transactions. That is why several problems arise when personal data are compromised: consumers and businesses may:

- **lose confidence in e-commerce.** Consumers lose confidence in the marketplace when they discover that their personal data is not protected and that organizations are not doing enough to protect their personal data.
- **lose their reputation** because of an identity thief's misuse of financial assets.[157]

[157]Zaidi Kamaal," Identity Theft and Consumer Protection: Finding Sensible Approaches to Safeguard Personal Data in the United States and Canada". (https://contacts.ucalgary.ca/info/ha/files/info/unitis/publications/1-9740597/Zaidi%2C%20ART%201.pdf).

- **accumulate additional debts** if identity thieves use stolen information to open bank and credit card accounts.[158]
- **be refused credit** or loans if loans and credit card accounts opened by identity thieves were never repaid.
- **gain bad credit ratings**.[159]
- **incur additional costs** to build and maintain adequate security measures, particularly by businesses in protecting employee- and customer information.[160]
- **incur big economic losses** due to liability issues, fines, and loss of clientele if security measures are not adequate.
- **incur price increases**, because identity theft drives up the costs of doing business and these costs are passed onto consumers.

Section VI: Conclusions

My aims with this research paper are to help enhance the reader's understanding of recent developments in identity theft, how to protect personal information, and how identity theft can impact IFA practice and how IFAs can help to protect people and companies against fraud and identity theft.

---

[158]Zaidi Kamaal," Identity Theft and Consumer Protection: Finding Sensible Approaches to Safeguard Personal Data in the United States and Canada". (https://contacts.ucalgary.ca/info/ha/files/info/unitis/publications/1-9740597/Zaidi%2C%20ART%201.pdf).

[159] A Report of the Federal Trade Commission, 2019 – 2020, https://www.ftc.gov/system/files/documents/reports/protecting-older-consumers-2019-2020-report-federal-trade-commission/p144400_protecting_older_adults_report_2020.pdf

[160] The impact of Identity Theft on Employees and their workplace, *available at* https://www.idtheftcenter.org/wp-content/uploads/2020/08/Identity-Theft-in-the-Workplace-Aura-ITRC-Report-081420-WEB-ADA.pdf?utm_source=button&utm_medium=AURApage&utm_campaign=AURAReport081720

From the information I provided, it is clear that we, as a society, are far away from reducing identity theft, and institutions such as police, courts, etc., are not very effective in the fight against the identity theft crimes. The issue is that the budget in law enforcement is insufficient to bring in a team of effective, but expensive, forensic accountants. Also, cases of identity theft have to do with stealing information for enrichment purposes, such as stealing credit card information, getting access to a person's bank account, changing a person's address, and redirecting mail to a thief's address to receive a person's credit cards and other financial information. It is almost impossible for police to solve those types of crime because they do not have enough resources.

When ordinary people listen to the news, they hear about physical crimes that police/law enforcement have resolved, but not about the number of identity theft cases resolved. Some information in identity theft cases is confidential and cannot be brought into the open until trials are over, and that can take years. Much identity theft is under-reported.

Saying that, each and every one of us must secure our own credit and identity:

- We must not rely on other institutions (e.g., police, banks, or courts).
- We should invest time and money to monitor our own credit. In Canada, credit reports are not free. Equifax charges $19.95 a month.[161]
- We should not rely on financial institutions when we have unrecognized transactions. We should check credit card transactions more than once a month, especially now, when everything is automated, and all the information is available live, and all transactions are posted in real time.

[161] From Equifax website

- We should pay attention to what we post online about ourselves and our families. Information like a mother's middle name or daughter's favorite colour can be found on many people's social media websites, but should not be, particularly because those pieces of information often form our passwords or answers to security questions.

Harsh penalties should be in place for identity thieves. Currently, they can be sued for fraud under consumer privacy/protection laws. Often, however, the identity thief may not be the only party that is legally responsible for the theft. Often individuals or entities that encounter the stolen information may also be sued under the same laws.

The increasing number and pervasiveness of identity theft present issues that IFAs will have to contend with. Moreover, as identity theft cases continue to evolve, and criminals find new ways to steal identities, IFAs must be aware of all new developments in the field in order to do their jobs. IFAs must become more cognizant of the fraud landscape against which they operate. As per references to IFA standard practices[162] creativity, professional skepticism, investigative problem-solving skills, knowledge of the legal process, and curiosity are characteristics that IFAs must possess to help address issues that identity theft can present to an engagement.

Fraud cannot be completely eliminated but can be reduced. IFAs can lead by example and advance the profession through their professional conduct and exhibition of abstract skills, like maintaining objectivity and integrity.

[162] CPA, Standard Practices for Investigative and Forensic Accounting Engagements, (https://www.muskratfallsinquiry.ca/files/P-00244.pdf).

Section VII: Bibliography

Abdullah Mahmood Hussain Shah, Waqar Ahmed, August 2016. “Identity theft prevention in online retail organizations: a knowledge sharing framework”, The Business and Management Review, Volume 8 Number 1, (https://www.researchgate.net/publication/325817772_Identity_theft_prevention_in_online_retail_organisations_a_knowledge_sharing_framework).

Allison Stuart F. H., Schuck Amir M., Lersch Kim Michelle, (2005). “Exploring the crime of identity theft : Prevalence, clearance rates, and victim/offender characteristics, Journal of Criminal Justice 33 (2005) 19-29, (https://scholarcommons.usf.edu/si_facpub/578/). Please note I accessed this document through University of Toronto Library.

Anderson Keith B., Durbin Erik and Salinger Michael A., Spring 2008. “Identity Theft”, Journal Of Economic Perspectives – Volume 22, Number 2, Pages 171 – 192, (https://www.aeaweb.org/articles?id=10.1257/jep.22.2.171).

Association of Certified Fraud Examiners, “How management Can Prevent Fraud in the Workplace”, (https://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/tone-at-the-top-research.pdf).

Blackier (2019). IFA 1907 - Legal & Legal Process Issues for Forensic Accountants Session 2: Applicable Legal Standards Governing the IFA Expert.

Blackier (2019). IFA 1907 - Legal & Legal Process Issues for Forensic Accountants Session 1: The Role of the IFA Expert with the Rule of Law.

Blackier, J. (2019). "Reigning In" Expert Witness Opinion Evidence in the Context of the Ultimate Issues Doctrine. Saint John.

Bryan Borzykokowski, “4 thing you need to know about identity theft right now”, CPA Institute of Canada, March 14, 2019. (https://www.cpacanada.ca/en/news/canada/2019-03-14-identity-theft-101).

Canada Revenue Agency, September 3, 2020. “Beware of schemes that promise large tax deductions or tax free income”, Government of Canada, (https://www.canada.ca/en/revenue-agency/news/newsroom/tax-tips/tax-tips-2020/beware-schemes-promise-large-tax-deductions-tax-free-income.html).

Canada, S. (2017, November 29). *Census Profile, 2016 Census*. Retrieved from StatCan: (https://www12.statcan.gc.ca/census-recensement/2016/dp-pd/index-eng.cfm).

Canadian Public Accountability Board, "Code of Ethics". (https://www.cpab-ccrc.ca/docs/default-source/governance/code-of-ethics-board-of-directors-en.pdf?sfvrsn=964c6f69_8).

Cassim F, (2015 Volume 18 No 2), "Protection Personal Information in the era of Identity theft: Just how safe is our personal information from Identity Thieves?", (https://www.researchgate.net/publication/282464503_Protecting_Personal_Information_in_the_Era_of_Identity_Theft_Just_how_Safe_is_Our_Personal_Information_from_Identity_Thieves).

Chan Siew H., Song Qian, Wright Arnold M., Wright Sally, July – December 2015. "The Effects of Mianzi and Professional Relationship Guanxi on Auditor Fraud Detection", Journal of Forensic & Investigative Accounting, (https://www.researchgate.net/publication/269709991_The_effects_of_mianzi_and_professional_relationship_guanxi_on_auditor_fraud_detection).

Common David, October 31, 2018. "Police raid Indian call centres linked to 'CRA phone scam' that have victimized Canadians", (https://www.cbc.ca/news/world/national-cra-india-rcmp-scam-1.4883796).

Connolly Amanda, November 18, 2019. "32 arrested in India after allegedly posing as Canadian officials in call centre fraud", (https://globalnews.ca/news/6182793/india-call-centre-scam-arrests/).

Copes Heith, Vieraitis Lynne M, Cardwell Stephanie M, and Vasquez Arthur, (2013). "Accounting for Identity Theft: The Roles of Lifestyle and Enactment", Journal Of Contemporary Criminal Justice, (https://www.researchgate.net/publication/258128130_Accounting_for_Identity_Theft_The_Roles_of_Lifestyle_and_Enactment). Please note I accessed this document through University of Toronto Library.

Copes Heith, Vieraitis Lynne M., Septembre 2009. "Understanding Identity Theft Offenders' Accounts of Their Lives and Crimes", Criminal Justice Review Volume 34 Number 3, (https://journals.sagepub.com/doi/10.1177/0734016808330589). Please note I accessed this document through University of Toronto Library.

Criminal code of Canada, sections 402.2 and 403. (http://www.criminal-code.ca/criminal-code-of-canada-alphabetical-A.html).

Cullen Catherine and Everson Kristen, May 1, 2020. “Canadians who don’t qualify for CERB are getting it anyway: and could face consequences”. (https://www.cbc.ca/news/politics/cerb-covid-pandemic-coronavirus-1.5552436).

Drew Armstrong (13 September 2017). "My Three Years in Identity Theft Hell". Bloomberg. Archived from the original on 19 September 2017. Retrieved 20 September 2020, (https://www.bloomberg.com/news/articles/2017-09-13/my-three-years-in-identity-theft-hell).

Engdahl Oskar, March 18, 2011. “White Collar Crime and Informal Social Control: The Case of “Crisis Responders” in the Swedish Banking and Finance Sector”, Scientific Research, (https://www.researchgate.net/publication/228424880_White_Collar_Crime_and_Informal_Social_Control_The_Case_of_Crisis_Responders_in_the_Swedish_Banking_and_Finance_Sector).

FATF (2020), “Guidance on Digital Identity, FATF, Paris”, (https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf).

Fortes, N., & Rita, P. (2016). “Privacy concerns and online purchasing bahaviour: towards an integrated model”. European Research on Mnagagement and Business Economics, 22(3), 167-176.

Government of Canada, Identity Theft, April 22, 2020. (https://www.ic.gc.ca/eic/site/Oca-bc.nsf/eng/ca03025.html).

Hoofnagle Chris Jay, Fall 2007. “Identity Theft: Making the Known Unknowns Known”, Harvard Journal of Law & Technology, (https://jolt.law.harvard.edu/articles/pdf/v21/21HarvJLTech097.pdf).

Jha Ruchika, ‘Identity theft: Is it a modern crime?’ (*Law Times Journal*, 14 March 2020), (http://lawtimesjournal.in/identity-theft-is-it-a-modern-crime/).

Journal of Forensic & Investigative Accounting Vol. 7, Issue 2, July - December 2015, (http://www.bus.lsu.edu/accounting/faculty/lcrumbley/jfia/Articles/final%20r/pdf/8.pdf).

Journal: Help Net Security. “COVID-19 online fraud trends: Industries, schemes and targets”. (https://www.helpnetsecurity.com/2020/05/15/covid-19-online-fraud/).

Komando Kim, January 6, 2020. “9 clever ways thieves steal your identity: and how you can stop them,” (https://www.foxnews.com/tech/9-clever-ways-thieves-steal-your-identity-and-how-you-can-stop-them).

Li Yuan, Adel Yazdanmehr, Wang Jingguo, Rao H. Raghav, 2019. “Responding to identity theft: A victimization perspective”, Elsevier Journal, Retrieved from University of Toronto Library.

Lindberg Debra, Summer 2011. “Prevention of Identity Theft: A Review of the Literature”, Portland State University, Criminology and Criminal Justine Senior Capstone, (https://pdxscholar.library.pdx.edu/ccj_capstone/10/?utm_source=pdxscholar.library.pdx.edu%2Fccj_capstone%2F10&utm_medium=PDF&utm_campaign=PDFCoverPages).

Lynch John J., (2005) ‘Identity Theft in Cyber Space: Crime Control Methods and Their Effectiveness in Combating phishing Attacks’, Berkeley Technology Law Journal 259.

Miller Harry, Published on March 20, 2021, by in CBC Mews online magazine, (https://canadanewsmedia.ca/as-covid-surged-indian-police-shut-down-scam-centres-targeting-canadians-now-theyre-back-cbc-ca/).

Monahan Torin, (2009).” Identity theft vulnerability. Neoliberal governance through crime construction”, Theoretical Criminology, (https://journals.sagepub.com/doi/abs/10.1177/1362480609102877). Please note I accessed this document through University of Toronto Library.

Nathaniel Popper, “Pure Hell for Victims’ as Stimulus Programs Draw a Flood of Scammers, April 22, 2020, Updated April 24, 2020. (https://www.nytimes.com/2020/04/22/technology/stimulus-checks-hackers-coronavirus.html).

Newman Graeme R., McNally Megan M., July 2005. “Identity Theft Literature Review”, National Institute of Justice, (https://www.ojp.gov/ncjrs/virtual-library/abstracts/identity-theft-literature-review).

Nicholson Katie and Ho Jason, May 1, 2020. “Canadians have lost more than $1.2 million to COVID-19 scams”, (https://www.cbc.ca/news/politics/covid-scams-fraud-crime-1.5551294).

Office of the Privacy Commissioner of Canada, (https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/).

Oxford English Dictionary online. Oxford University Press. September 2007. Retrieved 27 September 2010.

Perl Michael W., 'It's Not Always About the Money: Why the State Identity Theft Laws Fail to Adequately Address Criminal Record Identity Theft' [2003] 94 Journal of Criminal Law and Criminology 169.

Privacy by Design, "Strong Provacy Protection: Now, and Well into the Future", A report on the State of PbD to the 33rd International Conference of Data Protecton and Provacy Commissioners, 2011.

Rebovich Donald J., Allen Kristy and Platt Jared, November 2015. "The New Face of Identity Theft: An Analysis of Federal Case Data for the Years 2009 through 2013", Center for Identity Management and Information Protection Utica College, (https://www.utica.edu/academic/institutes/cimip/New_Face_of_Identity_Theft.pdf).

Rebovich Donald, "Identity Theft, Most Common schemes", (https://www.utica.edu/academic/institutes/cimip/idcrimes/schemes.cfm)

Report by Grant Thornton, (2018). "Fraud in the spotlight", (https://www.grantthornton.ca/globalassets/1.-member-firms/canada/insights/pdfs/fraud-in-the-spotlight.pdf).

Report to the Nations, "2020 Global Study on occupational fraud and abuse", (https://www.acfe.com/report-to-the-nations/2020/).

Romanovsky Sasha, Telang Rahul and Acquisti Allessandro, (2008). "Do Data Breach Disclosure Laws Reduce Identity Theft?", Journal of Policy Analysis and Management, (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1268926).

Saunders Kurt M, and Zucker Bruce, (1998). "Counteracting Identity Fraud in the Information age: The Identity Theft and Assumption Deterrence Act", Cornell Journal Of Law and Public Policy [Vol.8:661], (https://ww3.lawschool.cornell.edu/research/JLPP/upload/Saunders-Zucker-661.pdf).

Scott Steinberg, February 27, 2020. "The latest ways identity thieves are targeting you: and what to do if you are the victim".(https://www.cnbc.com/2020/02/27/these-are-the-latest-ways-identity-thieves-are-targeting-you.html).

Stana Richard M., February 12, 2002. “Available Data Indicate Growth in Prevalence and Cost”, United States General Accounting Office,(https://digital.library.unt.edu/ark:/67531/metadc289577/).

Standard Practices for Investigative and Forensic Accounting Engagements, Canadian Institute of Chartered Accountants, November 2006.

Sullins L.L., ‘‘Phishing’ for a Solution: Domestic and International Approaches to Decreasing Online Identity Theft’ [2006] Emory International Law Review 397.

Syed R. Ahmed, “Preventing Indetity Crime: Identity Theft and Identity Fraud” (2020).

Tan Veltrice, (2018). “The art of deterrence: Singapore’s anti-money laundering regimes”. Journal of Financial Crime”, (https://eprints.lse.ac.uk/88777/1/Tan_The%20Art%20of%20Deterrence_Accepted.pdf).

The Institute of Internal Auditors, The American Institute of Certified Public Accountants and Association of Certifies Fraud Examiners, “Managing the Business Risk of Fraud: A Practical Guide”, (https://www.acfe.com/uploadedfiles/acfe_website/content/documents/managing-business-risk.pdf).

Verizon 2018 Data Breach Investigation Report (DBIR), available at (https://admin.govexec.com/media/vz_assets/2018_dbir_public_sector_final.pdf).

Vigdor Neil, August 21, 2019. “5 Indicted in Identity Theft Scheme That Bilked Millions From Veterans”, The New York Times, (https://www.nytimes.com/2019/08/21/us/military-identity-theft-scheme.html).

Weisburd David, Waring Elin, June 2009. “White Collar Crime and Criminal Careers”, Cambridge Studies in Criminology, (https://www.cambridge.org/core/books/whitecollar-crime-and-criminal-careers/6D3DC88DCFCF9FEA7C8D9D9508CDD8E8). The Book can be downloaded from this website.

Weisburg David L., Simpson Sally S., January 2009. “Development Trajectories of White – Collar Crime” (https://www.researchgate.net/publication/226629733_Developmental_Trajectories_of_White-Collar_Crime). The Book can be downloaded from this website.

Appendix I: Interviews

The following interview questions were sent to Nadia Zyeva, Shulamit Finkelstein, Khaled Shoeb, Dwyne King and Caroline Dixon. The purpose of the interview was to learn about protection of confidential data in the workplace for interviews 1 – 3 and I interviewed two Senior Managers working in different forensic departments at Grant Thornton, see interviews 4 - 5. Consent was received prior to including answers from each interviewee.

All answers are recorded here exactly as provided by the interviewees, without any changes/additions from me. Interviewees answers are highlighted in yellow.

Interview #1

Interview Paper 1 with Nadia Zyeva

MFACC 2020 - IFA 2903 Emerging Issues Advances Topics

Interview questions for 2020 research paper for Anna Gubin

Research topic: Developments in identity theft and in the protection of personal confidential data and their impact on IFA practice and IFA standards.

Interview questions will be covering your role in the organization, handling of personal data on the daily/weekly basis and steps that are taken to protect and limit use of the confidential data. The focus in the interview will be on protection of personal identity and how different organizations are approaching this issue.

First and last name of the interviewee

Nadia Zyeva

Occupation

Accountant

Position in the organization

Accountant and financial analyst

Do you have access to the confidential information while performing your work? Please describe the type of confidential data you have access to.

Yes, financial statements that are not released for public, expense reports, confidential hiring information, payroll information and performance evaluation reports.

Please describe your work in details and how you handle confidential data, while working

Computers are password protected, VPN, each software needs its own login, all documents are physically secured, all PDF documents are password protected.

What steps are taken to keep confidential data, confidential. Please be specific and give examples. Steps can include password protection, encryption etc.

As above. All documents that are send by e-mail are password protected. Not all employees have equal access to the accounting system. Access is provided on the need to know basis.

Are there any additional steps taken to protect confidential data? Please be specific in terms of the steps and data that is being protected.

Computer updates, frequent change of passwords, all access on the need to know basis.

If information was to be leaked, are there protocols in place? What should be done if information is stolen or leaked?

I am not aware of such protocols.

Are you aware of the federal privacy commissioner rules and what mandatory reporting of breaches is? October 2018 came into effect.

No, I am not aware

Interview #2

Interview Paper 2: with Khaled Shoeb

MFACC 2020 - IFA 2903 Emerging Issues Advances Topics

Interview questions for 2020 research paper for Anna Gubin

Research topic: Developments in identity theft and in the protection of personal confidential data and their impact on IFA practice and IFA standards.

Interview questions will be covering your role in the organization, handling of personal data on the daily/weekly basis and steps that are taken to protect and limit use of the confidential data. The focus in the interview will be on protection of personal identity and how different organizations are approaching this issue.

First and last name of the interviewee

Khaled Shoeb

Occupation

Banking

Position in the organization

Senior Advisor

Do you have access to the confidential information while performing your work? Please describe the type of confidential data you have access to.

I do have access to confidential information while performing my work. I have access to Customer Data, Bank's financial and strategic information and Industry related sensitive information.

Please describe your work in details and how you handle confidential date, while working

I do Investigation and Risk Governance Work.

I request for information related to my work. I ensure the data is handled as per Bank's policy and with special care. I use encryption method when sending data from my desk. All sensitive data is highly protected with various passwords and other ways. The access level is also controlled and reviewed by another group of people. And their work is monitored by a separate group of people.

What steps are taken to keep confidential data, confidential. Please be specific and give examples. Steps can include password protection, encryption etc.

1. Data is classified according to the importance and need. Each classification has individual set of rules of handling.
2. Access level is restricted per user, per department.
3. Data cannot be generally shared outside the bank. This is completely tracked and classified. If someone wants to send data outside bank, there are higher levels of protocols and approval process with encryption.
4. All accesses are password protected.

Are there any additional steps taken to protect confidential data? Please be specific in terms of the steps and data that is being protected.

Already mentioned.

If information was to be leaked, are there protocols in place? What should be done if information is stolen or leaked?

I am not aware of such protocols. There is special department that deals with such issues.

Are you aware of the federal privacy commissioner rules and what mandatory reporting of breaches is? October 2018 came into effect.

No, I am not aware

Interview #3

Interview Paper 3: with Shulamit Finkelstein

MFACC 2020: IFA 2903 Emerging Issues Advances Topics

Interview questions for 2020 research paper for Anna Gubin

Research topic: Developments in identity theft and in the protection of personal confidential data and their impact on IFA practice and IFA standards.

Interview questions will be covering your role in the organization, handling of personal data on the daily/weekly basis and steps that are taken to protect and limit use of the confidential data. The focus in the interview will be on protection of personal identity and how different organizations are approaching this issue.

First and last name of the interviewee

Shulamit Finkelstein

Occupation

Business System Analyst

Position in the organization

System Analyst

Do you have access to the confidential information while performing your work? Please describe the type of confidential data you have access to.

Yes, I have access to live data, account info, addresses and names of the clients.

Please describe your work in details and how you handle confidential data, while working

We signed forms with the bank that prohibit us from sharing the info. We cannot send any private info files to personal e-mails or save information on the memory sticks.

What steps are taken to keep confidential data, confidential. Please be specific and give examples. Steps can include password protection, encryption etc.

Same as above and all programs are password protected.

Are there any additional steps taken to protect confidential data? Please be specific in terms of the steps and data that is being protected.

Not in my specific project.

If information was to be leaked, are there protocols in place? What should be done if information is stolen or leaked?

I am not aware of such protocols. There is special department that deals with such issues.

Are you aware of the federal privacy commissioner rules and what mandatory reporting of breaches is? October 2018 came into effect.

No, I am not aware

Interview #4

Interview Paper 4 – with Dwayne King

MFACC 2021 – IFA 2903 Emerging Issues Advances Topics

Interview questions for 2021 research paper for Anna Gubin

Research topic: Developments in identity theft and in the protection of personal confidential data and their impact on IFA practice and IFA standards.

Interview questions will be covering your role as Senior Manager in the forensic and anti -money laundering department at Grant Thornton. The focus in the interview will be on to show tasks/issues that you are dealing with on the day to day basis and how confidential information is protected at your organization.

First and last name of the interviewee

Dwayne King

Occupation

Senior Manager in the forensic and anti-money laundering department at Grant Thornton LLP

Position in the organization

Senior Manager in the forensic and anti-money laundering department at Grant Thornton LLP

You are working with forensic audit team. Please describe your usual day?

Typically working on the current engagements and these engagements range from investigation to regulatory reviews. Deal a lot with credit unions, law firms, small to mid-size companies. Big companies like RBC, TD, Rogers have either inhouse forensic auditors or are using Big 4.[163]

[163] Big 4 are Deloitte, KPMG, Ernst & Yonge and PWC (PriceWaterHouseCopper).

How you approach cases and what are the most challenging aspects in the case

First, I do expectation settings and based on the budget and expectations decide on the first step. After that I gather evidence. An investigator will examine evidence and get ready for an interview. After the interview, the report is being provided to the party that hired me. Usually it takes 6 – 8 weeks to conduct an investigation and to deliver report. Internal thefts are still going on a lot. People in the control position can rip employers. Usually, it is through whistle blower hotline that theft is uncovered.

Can they (employee) refuse to participate in the interview?

Yes, but they can get fired for that. Usually, thieves are going for an interview, since they think they are smarter, than investigators.

Are cases the same or they differ? Do cases have thing in common? If yes, what cases have in common?

Most common thing in many cases is a failure in the controls. It does not matter if it is internal or external fraud, issue is always with controls. Either controls are there but were never followed. Employees are not trained. In many cases, supervisors are not supervising. They can not adequately supervise. Usually (in many cases), it is not intentionally.

For example, expense fraud. Supervisor did not review in detail the expense report, and wrong expenses were reimbursed.

How likely it is that cases are resolved, and "perpetrators" are taken to justice?

Very, very rarely the person will be prosecuted, especially in an unionized environment. It is very hard to terminate a union employee. To be prosecuted, everything must go through civil or criminal court. Usually police are not involved, and companies are not reporting the crime. Police are not touching frauds less than $1M.

Do you have access to the confidential information while performing your work? Please describe the type of confidential data you have access to.

Anything that employees are using, and it was issued by organization we can access.

Please describe your work in details and how you handle confidential data, while working

Password protected computers, secure servers.

What steps are taken to keep confidential data, confidential. Please be specific and give examples. Steps can include password protection, encryption etc.

See above

Let us talk about victims of identity theft. Is there a legal path that is provided to the victims of identity theft? If yes, please describe?

Not much to do. Contact Equifax or TransUnion. There is no real path. You can go to police and file report, but no investigation (highly unlikely), since not much can be done. In reality, it is very long and expensive process, and judge can give you less that you lost.

If information was to be leaked, are there protocols in place? What should be done if information is stolen or leaked?

I do not know

Are you aware of the federal privacy commissioner rules and what mandatory reporting of breaches is? October 2018 came into effect.

Yes

Interview #5

Interview Paper 5 – with Caroline Dixon

MFACC 2021 – IFA 2903 Emerging Issues Advances Topics

Interview questions for 2021 research paper for Anna Gubin

Research topic: Developments in identity theft and in the protection of personal confidential data and their impact on IFA practice and IFA standards.

Interview questions will be covering your role as Senior Manager in the Risk and Forensic Services department at Grant Thornton. The focus in the interview will be on to show tasks/issues that you are dealing with on the day to day basis and how confidential information is protected at your organization.

First and last name of the interviewee

Caroline Dixon

Occupation

Senior Manager in the Risk and Forensic Services at Grant Thornton LLP

Position in the organization

Senior Manager in the Risk and Forensic Services at Grant Thornton LLP

You are working with forensic audit team. Please describe your usual day

Everyday is different and I do not know what to expect on the daily basis. When money is stolen from the client, we are helping to quantify the loss and figure out who is involved, and how money was stolen. A lot of times, there is a break down in internal controls. We are helping them (clients) to figure out where the gaps are in internal control and to reduce the risk of this from happening again.

In general, every time people fighting over money, they call us in to resolve the dispute and potentially assist with litigation.

How you approach cases and what are the most challenging aspects in the case

The most challenging part is, that all cases are different and there is no one solution to fit all cases. There are IFA standards to guide us, and we did enough of the cases, so they stared to look familiar. Because we have done enough of the files, we know how to approach them in general. The specifics of the case, it is where it gets different. We have a workbook, that guides us in developing an investigative plan. It guides us in term of which things to consider.

Are cases the same or they differ? Do cases have thing in common? If yes, what cases have in common?

Cases do have things in common, like the break down in internal controls, lack of segregation of duties and too much trust in someone.

How likely it is that cases are resolved, and "perpetrators" are taken to justice?

I feel like it does not happen enough. I write the report, but in many cases the company use our report to terminate the employee or for insurance claim. It does not happen a lot, that people go to jail for that. I believe that police services do not always have the resources to deal with all that issues. In some cases, police will use our work to charge a person and, in that case, people will go to jail.

Sometimes company does not have money to do full investigation, so report will be about fixing internal controls, rather than calculate how much money was stolen.

Can employee refuse to participate in the interview?

I think if they are asked by their employer, they cannot refuse. But, if individual was fired already, they do not have to talk to you (Forensic Accountants). We are asking employers to keep people on the payroll, but taking all the access away, so no future damage can be done. It is better to do investigation, while people are still there.

Do you have access to the confidential information while performing your work? Please describe the type of confidential data you have access to.

Yes, I have access to bank accounts, tax records, Financial Statements, General Ledger accounting records, court documents.

Please describe your work in details and how you handle confidential data, while working.

We have a secure server, just for the forensic team, so other people in the firm can not access these records. We try to keep things out of e-mails. We have secure file transfer for the clients to send us e-mails and to upload information. E-mails can be compromised. So, we use e-mails just for communications, but documents are sent through secure file

transfer. Our laptops for work and our IT make sure our laptops have all latest security upgrades.

As part of the contract with the client, paragraph on the confidentiality is included in the engagement letter. Information that are on the servers are in Canada.

What steps are taken to keep confidential data, confidential. Please be specific and give examples. Steps can include password protection, encryption etc.

We issue reports with a locked PDF, so information can not be changed or misused, and signatures are not taken out and used somewhere else. Clients usually send us information that is password protected. We are asking out clients to send us information through secure file transfer site, so it is encrypted. The training of our staff is very important to us, and we make sure that no physical documents are left on the desk and chain of custody protocols are followed for litigation purposes.

Forensic auditors can either be an expert witness or consultant when assisting lawyers. From your experience, please describe both roles and which role you prefer?

I never worked as a consultant and my role was as an expert witness to the court/lawyer. I was hired by a lawyer to gather facts in relation to the case. I was going through the financial records to determine how the money were used. I wrote a report that was used in court that summarized my findings. I had to testify in court, and I was crossed examined and the whole time I had to give my conclusion and my opinion based on facts only. It is unbiased, independent, based on facts role.

Let us talk about victims of identity theft. Is there a legal path that is provided to the victims of identity theft? If yes, please describe?

I do not think that there is a clear path. I think victims are left to figure it our on their own many times. My understanding is that people will not get much support from RCMP and other authorities. Many things they (victims) will have to do on their own. Things like repair credit history/score and contacting financial institutions.

What rights do victims of identity theft have? Are there any federal laws to protect the victims?

If victims know for sure that their information was leaked from certain person or organization, there are laws that can make these organizations accountable for that. It is hard to prove who leaked the information, and unless it is proven in court and there is threat of significant harm, that organization has to report it to the Privacy Commissioner in Canada and they have to notify the individuals, who's information was leaked, or they can get a fine.

For example, if individuals fall a victim of CRA calls from India. What victim can do and what are his/her options?

Because it is a well-known scam now, police are giving it more attention. I never heard of anyone getting their money back. Victims should contact police, CRA and the Canadian Antifraud Centre. Also, credit check must be done, and financial institution should be contacted.

If information was to be leaked, are there protocols in place? What should be done if information is stolen or leaked?

An organization has to follow mandatory reporting requirements. If there is a significant threat, organizations must contact individuals. The issue is that organization is the one to decide/assess if there is a significant threat.

Are you aware of the federal privacy commissioner rules and what mandatory reporting of breaches is? October 2018 came into effect.

Yes, I am aware of the rules.