Credit Card Fraud in Canada

Research Project in Emerging Issues/Advanced Topics Course

Diploma in Investigative and Forensic Accounting Program

University of Toronto

Prepared by Ann-Marie Deboran CPA CMA

June 20, 2017

For Prof. Leonard Brooks

TABLE OF CONTENTS

ACKNOWLEDGEMENT

I wish to acknowledge the guidance and feedback made by Suzanne Poulin, CPA CA, Directrice principale Banque Nationale during the research for this report.

1.1 Executive Summary

Research has shown that in Canada (and even globally) that it is increasingly difficult to detect when credit card data breaches occur, and to prevent data theft, account takeovers, and card-not-present fraud (CNP). Between 2008 and 2015 credit card fraud increased from $407.7 million to $726.5 million or 78%, as per the Canadian Banking Association's (CBA) Credit Card Fraud and Interac Debit Card Fraud Statistics, 2015 (Appendix A). The CHIP and PIN card technology implemented in Canada from 2007 onwards, has been shown to be effective in reducing Lost, Stolen, Non Receipt, and Domestic Counterfeit Card Activity. The same CBA report has also shown that Fraud applications, Account Takeovers, and Card-Not-Present fraud increased between 2008 and 2015.

Fraud continuously innovates and migrates to new channels and countries. This results in economic loss, identity theft, and cyber fraud which is increasing and therefore highlights an imperative need to have cooperation between stakeholders in different jurisdictions. As a general recommendation, improvements in cooperation between federal agencies and financial institutions, respectful of industry cultures, regulatory standards and clear definitions of what constitutes or measures criminal activities, will help to detect crime rings and prevent criminal activity on credit cards data theft.

Organizations in Canada need to prioritize a fraud prevention attitude first, followed by detection and recovery of data. With the expertise to protect devices and data, the time has arrived to implement corporate governance policies, legal measures, transform operational risk policies, build capacity, and develop county wide / global initiatives to report and prevent cybersecurity threats. In Ontario, cyber security

subject matter experts received $250 million in venture capital funding between 2011 and 2015, and Canada ranked 4th in the global cyber security sector deal flows between 2012 and 2016 (Greiner 2017).

Large data breaches such as Targets' 110 million card numbers and Home Depots' 56 million card numbers, have provided many learning opportunities for corporations, and have shown breaches as occurring either internally or externally. Research is lacking in the area of insider-outsider credit card breaches. My own research and experience in banking, asserts that there are different levels of internal-external schemes in existence and this should be studied, and evaluated as part of a good fraud risk strategy. Gaps in IT security, lack of specific governance, missed operational risks, incomplete policies, and one time only due diligence, all open the gateway to internal-external fraud and cyber-breaches.

Therefore, boards and management must also focus their efforts on developing internal-external threat detection and mitigation fraud programs to combat data breaches. On the enterprise level, an experienced Executive Leadership Team should be responsible for data protection, cybersecurity risks, control frameworks and allocating funds for data protection. In the past, preventing and controlling fraud was done at the local or regional level of business. But with the internationalization of economies, global banking and markets have created opportunities and risks for international frauds on credit cards. Collaboration on the international front is necessary to recognize and disable the increase in card frauds to limit other spin-off crimes such as ransoms, money laundering, and terrorism. An international body of federal authorities should be established to research, study, share information, and create a framework to investigate, fight and prosecute data theft, and cyber frauds.

The consequences of not addressing these issues in a timely manner will result in lost consumer confidence, falling share prices, reputational risk, financial and regulatory implications, class action law suits, settlement reserves and legal costs. Investors are becoming more interested in an organizations' Management Discussion and Analysis reporting on data breaches and cyber security exposures which can be material and vary in format.

1.2 Objective, background, and Scope of Research.

This paper examines the evolving trends in the Canadian credit card industry, and the technologies in place to prevent the frauds that occur as reported by the Canadian Banking Association's Credit Card Fraud and Interac Debit Card Fraud Statistics 2015, in the following categories: Lost, Stolen, Non-Receipt, Fraud application, Counterfeit domestic, counterfeit cross-border, Card-not-present, and Account take over (Appendix A). Credit card data is not only stolen to fraudulently purchase expensive goods, but this behavior extends beyond consumer shopping to play a role in the bigger picture of personal data theft cyber-crime. The nature of this manner of fraud can have global reach.

The motivation to write this paper stems from the need for further contributions to the field of Forensic Accounting, and to support future knowledge developments for other CPAs and IFAs working in the credit card industry. My personal experience in dealing with this area of fraud signals the need for awareness of the trends, the prevention and detection of card fraud perpetrated through card payment methods system-wide, and especially for those who are in the field of Risk Management, Identity Theft and Cyber-Crime.

Card data breaches are becoming more prevalent as fraud migrates to new channels and methods that are more difficult to detect. The challenges faced by the card industry is the slow response rate in detecting anomalies, customer behaviors, new patterns, predictions, the response time in reporting suspicious activities, and the lack of enforcement over installing appropriate technologies and specific procedures to secure and defend digital systems.

Card issuers are faced with customer and merchant demands for emerging digital and mobile payment technologies, safety over personal data and the additional resources required for new fraud management technologies and analytics. This has led to an increased need for outsourced third parties to support card issuers, oversight of their work, increased governance, increased regulatory complexity, capital costs of next generation Chip Kernels for contactless and mobile channels, and the expense of reissuing new cards after security breaches. There is also a limited ability to influence the Regulatory and Financial industry's policies and network rules. These all affect reputation, marketing risk, legal risk, regulatory risk, shareholder interest and value.

Examples of card fraud are presented based on recent data thefts in Canada and the U.S which include the *Home Depot Point of Sale breach* (2014), the *Ashley Madison*, cyber-fraud case, as well as two other small card rings identified here in the Greater Toronto Area in 2017.

On May 8th, 2017, in Toronto, the Globe and Mail reported that a cross border credit card theft ring stole ten million dollars from its victims. "Project Royal," as referred to by the Toronto Police, was investigated by the RCMP and U.S. Agencies alleging that a four-person fraud ring had intercepted stolen mail with both personal and credit card data. The "ring" reviewed this information for credit

worthiness, and the ability to apply for new credit cards, which amounted to application fraud and identity theft.

From organized crime to structured rings, cybercrime in credit cards is now involving low profile users, employees, and "normal" citizens.

Another recent case, reported by CBC News on Feb 17, 2017 known as Project Fellowship used counterfeit ids to open credit cards and bank accounts. Toronto police arrested a husband and wife from Ajax, allegedly involved in a fraud and money-laundering ring of fourteen participants. The scheme was estimated to have run for many years, with more than $8 million dollars stolen, and over 10 financial institutions in Ontario and Quebec defrauded. The woman, a 30-year-old Fraud Detection Agent worked at one of the top five big banks in Toronto.

The Globe and Mail Aug 23th, 2016, reported that a cyber-breach occurred when the Canadian-owned AVL Ashley Madison website, whose slogan is "Life is short. Have an affair," had their database of 30 million hacked and posted on Bit Torrent as a 10-gigabyte file with a link; it is still posted on the dark web. The database included priests, celebrities, government workers, the RCMP and the military, many of whom had used government networks. The leak identified customer names, addresses, card numbers, height, weight, and even some of their personal preferences.

The hackers known as the Impact Team, were disgruntled employees who accused Avid Life Media (ALM) (who owned Ashley Madison), of deceptive practices, and not delivering security over personal data as promised. The hackers explained AML was loose with data, created fake profiles of women, which was fraud and deceit by ALM and their members. This hacking incident had psychological,

social and economic consequences, as well as opportunities for spin-offs crimes. The Impact Team's breach was ethically provoked, and though popular opinion deemed this to be an act of internet vigilantism, nevertheless, the act was criminal with far-reaching consequences. AVL's management may have averted the breach if they had paid attention to the employees' concerns over weak security around personal customer data, immediately addressed the issues, resolved it internally, acted with professionalism, and kept detailed records of the incident.

With that in mind, companies that retain profiles, account information, and billing information data have a duty to implement a risk management and governance frameworks to identify risks over communications networks. A report from the Globe and Mail Newspaper on August 23rd, 2016 stated that "The Office of the Privacy Commissioner of Canada demanded the company build better internal security systems, offer users more control over their data in order to mitigate the risk of another data breach, and also remove the fake "security awards" the company had posted on its website."

The threats of hackers, insider-outside collusion, and operational risks must be addressed by merchants, financial institutions, and card issuers with the strict enforcement of an Industry standards-based internal control framework and IT Security program.

A dynamic best practices Fraud framework would include self-assessment tools to determine control effectiveness, education, and training to promote awareness and safeguarding of sensitive information through a Code of Conduct course, legal compliance programs, different frequencies of due diligence over employees, recurring security checks over contractors and third parties, surveillance video, electronic

communications filters, and a corporate culture that instills values such as integrity, a duty of care, safe guarding of assets, whistle-blowing, and the consequences of corporate misconduct.

The scope limitation is that the Canadian Banking Association's (CBA) Credit Card Fraud and Interac Debit Card Fraud Statistics, show card fraud trend to 2015, and has not been updated to 2016, to show the impact of new security measures such as Verify by Visa, 3D Authentication and biometric authentication.

2.1 Card Fraud Transactions and Consumer Attitudes in Canada

This research paper examines the overall trends of credit card fraud with a focus on Canada but with a global perspective based on documental sources such as the Canadian Bankers Association's Statistics on debit and credit card fraud in Canada from 2008-2015, other academic and industry reports.

I will focus on the CBA's categories of card fraud, their methods, and other characteristics as these results are relevant to the credit card, banking industry, customers, and other stakeholders because it indicates that as card usage increases, so will fraud.

The scope of this research will cover data on credit card usage in Canada (Bank of Canada, Method of Payment survey of 2016), which shows Canadians are shifting away from using cash to credit cards, transacting in two channels contactless Point Of Sale (POS), and the online transfer ecosystem, with payment innovations such as Online e-wallets, and e-commerce P2P (e.g. PayPal). These two payments channels will continue to be vulnerable to data thefts as card usage increases, requiring more viable and dynamic strategies to keep pace with the safeguarding personal information.

The Canadian Banking Association reported that with the 2016 conversion to contactless cards there were 68.5 million Visa, MasterCard and other credit cards were in circulation in Canada, and were used by 95% of the population. The growth in credit card volumes and values as reported in the Canadian Payments Methods and Trends survey 2016, found that over 40% of Canadians used their credit cards at an average of $1,700 in purchases per month in 2015, which increased 28% since 2011.

Cash transaction volumes as a payment method have steadily declined in Canada between 2011 and 2015 from 41% to 32% respectively, which occurred as a result of credit card marketing. Debit cards volumes increased from 20% to 24%, and credit cards increased 17% to 21.8%, which occurred as a result of evolving to electronic methods. Other payments types include cheques, paper, ABM, prepaid cards and online-transfers, which make up the other 22% have varied slightly between 2011 and 2015 (Fung, Huynh, Stuber 2015). The shift to increased credit card usage is led by convenience, efficiency, acceptance in 200 countries around the world, access to credit, and the idea of rewards through loyalty programs for cashback, gas and travel competitively marketed by card issuers and financial institutions.

In 2015, there were 4.75 billion credit card transactions made in Canada with a value of $489.5 billion. As card payments increase so have the merchant Point Of Sale devices, and in 2016 approximately 40% were contactless payment enabled. In 2016, it was reported that 16.9 M Canadians made contactless card payments (Tompkins, and Galociova, (2016). Due to the rapid pace of transition from cash to cards and e-commerce payments, few academic sources of research are available to track trends, document the fraud, and identify routes and strategies for future fraud analysis,

detection, and design of preventive measures. The present study hopes to contribute to this goal.

2.2 Analysis of CBA statistics 2015

The Canadian Banking Association uses two measures to describe credit card fraud which are transactions volumes, and consumer attitudes. Because of the close connection to technologies present in practically all dimensions of our globalized way of living, the technological aspects of fraud will be also discussed.

Lost, Stolen, and Non-Receipt credit cards

The Canadian Banking Association's Credit Card Fraud and Interac Debit Card Fraud Statistics – Canadian Issued Cards 2008 to 2015, reported that Fraud Losses in CAD dollars decreased as follows:

- Lost credit cards decreased from $16.5 to $11.2 million or 32%,
- Stolen credit cards decreased from $32.2 M to $20.6 million or 36%,
- Non-Receipt credit card decreased from $13.2 million to $6.0 million or 54%

The Average Amounts Loss per credit card account also decreased by 38%, 18% and 57% respectively. Debit Card fraud also declined from $104 M to $11.8 M but will not be covered in this paper. This is as a direct result of three factors:

i) Cardholders' use of the EMV chip card which requires a Personal Id. Number (PIN) to authenticate the cardholder as the authorized user

(ii) Chip data encryption which prevents card skimming, and,

(iii) Merchant installed chip enabled Point Of Sale terminals, which no longer store card data.

Chip encryption, tokenization and PIN authentication technology has eliminated skimming as a means of obtaining customer data, used in producing counterfeit cards in Canada.

Mastercard Payment Gateway services describes Chip Tokenization as a feature that removes sensitive cardholder data and replaces it with a unique one-time value when authorizing a payment. It replaces the card number in all documents requiring business data and analytics, and therefore cannot be used for external fraudulent transactions. There is also a multi-pay token that can be used for additional purchases made by the same customer profile, credit card and specific merchant. That specific merchant can process additional sales for the customer by submitting the token to a processor gateway with access to a token vault, which authorizes the payment. This circumvents card number storage, providing it by phone or email, and reduces Card-Not-Present fraud, online commerce fraud and the risk of card data breaches.

Counterfeit Domestic Card

The CBA's Credit Card Fraud Statistics 2015 also reported that from 2008 to 2015:

- Counterfeit Domestic Card Fraud Losses in $CAD declined from $162.2 million to $37.7 million or -77%
- The number of accounts decreased from 130,765 to 64,299 or 50%.
- Average Loss per Account declined from $1,240 to $582 or -53%

Counterfeit credit cards produced from stolen identities, have also declined in Canada due to the Chip encryption, tokenization and PIN authentication Chip being

extremely difficult for criminals to duplicate. As a result, counterfeit cards would most likely be used for online, and cross-border purchases in the United States because small and mid-sized US merchants have been slow adopters of Chip access POS terminals citing costs and certification by the issuers.

Card Issuers and banks have been supporting larger enterprises in migrating to CHIP terminals first, with smaller businesses last. Card data stored on the POS terminals and in data warehouses of larger entities, are used for marketing and customer analysis and are also seen as valuable target for fraudsters.

EMVCo was established to ensure card infrastructure uniformity, and global interoperability of secure payment transactions. It is comprised of representatives from Mastercard, Visa, Am Ex, Discover, JBC and Union Pay. EMV Co. reported that in the United States migration to EMV chip is still underway. At Q4 2016 EMV enabled transactions for both the cardholder and merchants were 18.6 % (Appendix B). Fraudsters will continue to exploit the remaining magnetic stripe Point-of-Sale terminals until they are completely replaced by Chip 'reader' POS terminals. It is evident that identity theft, counterfeit card fraud, and Card-Not-Present fraud will increase in the United States until EMV terminals become the standard.

The liability for losses shifted from the banks to merchants on October 1st 2015, however, it was not mandated in the U.S., which means that merchants were not penalized for non-compliance. U.S. Merchants could however be held liable for counterfeit or lost/stolen card frauds if their POS terminals are not EMV chip enabled.

Card-Not-Present (CNP)

Card-Not-Present fraud is increasing through e-commerce, mail and phone channels, and it is difficult for merchants to verify if the true cardholder is authorizing

purchase because EMV validation is not being used. The CBA 2016 Statistics show that between 2008 and 2015:

- Card-Not-Present fraud losses increased $128 M to $537 M or 318%.
- CNP Average Loss per Account increased to 20.5%.
- The CNP number of accounts increases from 210,430 to 730,945 or 247%

If a cardholder reports a fraudulent CNP transaction after the review of their monthly statement, the merchant's bank account (acquiring bank) where the payment was received must make restitution. Whereas, with a Card Present Transaction (which is read at a POS terminal) the Card issuer (MasterCard, Visa etc.) is liable for restitution. Merchants who do offer online shopping where the payment method is Card-Not-Present often face a greater risk of loss, and as a result, some card issuers do charge an increase transaction fee.

Card-Not-Present fraud is a financial loss to the merchant if the true customer disputes the purchase. Merchants who process CNP purchases should question first time large dollar orders, large volumes if the goods are easy to convertible to cash, if the billing and shipping address differ, if there are different card numbers from a single IP address, and especially if priority shipping is used, and the order is sent outside of the geographical region.

There is a Verified by Visa service made available by RBC, Scotiabank, TD Bank, and others, which allows the cardholder to register before shopping online at a participating retailer. This technology shifts any potential loss from the participating merchant to the Issuer (Visa). Each authorized user of the card must register with their own password, will have online viewing access to activity on the card, and be able to

make changes to email addresses or passwords using the Banks Personal Account Manager.

Verified by Visa Point of Sale authentication will become a payment standard, creating cardholder and merchant confidence, and decreasing Card-Not-Present fraud. Merchants will be inclined to enroll as cardholders will not have to re-key security details each time they shop on-line; another benefit is that "drop out" rates decrease when a customer decides to abandon a purchase. A joint compliance program between the Issuer (Visa) and the Banks (for example RBC, TD, Scotiabank) will monitor fraud and breaches to prevent further recurrences.

EVMCo and PCI Standards Security Council will also release a 3-D Secure 2.0 security feature in 2017 to enable cardholders to self-authenticate when making on-line purchases on PC web browsers. This will improve security over on-line purchases and reduce threats.

Account Takeover and Other fraud

With EMV Point of sale security over data, fraud has also shifted to Account Takeovers. The CBA Credit Card Fraud Statistics 2015 reported that between 2008-2015:

- Account Takeovers and Other increased from $9.6 M to $16.9 M, or 75%
- Average Loss per Account remained unchanged $3,397 to $3,301.
- The number of cards has increased from 2,844 to 5,109 or 79.6%.

This is in line with the strategy of avoiding suspicion by making smaller unauthorized purchases, on more taken over accounts. Account takeovers may occur when a hacker gains access through phishing emails for personal identification and

accounts, and infiltrates the accounts taking control of online banking or credit cards. The hacker can then make changes to contact and security information, make unauthorized purchases, and send electronic bill payments from a bank account to new or other fraudulently opened card accounts. The type of purchases are easily convertible to cash such as computers, gift cards, jewelry, cash advances, air fare and then they follow through with a bad cheque to "pay" on the credit card account, which results in a "bust out".

It is reasonable to anticipate that with the EMV terminals protecting card data, an updated IT security processes blocking malware, criminals will pivot their focus to users of mobile banking apps, through hacking and breaches of their credit card and bank accounts. Hackers, who are technically knowledgeable, gain access to mobile apps, on-line channels, infiltrating on-line bank accounts and compromising personal data, contact information and security information. Future solutions could involve new authentication methods using consumer behavior, and interactional signals that cannot be deceived in communicating with computers and wireless devices, such as voice response applications, using biometric or speech capability. Fraudsters being innovative, can also just as easily build their own ATMs and leaving them at bars, unsafe areas and tourist spots to skim card data.

Fraud Applications

The Canadian Banking Association's Credit Card Fraud and Interac Debit Card Fraud Statistics 2015, reported that between 2008 and 2015:

- Fraudulent Applications increased from $11 million to $19 million or 68.7%
- New fraud application accounts increased from 3,600 to 6,800 accounts, or 80%

- Average Loss per Account decreased slightly $3,038 to $2,742, or 9.75%.

Fraudsters, reacting to the EMV Chip's data security over Lost, Stolen, Non-receipt, and Domestic card fraud, have also turned their attention to Fraudulent Applications. Fraud application volumes have increased due to identity thefts from hacking, internal/external breaches at financial institutions, and purchases from the dark web. The average loss per credit card account decreased as fraudsters have attempted to avoid being noticed by staying under the radar with lower dollar purchases.

Visa, MasterCard, and other issuers have reacted and supported merchants by issuing new rules and guidelines and waiving the merchant's annual audit of Payment Card Industry Data Security (PCI-DSS), if 75% of the card transactions processed through the dual remain contact and contactless EMV certified device. Merchants who have not upgraded to chip-enabled technology will be financially liable for card-present Counterfeit Domestic, Lost and Stolen cards fraud that could have been avoided if a chip enabled Point of Sale system had been implemented. As of January 2016, there was 90.7 % EMV Chip penetration in Canada. (Appendix 2)

In the U.S., merchants have been liable for any card fraud due to not being EMV compliant since October 1, 2015. Customer awareness and chip-enabled advancements have deterred fraud, but are driving fraudsters away from manual methods to more elaborate, technologically based and electronic means of theft.

2.3 Mobile Payment Technology

Mobile devices such as Apple Pay, Android Pay, Samsung Pay and Master Pass (PC Bank) are the future of payment technology. Credit and debit cards apps on

phones gained momentum when EMV technology emerged to have near field communication (NFC), and tap-to-pay features.

Apple Pay uses the iOS wallet app to add credit/debit cards on the Apple watch, smartphone, MacBook and E-Mac to make "in-app" and on-line purchases. It also uses "tokenization" on the chip card to issue a random number for each payment, and requires thumbprint identification or a passcode to process a payment. This ensures all personal data remains on the phone's app and not on the Merchant's card reader, eradicating stolen card data and fraud. Apple Pay is supported by more banks, merchants and card issuers that any other mobile devices, and is available in China and the U.K.

Android Pay stores debit, credit, gift and Loyalty cards and also uses Near Field Communication to transfer a virtual account number to the EMV Point of Sale terminal. Unlike Apple Pay, however there is no fingerprint authentication.

The Samsung electronic wallet is available on Samsung products such as the Galaxy S6 Edge+, Galaxy Note5, Galaxy S6, and Galaxy S2 and S3. It works with both types of card readers using Near Field Communication and Magnetic Secure Transmission (MST). Their securities features include verifying purchases by thumbprint, PIN, with a random number generation instead of a credit card number. It cannot be used with in-app purchases, but can be used on more POS terminal because of MST. All credit account information is encrypted and stored on a vault.

Credit card issuers and banks place risk mitigation controls on mobile wallets, when used at a EMV POS terminal with NFC, using radio-frequency identification (RFID) there are purchase limits, and limits by location as well. For example, purchases up to $100, can be tapped, those over $100 require a PIN to complete the

transaction. In the United Kingdom, contactless cards have a 30-pound Sterling limit and after 3 transactions, a PIN is required, which lowers the risk of fraud.

The 2017 CPA Canada Fraud survey reported that 71% of the participants believe that electronic payments made by tapping debit and credit cards or smartphone apps, makes fraud easier. This belief is partially responsible for the slow adoption rate for mobile devices. However, users will adapt with the trend of corporations encouraging staff and third parties to Bring Your Own Device to work, for use and integration with the company's platforms such as email, SharePoint and videoconferencing.

Organizations have recognized that data moves and can reside anywhere and that mobile devices can be the in-points for security breaches, therefore data privacy and security will have to move with the devices. The CPA D&A 2016's article Passion and Purpose featured Nandini Jolly, CEO of Cryptomill Technologies in Toronto, who designed "Circles of Trust" a software that encrypts data wherever it is stored, enabling secure, private sharing of data and collaborating within and outside organizations.

Even if hackers invade the networks, the data is encrypted, only shared with authenticated recipients, and the user is only given the level of access provided by the originator. If the data is downloaded, the originator stills controls the access, and can revoke it. The concept of Privacy By Design developed by the Information and Privacy commissioner of Ontario recommends being proactive and preventative from the start, not only trusting in compliance, legislation and frameworks, but asserts that Privacy assurance must become the organizations default mode of operation.

Future innovations on mobile devices will improve on user interface (design), will simplify user flows, and will expedite one-click payments. New security features will be in biometric authentication apps which scan the owner's face to make a payment.

3.1 Identity Theft and Phishing schemes

Typical Identity fraud may occur through socially engineered hacking, fake websites on social media, mass marketing, phishing techniques, all which scam people into inadvertently providing personal and banking information. Identity theft is the unauthorized use of a person's personal information used with an intent to commit fraud. Personal information includes debit and credit card numbers, email address, passwords, social insurance number, driver's license number, health card information, hospital information, business contact information etc.

In the following case of the Toronto "Project Royal" credit card and identity theft, it was alleged that there was collusion with employees in the financial industry. Identity theft rings can conspire with "moles" working in the banking system to commit insider identity theft by robbing customer accounts, adding authorized users or opening fake credit cards in the victims' names. As a result, banks do more than just credit checks, screening, and training of new hires. There are continual due diligence checks, regular credit checks, review of employees' accounts opened, and monitoring of the accounts the customer service representatives log into, routinely looking for patterns and anomalies. Credit card and banking employees are not permitted to keep customer data on their laptop, accessing it only through a SharePoint site, or through application such as TSYS and First Data Resources that log the accounts reviewed.

Employees who do have customer data should only use a desktop at the office, and have encryption on credit card numbers.

By benchmarking employee activity to other employees in the same job, by reviewing link analysis to spot associations between employees, by reviewing dormant accounts that are accessed, by reviewing client accounts when the client is not at the bank, reporting negligence, web and file usage, instant messaging, screenshots taken, downloaded software, use of a USB to save information, these are then all be used to determine if there is collusion and internal breaches of customer information. It has been said, there are informants or "moles" working in every bank, reporting to organized crime networks.

As an example of the above, a Customer Service Representative who has worked at a bank for 10 years, has recently gotten married to an extended family member of a mobster's family. It is possible that one day, the bank CSR would be told to get information on a specific customer's purchases and location and provide it to the mob family. The mob would know the customer's whereabouts, placing the customer in imminent danger. Here is an example of a case as reported in The Toronto Star on May 8th, 2017 demonstrating internal breaches of customer data:

"On May 8, 2017, in Toronto, it was reported that a cross border credit card theft ring stole $10 million from its victims. Four Toronto men lived a lavish lifestyle, spending money as fast as it came in on items such as expensive cologne and shoes, as part of an alleged identity theft ring that bilked banks out of $10-million, according to police. The cross-border investigation—dubbed Project Royal—involved Toronto police, the RCMP, several provincial ministries and U.S. agencies, and has led to charges against two men and arrest warrants for two others.

> "Detective Mike Kelly said one of the men allegedly had connections with people who had access to legitimate identity

> information for a price. He said police discovered a notebook with about 5,000 names of Toronto-area residents along with their identification information, including credit card numbers. The perpetrators would check the credit of those on the list to see if the information was worth using, then somehow get the companies to issue new cards to a "legitimate person" and intercept the cards in the mail, Kelly alleged." (The Toronto Star, May 8, 2017)

Card issuers do have processes in place to mail the new credit card to the client's address first, and then mail the PIN number in a separate envelope, a few days later. In this case the "Project Royal ring" must have maintained a stake out, intercepted both letters, activated the card, and likely used it for on line purchases in Canada, over the phone (card-not-present), and for on-line and cross border transactions at merchants in the US who are not Chip and PIN ready.

Card issuers use technical solutions that compare the devices GPS real time location to the merchants address and to any suspicious activity that recently occurred at that location, it is this decisioning that determines if a suspicious transaction is about to occur, and then declines the transaction. An online solution, verifies the mobile device's number to the phone provider's records and sends a passcode to the device to be entered on its login screen, thereby confirming if the owner is holding and using the device. If it not confirmed, the transaction is not processed, and through manual investigation, it is either verified or determined to be fraud at another location.

Canadians do have serious concerns about card fraud and identity theft, and on the 2017 Chartered Professional Accountants of Canada (CPA Canada) Fraud Survey conducted by the Harris Poll, of 1001 adults surveyed, 320 reported having been a victim of credit card fraud at a rate of 72%, followed by debit card fraud at a rate of 28%.

Financial institutions share the same concerns on fraud, and in The Toronto Star article of July 22, 2016, "How Canadian banks are turning to biometrics to use your body to fight fraud" it is reports that banks and financial institutions are the early adopters of biometrics in response to Know Your Customer, and to fight money laundering and fraud. Security and identity verification techniques can recognize an individual from iris scanning, face recognition, speech recognition, fingerprint scans, and the electrical activity of your heart.

Financial institutions such as RBC and TD are testing and are ready to launch more biometrics, voice recognition is already in use. With the rise of the fintech sector, biometric authentication will likely be included in the PIPEDA Regulations, as mobile devices and card issuers are already using fingerprint and facial recognition which are improvements over the current regulations to protect against data security and fraud.

Phishing Schemes

At every point of person-to-person or person-to-organization contact in our society, the first request is to provide an email address, with little or no contemplation or warning given over providing this information. Hackers known as "Spammers and Phishers" send millions of email messages daily, in their search for potential victims. Voice phishing is still in use, and occurs when a fraudster uses a landline telephone service to contact a bill-payer by name, and authoritatively commands that money is owed on an invoice, or a server issue exits, or that a bill payment was not fully completed and they would like the card number and other personal information to correct it. The result can be an unwittingly given credit card number, address or other information which is then used for identity theft, card fraud schemes, and to access computer network architecture for theft of intellectual property, customer lists or

strategic information. The fraudster can use Caller ID "spoofing" to display a number or business name of their choice i.e. the Canada Revenue Agency, Microsoft, your Bank or they can use an automated system IVR to dial into the cardholders' numbers for bank account information.

Banks use an automated IVR system to allow customers to make changes to their PINs. If criminals know the security questions such as the customer's date of birth, postal code, mother's maiden name possibly obtained from mail theft, the internet, or black market, the fraudster could reset the customer's PIN and completely takeover and drain the account. In general, the public must be suspicious and practice caution in protecting their identity, card numbers or bank account numbers because email and voice phishing are difficult for the police or other agencies to monitor or trace.

Please see the email below which I received supposedly from CRA on May 25, 2017, requesting my credit card account number.

From: Canada.Revenue.Agency.CRA-ARG.TAX.message.2017.BFM.msg.7511387783-VOEF@CRA-arg.dot.CheapAirMailer.com <Canada.Revenue.Agency.CRA-ARG.TAX.message.2017.BFM.msg.7511387783-VOEF@CRA-arg.dot.CheapAirMailer.com>
Sent: May 25, 2017 3:10 PM
To: xxxxxxx@hotmail.com
Subject: CRA - Tax return: balance update [May 25, 2017 VO7voef]

Canada Revenue Agency (CRA-ARG) After the final
2017 annual calculations of your fiscal activity
we have determined that you are eligible to receive a tax return of **403.27 CAD**.

Please **submit the tax return request act** by having your tax refund **sent to your credit card within 48 hours.**
To release this hold please visit the link below and proceed through our secure form:
For tax refund click here » Please follow the instructions on your screen once you reached our secure server.
If you have already confirmed your information then please disregard this message.
(c) 2017 Canada Revenue Agency | (Rec-ID-pm: JVVKU-377J3-j3773|smtp.mcs.fr);

Email Phishing scams are sent via text messages and fake websites designed by criminals to "brand spoof" and imitate the logos and websites of well-known, trusted, businesses, financial institutions and government agencies attempting to elicit a quick reaction, and dupe the cardholder into providing credit card or bank accounts with the intent to defraud.

Sproule and Archer (2012), surveyed Canadian participants on the preventative methods cardholders' and Card associations used to safeguard personal information, this included account monitoring, agency monitoring, password security, and the avoidance of risky behavior. It was found that cardholders latch on to one method of safety, and ignore other components of vigilance. In 2008 Sproule and Archer reported that 6.5 per cent (estimated that 1.7 M) of Canadians had been victims of identity fraud in a single year. The financial loss to Canadian victims was approximated at $150 million, and it is estimated that it took 20 million hours to recover from the resulting psychological impacts, time to request new identification, lost work time and other missed opportunities. Cardholders should also assume some of the responsibility to protect their data from man-in-the-middle interceptions, and knowing who they are giving their data to.

In Canada, the Uniform Crime Reporting Survey (UCR2) has official police statistics reported on identity theft, and in 2010, police-reported 796 cases of identity theft and 6,141 incidents of identity fraud. The Canadian Anti-Fraud Centre collects information on criminal intelligence and identity related fraud and recently reported that between January and November 2016 over 17,000 Canadians reported being victimized by identity fraud and incurred losses totaling $10.7 M. This represents a reported increase of 177%.

This has led to extensive research and development of new detection systems which have since surpassed the traditional statistical methods and machine learning techniques. The article Statistical Methods for Fighting Financial Crimes (Sudjianto and Yuan 2010) explained the methods used as a) Suspicious Activity Identification, d) Case prioritization for further investigation, c) human investigation to analyze the card's transactions by amount, merchant, frequency, channels used, if it seems abnormal for the cardholder i.e. Counterfeit card or fraud application and d) Filing the suspicious transaction report with FINTRAC in Canada or FinCEN in the US.

The challenges noted in designing effective systems to detect suspicious activity in real time includes the complexity and volume of transactions by channel, the imbalance between legitimate vs illegitimate transactions, concept drift which is the dynamic and evolving patterns in detecting fraud require the algorithms to be retrained; and class overlap which is the strategies that fraudsters use to make illegitimate transactions look normal.

In Canada, Bill S-4 the Digital Privacy Act (PIPEDA) amended the Criminal Code for theft and included 3 new offenses related to identity theft related crime and misconduct, which are subject to 5 years in prison. There has also been a restitution provision which allows for the reasonable expenses that one may need to reestablish their identity, includes replacement of identity documents, and the updating of credit history and credit ratings.

On Jan. 19th, 2017, the Canadian Securities Administrators published CSA Multilateral Staff Notice 51-347 Disclosure of cybersecurity risks and incidents which was based on 240 S & P listed entities, who had filed cyber security disclosures on the impact to business operations, if sensitive material had been exposed, who took

responsibility for the attack, and if any previous incidents occurred, and why they might be exposed. The area of timely disclosure is also a concern, as it takes time to assess, determine the materiality, and estimate the number of accounts or financial loss. This requires more systems ability to detect and track information to on how and when breaches occur.

3.3 Personal Information Protection Electronic Documents Act (PIPEDA)

Financial institutions have a legal obligation to protect consumers' data in compliance with The Personal Information Protection and Electronic Documents Act (PIPEDA). This federal privacy law, for private-sector organizations governs and protects the privacy of individuals and the collection, use and disclosure of personal data without the knowledge or consent and of the individual, by an organization in both electronic and non-electronic form.

Regulated entities have been given more flexibility in how they verify identification before opening accounts and accepting transaction. PIPEDA has recently updated the identity verification methods including those used by credit card issuers. After June 17, 2017, the Regulations have set out the following 2 of 3 methods to be used:

- "Referring to information from a reliable source containing the name and address of the person being identified and verifying that the name and address are those of the person.
- Referring to information from a reliable source that contains the name and date of birth of the person being identified and verifying that the name and date of birth are those of the person.
- Referring to information that contains the name of the person being identified and confirming that the individual has a deposit account

> or credit card or other loan account with a Canadian financial entity and verifying that information".

The "two out of three" method for identity verification must be from other independent sources than the person whose identity is being verified by themselves. While PIPEDA allows more flexibility over identity verification, it does not yet consider the use of biometric methods (voice, face, heart rate), or their submission through live video connection.

PIPEDA in 2016 also provided guidance over the Internet of things, which are a group of devices that connect to and exchange data over the internet, applications, and cloud service providers. Examples are as Smart watches, health monitors, IP security cameras, and connected cars. While not directly personal when this information is combined it can create a profile that discloses a person's habits, health, and lifestyle, which then become personal data. This information must be protected by physical organizational, and technological measures. As per Clause 4.7 of PIPEDA if a loss, unauthorized access, or unauthorized disclosure occurs, then under the Digital Privacy Act it must be reported to the individuals and to the Privacy Commissioner.

Then companies who design devices as described under the internet of things, must inherently consider cyber security, building it into the device, with monitoring auditing and analytical tools in place, to protect from unauthorized access and breaches right from the start of product development.

3.3 Financial Institutions fight crime with Big Data Analytics

The difference between an auditor finding irregularities through random sampling and IFA finding fraud is that it is not random. Big data analytics improves the accuracy of finding fraud with inexpensive and powerful computer tools

identifying anomalies in real time, this allows the user to investigate and confirm or refute it if it is unlikely be fraudulent. These results decrease false positives and false negatives. Big Data is based on large volumes of data that is structured (a highly organized relational database), semi structured (such as emails) and unstructured data (all else), all of which affect the speed of assimilation (Debenham, 2016).

Banks and financial institutions rely on Big Data to comply with various statutes including data protection, money laundering and anti-terrorist financing. Big Data analysis identifies "corruption" based queries on Financial Action Taskforce on Money Laundering compliance, and transactions with organizations on the list of noncooperative counties and territories. The list is infinite and includes Cash transactions just below Regulatory reporting thresholds, cheque tampering due to not matching the cheque issued to the bank or deposit, skimming and kiting, duplication of credit card transaction number used at different locations, account takeovers, sudden activity in dormant accounts, isolate mortgage fraud schemes and "straw-buyer" scheme indicators (Debenham, 2016).

In the case of preventing employee fraud, a chain of transactions may cause suspicion such as the number on enquires made on a customer account, and the transfer of those funds to another account. Through payroll records, next of kin, addresses, schools and other names a link may be established between the employee and where the funds were transferred. Merging the internet and Big Data's use of unstructured data such as Facebook, LinkedIn, and personal emails may show associations between employees, and accountholders to fraudsters and their business activities (Debenham, 2016).

Some of the new features used by DBA include: 1) predictive coding or algorithms to process large amounts of e-documents for evidence of fraud, rather than a fraud analyst using keyword or number searches ii) Combining data such as Mapquest to find health clinics with the age of a patients visiting them, and with the results on map with clusters, allows a researcher to suspect health care fraud if a person uses a clinic more than 20 kms outside of their area where they are not known (Debenham, 2016).

Using Credit cards as the data base, fraudulent and non-fraudulent transactions can be compared and analyzed for being statistically significant using the following red flags: amount of time between transactions, number of declines, number of cash purchases, number of ATM transactions, Merchant code, and transaction amount (very small or very large). These are relevant as fraudsters work quickly to buy high end jewelry, electronics, and take cash advances before the card is detected as suspicious and cancelled. Scoring is done based on 1 or more" red flags identifies 79.4% of the frauds and 2 or more" red flags captures 54.9% of frauds etc. It is then up to the decision makers to allow or revoke or suspend the credit card transaction.

Behavioral analytics are also used, which saves the account holder's activity on each session, from login to logout, what is bought, when, if it is from a phone, laptop, tablet or other mobile device, the geographic location. From there BGA predicts when the hacker makes an "account takeover" by using the customer's account from another device and with behavioral anomalies, provides a probability that someone other than the customer is making the purchase.

When a suspicious transaction is identified, the financial institution has a duty to protect their interests, the affected persons' interest, and the public against fraud or

crime. One limitation of Big Data is that is uses mathematical models, which do not explain why transactions are suspected as fraud, and therefore it is left to the stakeholders to decide their criteria for decision making.

4.1 Cyber Security Threats

Recently, fraudsters have been using mobile device hijacking through malware infections through mobile apps that simulate random clicks to distribute denial of service, investment scams and fake websites. Cyber spies use malware with keystroke loggers that hack the passwords, allowing access to set up "back doors" to download corporate data. Other ways of gaining access to associated corporations, is to create a "watering hole" which infects websites with malware that spreads to visitors of the site, and transmits digital signals back to the hackers. This then provides entry points to large organizations and their clients such as private health insurers and their suppliers. In response organizations must use detection tools to scan for intruders who may gain open internet access on company computers, though employee mobile devices, and ensure employees don't ignore warning about unsecured flash drives or fail to update software. Stolen data can be sold to competitors, organized crime or foreign governments. Testing and remediating affected applications, database and network vulnerabilities is critical, and so is using external expertise who can audit and recommend recovery plans and solutions.

The Price Waterhouse Coopers' Canada's 2016 Global State of Information Security Survey in which 157 Canadian organizations responded, advised that cybersecurity related threats increased by160% year over year with the objective of data thefts and crime.

The 2016 Charter Professional Accountants (CPA) survey found that and the

American Institute of CPAs found that preventing security threats was the top technology related priority among accountants in each organization. Of concern, were mobile device vulnerabilities and sophisticated, persistent cyber threats. Cyber-security concerns of Canadians align closely with those of professional accountants in Canada and the United States. This awareness gives CPA's the power to influence their clients and employers over the need for updated technologies, policies, procedures and budgets to protect their digital assets from breaches that are estimated at $4 million USD on average.

Rajesh Kumar, Deepak Kumar (2015) in the article Top 5 Cyber Frauds lists the categories of malware as Trojan, Adware, Worm, Virus and the downloader, which break the security protocols in the IT systems, provides remote access to the infiltrator and sends data on the system to a third party without the permission or knowledge of the user. The most numerous frauds have been Tax refund fraud, corporate account takeover, identity theft, theft of sensitive data (background and behavior), and theft of intellectual property.

Cybercrimes are growing because governance is needed over the use of the internet, which has largely been used as a platform for sharing information, research and communication. The lack of policies and monitoring over the internet has made it difficult to locate the origin of cybercrimes and the persons responsible, highlighting the need for an international Cyber Security body to investigate cross border crimes. While Interpol represents collaboration between police services, a specialized federal agency should be created to focus on reporting and sharing information. While other agencies cooperate, the question remains on the level of commitment allocated to cross border crimes (Button 2012). Apart from phishing, skimming, and cyber theft of credit

card and personal information, another type of cyber-attack occurred recently, known as the Ransomware attack of May 12th, 2017.

A massive ransomware worm which used a "wannacry" virus hacking tool", affected 200,000 victims in at least 150 countries, its victims were requested make payment in Bitcoins. Sent via a phishing email it invited users to click on a link that looked like it came from a reputable organization, FedEx, after which a malicious software infected computers with a virus that blocks access to the hard-drive and "kidnaps" it.
Microsoft President Brad Smith acknowledged that the hacking tool was created by the US National Security Agency (NSA) and had been leaked online in April 2017.
The prevailing global response was the need for public education, enhanced security over computers, defenses, and the role that national governments should take in internet security. (Khomami and Solon 2017)

According to Button 2012, there seems to be "scope for the development of single bodies to administer data at a national level covering a much wider range of information that is collected to common standards which is then shared at the international level".

The CPA magazine March 2017 article Eye Spy recommends that key meeting rooms be swept for "bugs" regularly, warn employees who attend trade shows that spies use these types of events to gather information, have guidelines over the use of flash drives, question if competitors may have insider knowledge, train employees on recognizing phishing emails, and retain experts to recognize signs of breaches, espionage, and how to respond to such attacks.

4.2 Data Breach Trends Study

Holtfreter and Harrington, 2015 in their article Data Breach Trends in the United States, combined 2 sources data on security breaches, to analyze and create a

framework which could be used to design strategies for safeguarding personal information. They created a new data model based on the Privacy Rights Clearing House, (a US nonprofit consumer education and advocacy project whose purpose is to advocate for consumers' privacy rights in public policy proceedings), and the Identity Theft Resource Center.

The PRCH categorizes security breaches as having occurred from 7 sources; i) unintended disclosure - mishandled or sent to the wrong party via email, fax or mail, ii) hacking or malware, electronic entry, iii) payment card fraud on magnetic strip card terminals used in the United States, iv) legitimate insider access and intentional breaches, v) physical loss such as stolen laptops, smart phones, portable hard drives, etc. vi) Stationary device that were lost, discarded or stolen, and vii) by other unknown methods.

The US Identity Theft Resource Center, classified types of breach as i) data on the move, ii) accidental exposure, iii) insider theft, iv) subcontractors and hacking, and the industries affected as business, financial/credit, educational, governmental/military and health care. Their study used the PRCH's records of 2,280 reported security breaches and 512,289,020 related data compromises for the years 2005 and 2010.

Of the 2280 reported data breaches 38% were internal, 56% were external and 6% were unknown. And from the number of compromised records 13% was internal, 86% were external and 1% was reported as unknown. The "Unknown" could be due to an insecure flash drive, with a virus on it, or either no method of detection existed at these organization.

The results of this study showed that the majority of Internal breaches fell under Operational risks which led to improper security over the protection, disposal

andtransit of data. External threats executed by hacking and theft far outnumbered Internalthreats by 56% compared to 38%. External hackers target larger organization tomaximize the number of data records they can compromise in one attempt. The following recommendations were made:

Internal breaches	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**Total**
Internal - hacking	1	2	1	6	4	15	29
Internal - theft by a current/ former employee - low probability of fraudulent intent			2			4	6
Internal - theft by current / former employee - absolute or high probability of fraudulent intent	6	20	17	21	28	87	179
Internal - loss of data ie a computer lost in transit	3	24	32	27	27	10	123
Internal - improper protection/ disposal of data	24	90	111	90	63	151	529
Total Internal	**34**	**136**	**163**	**144**	**122**	**267**	**866**

Table 1. Internal Fraud Security Breaches.

Adapted from Holtfreter and Harrington, 2012

External breaches	2005	2006	2007	2008	2009	2010	Total
External - hacking, unauthorized intrusion	50	79	76	62	52	96	415
External - partner/third-party theft or loss of data by improper exposure or disposal	13	52	42	26	14	33	180
External - theft of data by a non-employee with low or no probability of fraudulent intent	8	31	28	27	16	43	153
External - theft by a non-employee with absolute or high probability of fraudulent intent	27	155	122	72	48	105	529
Total	**98**	**317**	**268**	**187**	**130**	**277**	**1277**
Unknown (Non-traceable)	4	29	20	24	17	43	137

Table 2. External Fraud Security Breaches.

Adapted from Holtfreter and Harrington, 2012

1. Employees, contractors and third-party vendors should be trained on the risks

of managing personal data, and the security around in-transit data. Also implement criminal background checks.

2. Restrict access and implement fingerprint validation on entering the Data Centre.
3. Develop a policy to remove all access from former employees/third parties upon leaving the company.
4. Perform due diligence checks and industry ratings on Service Provider used to
5. Implement security practices over internet data security. In this study 25% of breaches and 50% of the compromised data was due to external hacking.
6. Limit direct access to servers by unauthorized personnel, have a segregation of duties between access to servers and restricted access to network data security.
7. Data centre security should be outsourced to a data center that provides internet network data security, a disaster recovery plan, and a strict physical data security to prevent access by any unauthorized personnel.
8. Upgrade to Internet network data security firewalls.
9. Implement remote network security backups, test, replicate and safeguard backups regularly.

While this study aspired to create a framework for the strategic management of internal and external breaches, it is evident that further research, investigation and classification is needed to track and trace the threats from insiders to external parties who collude to compromise sensitive data. The data also shows that for the 6 years between 2005 to 2010 data breaches increased as did the number of compromised records.

The flawed assumption is this study is that breaches are internal or external, when in fact it can arise from human error and negligence, not following policies, and outdated technology or software scans that fail to detect the malicious intent of intruders. The efficient protection over sensitive data and devices would have reduced access and risk of loss, from external breaches.

In general, there are blurred lines between internal and external networks and these access points must be identified and blocked to protect the organization's devices and data. One of the goals of a Board of Directors and management should be to create a security mindset throughout the organization. Previously the Chief Information Security Officers' role was to oversee the Information Technology, and computer systems supporting the CIO and the organizations goals. It should now involve formulating a security position for management and the Board, managing cyber threats and advocating for security investments. The CISO will also play in role in customizing a risk management strategy for all employees and third parties in compliance with safeguarding data and devices.

Home Depot Data Breach 2014

In reviewing the Home Depot cybersecurity breach of 2014, all the recommendations of the Holtfreter/Harrington 2015 study were applicable and had they been implemented would have prevented the breach. The question remains then why have organizations shown a "relaxed attitude" in prioritizing effective governance security over data breach and cyber fraud? The benefits obviously outweigh the costs.

Card issuers, financial institutions, Communications and IT service providers, and governments and other stakeholders should consider developing an Insider - Outsider Threat Detection and Mitigation Fraud Program, relying on polices and

technology to monitor and gather company data sent in emails, web gateways, cell phones, virtual devices and the cloud to non-business associates and entities. And once there is a threat, forensic accountants and forensic tools should be used to investigate and document the information for reporting it and prosecuting it.

Home Depot 2014 Data Breach

In September 2014 Home Depot reported that it had suffered a data breach in Canada and the US which included 53 million email addresses and 56 million credit and debit card payment data.
Criminals used a stolen password from a third-party vendor to log on to their network, and then acquired additional rights to navigate their networks. The hacker released RAM
scraping malware on the self-checkout systems to copy payment card data, email address and passwords. Once the hacker accessed the network, they looked like any other vendor or employee updating the system, making it difficult to detect as being unusual or suspicious.

The hacker then took their time stealing large amounts of data. Process improvements meant to gain efficiency over payroll costs allowed large companies to give vendors and supply chain merchants access credentials to networks such as Home Depot's.

Vendors can update Purchase Orders, show fulfillment of orders, and upload invoices for payments. With vendors focusing more on their core business, manufacturing and delivery, they may not be as aware of security over their systems and employees, implementing separation of duties, and safeguarding or limiting access to systems.

Vendors may be using outdated software, not have updated internal controls, or not be aware of who has been sharing or selling passwords to their retailers' systems.
Home Depot's breach shows us there is a greater need to have due diligence over vendors, tighter controls over the integration of inventory modules, segregation of duties on teams, and security over vendor systems that are not using encryption.

One of the control weaknesses is that Home Depot's payment network was not segregated from the rest of their networks, which would have prevented the criminals from gaining access rights to both.

To respond to this breach, Home Depot updated their Point of Sale in the US to accept EMV (Europay, Mastercard and Visa) Chip and Pin cards systems which was already available from 2014. The chip in the card encrypts the card number and does not allow it to be stored in the POS system. Point to Point encryption (P2P) on all payment

transactions, would have made the data unreadable and prevented the breach. (Brett 2015)

The Home Depot Security / IT staff should have had a security policy, privacy and security training for staff and third parties, a customized risk management policy and made the transition to EMV terminals which was available in the US. In Q4 2016, it was estimated that 52% of cards in the US were EMV compliant, and just 19 % of all vendors have upgraded systems to process chip enabled cards.

The consequences of a breach such as Home Depot email's and credit card breach is that information is sold to brokers who in turn sell it to carders on the internet's deep web. Counterfeit credit cards are immediately used to purchase gift cards from Amazon, Apple, Best-Buy etc. which are then used to purchase electronics such as game consoles, computers and cell phones. Innocent parties are hired to work from at home in the US, diverting attention away from the fraudster, and their address is used to reship these goods to someone who has bought the electronics from a website such as EBAY, where the fraudster posted the goods for sale. As the banks, financial institutions and Card issuers strive to monitor, trace and block activity on thestolen cards, the 'carders' have moved quickly to sell the electronics and cash out.

The 3 lines of Defense Model

Whether an organization is small, medium or large, regardless of it complexity its governance can benefit from a control based environment, a risk management strategy and from the independent review of external assurance if it is a regulated industry. An entity's Board and senior management are accountable for setting clear objectives, defining the strategies to achieve its objectives and implementing the

corporate governance structure that mitigates the risks in accomplishing the objectives. The Institute of Internal auditors defines the three lines of defense as

- functions that own and manage risks,
- functions that oversee risks and
- functions that provide independent assurance.

In additional the management should clearly define the roles and responsibilities, to ensure there are no gaps or duplications, and understand how each function fulfills the risk and control framework.

Operational Management fills the role of the first line of defense, designing procedures, identifying and implementing controls to mitigate risk on a daily basis while supervising the daily processes. Management is expected to recognize and correct deficiencies, exceptions and control breakdowns, by complying with internal controls. Since the first line of defence is in direct contact with transactions and processes, there should be a formal process to report any deficiencies, risks and their correction upwards to senior management so that controls and trends can realign and update polices and procedures to prevent their reoccurrence.

The second line of defence is filled by the Risk Management and Compliance functions, and its role is to implement a Risk Management Framework to assess, define, communicate risk exposures throughout the entity. Some of the responsibilities include identifying emerging regulatory issues, new laws, monitoring the adequacy of internal controls, guidance and training on risk management, accurate reporting, timely management of deficiencies and recognizing the need for shifts in risk appetite. It is

reasonable to expect that the second line of defense should also provide feedback and quality assure the first line in provide defences against risks.

Internal audit provides the third line of defence, they provide independent review over the effectiveness of internal controls, risk management objectively assess ow line one and line two accomplish their roles and responsibilities. Internal Audit objectively reports to the Board of Directors, on topics such as the efficiency and effectiveness of controls over operational processes, the safeguarding of assets, the accuracy, reliability and integrity of financial reporting, planning and regulatory reporting.

In addition, external audit, rating agencies, the regulators such as Ontario Superintendent of Financial Institutions also provide additional assurance, and information on trends, new threats, new laws and economic or industry specificguidance. For example, OSFI recognizes that external fraud may be currently categorized a business risk as opposed to operational risk, and suggests that entities reconsider external fraud events in the definition of operational risk for risk management purposes.

The 2015 OSFI exposure draft describes the three lines of defence much more concisely than the 2013 IIA position paper, although it follows long established risk governance and assurance methods. The exposure draft states that the first line of defence should report upwards on residual operational risk. However, the OSFI draft does not consider that the role of the second line of defense is also to also assist the first life of defence in reporting on and assessing the risk event. It also does not elaborate on the third line as having to assess and report on the reliability of the first line of defence's residual risk report, or the second line role in guidance and providing

assurance on the first line's efforts. It is evident that enterprise wide cooperation and a shared mindset over risk and the protection of data is part of good comprehensive governance.

The COSO Framework

The COSO framework updated in 2013, was prompted by the need for increased governance, the effects of globalization, the complexity of business transactions, increased regulatory reporting and new laws, greater expectations for accountabilities and competencies, technological advancements, and most importantly the need to prevent and detect fraud, as criminals react to controls and move on to more advanced schemes.

There are 17 Principles cited that are considered necessary for effective internal controls, which are organized under the following 5 integrated internal controlcategories: Control Environment, Risk Assessment, Control Activities, Information and communication, and Monitoring Activities. (See Appendix 3).

An awareness of how and where fraud may occur and its prevention is the first line of defense in an organization.

Principle 1. The Control environment.

The governance function of an entity mandates that an effective risk Fraud Risk Management strategy be implemented, with policies and procedures that clearly communicate the Board's and management's intent to manage fraud risk. The Board as fiduciaries, also set the Tone at the Top to demonstrate their ethical integrity and establish the internal control standards for management, staff, customers and other third parties. The Board has oversight for the entity's financial accountability, internal

control environment, fraud risk framework, lines of authority, and responsibility to attract, hire and retain skilled competent staff.

Principle 2. The Fraud Risk Assessment.

Management must be proactive in creating a single, comprehensive fraud Assessment program that is dynamic and timely. It is customized for the organization and explicitly identifies the likelihood, impact and management of fraud risks such as financial statement misrepresentation, misappropriation of assets, corruption, bribery, theft of personal information, and other illegal activities.

External experts such as audit firms are beneficial in developing the scenarios on inherent risk, likelihood and impact of occurrence, and the response to the inherent, likely and residual fraud risks. Clear and appropriate preventative and detective strategies assist management in prioritizing, and providing resources to mitigate fraud risks. The COSO 2013 Framework Principle 8 specifically addresses this as "The organization considers the potential for fraud assessing risks to the achievement of objectives".

Principle 3. Control Activities.

Control activities are specific policies and procedures for management approved processes that either prevent fraud from occurring or fail to detect it in a timely manner. The selection, application and monitoring of fraud controls are essential in preventing key fraud events from occurring. Fraud control activities are documented to identify the action and scheme, the controls that mitigates the risk, and the role / or person that is responsible for performing the control activity. Detective controls are also implemented to expose fraud activity when preventative controls are

bypassed. The fraud risk program assesses the policies and procedures for each process to be evaluated.

Principle 4. Information and Communication

It is not cost effective to eliminate fraud with established controls as processes and technologies are ever evolving. Therefore, management must also rely on formal channels to receive input from internal audit, employee tips, feedback, and "accidentally noticed events" so that a collaborative approach to investigation and mitigation can occur in a timely and efficient manner.

Employees and staff are the organization's most valuable asset in detecting fraud, and worst liability in spying. Especially in the R&D, health, pharmaceutical and data driven financial industry, staff and third parties should be given regular and updated training on fraud and internal-external collusion, recognizing anomalies, the Code of Conduct, a Fraud Control policy, conflict of interest, insider trading, whistle blower reporting and protecting data. On hiring all staff should affirm their understanding of the pressures and incentives, they may be faced with and the organization's zero tolerance for fraud. Vendors, consultants and thirds parties should also have background checks, provide their audited financials, anti - fraud training and complete a code of conduct policy.

Principle 5 Fraud Risk Management monitoring activities.

The organization must develop a continuous and periodic monitoring process of the fraud risk management policy to investigate misconduct and ineffective controls. The 5 principles of fraud management must be upheld; however, processes should be updated to reflect new measures that identify, update and develop new controls over people, technology and new risks that create other opportunities for

fraud. Internal audits and business process reengineering which focus on different procedures and departments, at various times may uncover and evaluate deficiencies at which time corrective action must be taken to strengthen controls and detect fraudulent activity. Otherwise, non-compliant activities may be missed if the company's controls failed to satisfy the framework.

5.3 Control Objectives for Information and Related Technologies (CobiT)

COBIT is described as a Business Framework for the Governance and Management of Enterprise IT. It is based on global thought leadership and a best practices framework for governing and managing the enterprise's information technology innovation and business success. It covers organizational structure, policies, procedures, skills and talent, information, and other enablers, and provides information for the board of directors down to incident management specialists working in operations.

Principle 1. Meeting Stakeholder Needs

Stakeholders are presumed to have 3 needs, Benefit realization, Risk optimization and Resource optimization which cascade to specific, actionable and customized goals. These drivers create the enterprise's goals, IT Goals and Enabler goals. Each of the goals begin with the enterprises' goals, directing the others which are IT-related goals, which in turn determine the enabler goals. The components are Financial, Customer, Internal, Learning and Growth and all have related IT Related Goals and Enterprise Goals such as Stakeholder Value, Customer service, Optimized process functionality and Skilled motived employees.

Principle 2. Covering the enterprise end to end.

Value creation around Benefit realization, Risk optimization and Resource optimization identify key governance drivers as Governance Enablers and Governance Scope. The interaction of delegation and accountability between Stakeholders, Governing bodies, Management and Operations influence the accomplishment of the goals through enablers.

Principle 3. Applying a single integrated framework

COBIT 5 creates value as an overarching governance and management framework that works in leveraging other standards such as COSO, COSO ERM, ISO 9000, ITIL, CMMI etc. to focus on achieving strategic goals through the efficient and innovative use of IT and for business decisioning.

Principle 4. Enabling a holistic approach.

The approach identifies the elements that perform the activities i) Principles, policies and frameworks that describe the required activities ii) Processes are the organized activities that reflect the objectives and result in outputs. iii) Organizational structures are the decision makers, iv) Culture, ethics and behavior are a key success factors in governance and management. v) Information is the ultimate product itself, which keeps the entity running and well governed vi) Services, infrastructure and applications are the IT processing and services, vii) People skills and competencies are required for completing activities, and correction of errors.

Principle 5 Separating governance from management.

Cobit 5 sees the role of governance as directing, evaluating and monitoring management's actions and results in planning, building, running, managing risk, and monitoring daily operations. The governance role supports the compliance of laws, regulations, reporting, contractual agreements and policies.

With a variety of risk management frameworks available, COBIT has the advantage of being able to integrate with the COSO fraud framework and other qualitative measures to manage risk. Financial institutions, governments and other collectors of personal data should use the foremost IT applications, platforms and infrastructures to carry out daily operations and deliver best in class customer service.

Banks proactively address intruders through surveillance of attempts to hack an administrator's account and download "mock" files deliberately left as decoys. The perimeter of the architecture is checked to see why the firewall failed to prevent unauthorized intruders. Remediation include military techniques to detect the location of the malware, tracking their movement, targeting, engaging and destroying them. Therefore state of the art risk management practices and cyber security experts must be appointed to safeguard against the ever-evolving threat landscape.

6. Conclusions

With the increased awareness of data compromises and cybercrime, many large data collecting entities still have vulnerabilities within their computer systems, gaps in their risk management process to address privacy and information security, reflecting the need for expertise and understanding, and specific privacy and security training for staff, contractors and third parties.

Customer credit card information is now safe from skimming as result of EMV Chip and PIN technology, but research shows that internal and external hacking are responsible for large personal data breaches. Customer payment details such as email addresses, and bank account information are valuable targets for cyber criminals whose intentions are theft, fraud and extortion.

Canada has the expertise and technology to proactively manage cyber threats, and with the changing roles of Chief Information Officers, Chartered Professional Accountants and Investigative Forensic Accountants should now advocate for cyber-security governance frameworks, investments in technology, and specific risk management frameworks.

Organizations have not always been able to detect when breaches are occurring or how many accounts have been breached until a significant amount of damage has been done, which creates a need for real-time awareness and threat intelligence. Large organizations are looking to externally managed security services to integrate and operate cybersecurity technologies and cloud architectures. Some of these technologies include running the IT function in the cloud, employing biometric verification, integrating big data analytics for fraud detection and security and investing in a security strategy for the internet of things.

Bank and financial institutions will become more reliant on technologies such as machine learning, artificial intelligence and Big Data Analytics to predict fraudulent card transactions, non-compliance with regulatory requirements, and cyber threats by providing the who, what, when, where and how to quickly report and address threat intelligence.

It has been observed from the credit card fraud rings investigated and caught in Toronto that cooperation and communication was required between the Toronto police, the RCMP, several provincial ministries and U.S. agencies. This points to the need for a federal review of the existing protocols protecting Canadians and a future plan for an offensive infrastructure to protect from cyber threats. Mobilization at the federal level is required to form a cybercrime coordination center to help police,

government, and private sector to collaborate in investigating personal data theft, identity fraud and cybercrimes.

Card issuers, merchants and banks should also promote safety over card data and KYC information, and this should be a requirement of Federal governance program for the financial industry. It seems that once a person is defrauded, they look to the CBA, the Competition Bureau, the Better Business Bureau and the Canadian Anti-Fraud Centre to guide them. Organizations and the markets they serve are often global, and action must be taken to protect data privacy.

The "Privacy By Design" framework over privacy is meant to enforce a proactive and preventative foundation for organizations to follow in building future privacy assurance methods. It must become the default mode of operation for good business practices and competitiveness. The European Union will implement a General Data Protection legislation in 2018, incorporating Privacy By Design which focuses on data privacy over goods and services purchased by EU citizens. Canadian organizations must also keep pace and create the regulatory compliance to prioritize privacy protection in training materials, review of data governance frameworks, and the life cycle of data.

7. Interviews
Interview 7.1

In order to protect the identity and confidentiality of the interviewer any names and companies have been blacked out.

Interview #1
Friday, June 16, 2017 10:19 AM
To : [redacted]
Objet : Card fraud questions - DIFA

Hi [redacted],
Thanks in advance for taking these question, on fraud and AML on credit cards for the DIFA research project. I can be reached by phone or in person if you would like to further discuss the topics of fraud or money laundering on credit cards.

1. Card Chip encryption has prevented Skimming of the cards' magstripe, what other types of fraud have criminals pivoted to in general? Can it be compromised?
Interviewed [redacted] :

1.1 criminals have majorly pivoted to cyberattacks to get hold of id or credit card information by attacking retail stores IT eco-system or mocking real website to gather clients private information and/or credit card info

1.2 the chip encryption is of military kind. It cannot be compromised. You can research rapidly on Wikipedia of what military encryption consist of.

2.What detective strategies exist for id theft used in "card not not present fraud"? Is big data used? Is "shimming" a threat to the card chip?
[redacted]:

2.1 very basic control : client will call because purchases are appearing on card statement.
2.2 big data can be very helpful to identify compromised or mock point of sales, whether a physical point of sales or virtual. The info of a mock or compromised point of sales can then be reported to the CBA (for the banking industry) and the RCMP for further investigation.
2.2 Shimming got more sophisticated but it is the same concept of intercepting the data between the card and the machine while the credit card holder enters his PIN and/or CCV number. So it doesn't defeat the encryption of the chip.

3. Amendments to Canada' PCMLTFA on identity verification request government issued photo id, credit file in existence for at least three years, or that a regulated entity has previously ascertained the person's identity. How far away are financial institutions from using voice and face biometrics as identification to reduce identity theft?
[redacted]**: Desjardins uses biometrics for identification, so the banking industry is already there.**

4. The 2017 CPA survey reported that 71% of participants believe that electronic payments made by credit cards or smartphone apps, actually make fraud easier.? Doesn't it also use Chip and tokenization technology?
[redacted] **: I think apps open new doors but they don't make it easier. At the end of the day if the user isn't careful, he/she will fall into a trap. The "tap" facility makes fraud easier and the "bumping" scam will hinder new fraud losses**

5. Electronic funds transferred to and from credit cards without the use of a clearing environment, makes the detection of money laundering more difficult, do you have any opinion on this?
[redacted] **: I am not aware of EFTs in a non-clearing environment … in what country do they operate EFTs in a P2P or B2B or B2P without a clearing environment? The only "setup" I can think of that would come near what you are describing is with Bitcoin. But not EFTs. Thank you for letting me know so I can learn about this.**

6. Are Canadian FIs lagging in detecting ML? Jonathan Cooperman, a Toronto-based forensic accountant, says moving money through Canada doesn't raise red flags the way money from other jurisdictions might. (David Donnelly/CBC) http://www.cbc.ca/news/business/russian-money-canada-1.4102132 Doesn't Big data analysis detect this?

[redacted] **: Canadian FIs are not lagging from my point of view since the ML infrastructure is mature in all FIs (the big 6 DSIB). I think the money launderers have a false sense of flying under the radar by coming to Canada but they still get flagged and reported. Big Data is mainly used by CANAFE to which FIs report data.**

7. Do you think that there should be an international organization that shares information on money laundering, card theft, and identity theft, and collaborates to detect it, prevent it and prosecute it?
[redacted] **: there is ! Interpol**

Many thanks for all your help and best regards.

Interview 7.2

From: [redacted]
Sent: May 23, 2017 9:08 AM
To: 'Ann-Marie Deboran'
Subject: RE: Credit card questions

Hi Anne-Marie – see below. I've answered to the best of my ability and reflect general personal opinions, and do not in any way represent [redacted] Unfortunately, several of your questions cannot be answered as it is too difficult to provide a response without referencing specific information that is proprietary to [redacted] or providing opinions on other FIs. I would suggest perhaps that you reach out to someone at the CBA who can provide more general responses and opinions without the risk of disclosing confidential information.

If you do plan to use any of the information provided, I would ask that you please do not reference [redacted] in your paper. My apologies – I know I probably wasn't as helpful as you would have liked, however, I hope you can understand my inability to provide opinions/info. Thanks.

Hi [redacted],

Thanks for returning my call.

Thanks in advance for taking my questions on fraud and AML on credit cards for the DIFA research project.

I can be reached by phone or in person if you do have time to discuss the appropriateness to the topic.

1. Card Chip encryption has prevented Skimming of the cards' magstripe, what other types of fraud have criminals pivoted to in general?

In general, as banks move more to the online space, they face increasing threats in online fraud/cyber crime.

2.What detective strategies exist for id theft used in "card not not present fraud"?

Cannot comment on detective strategies.

Is "shimming" a threat to the card chip?

My understanding of shimming is that while the card information is stolen, it cannot be used to create or duplicate "chip" card. Therefore, existing security measures associated with chip cards still cannot be compromised. Also, the "tap" function of

chip cards are not vulnerable to “shimming”, and therefore, the threat is not to the same extent as “skimming”.

3. Amendments to Canada' PCMLTFA on identity verification request government issued photo id, credit file in existence for at least three years, or that a regulated entity has previously ascertained the person’s identity. How far away are financial institutions from using voice and face biometrics as identification to reduce identity theft?

Cannot comment – however, in general, I believe all financial institutions are constantly evaluating new technologies to improve security for clients. Several banks have already introduced voice recognition as a security measure to protect clients.

4. The 2017 CPA survey reported that 71% of participants believe that electronic payments made by credit cards or smartphone apps, actually make fraud easier. Does the use of mobile wallets, Apple Pay and Google Pay actually reduce fraud, if so will the transaction limits be increased?

Cannot comment or provide statistics to show any fraud trend.

5. Electronic funds transferred to and from credit cards without the use of a clearing environment, makes the detection of money laundering more difficult, how is this being mediated?

Cannot comment.

6. Are Canadian FIs lagging in detecting ML? Jonathan Cooperman, a Toronto-based forensic accountant, says moving money through Canada doesn't raise red flags the way money from other jurisdictions might. (David Donnelly/CBC) http://www.cbc.ca/news/business/russian-money-canada-1.4102132

Cannot comment

7. Do you think that there should be an international organization that shares information on money laundering, card theft, and identity theft, and collaborates to detect it, prevent it and prosecute it?

Global collaboration between organizations can only help combat fraud/money laundering, as all banks face the same threats. International organizations already do exist where information on fraud/money laundering is shared and members communicate on a regular basis at conferences and events (e.g., IBSA, ACAMS).

Many thanks.

8. BIBLIOGRAPHY

Arango, C., Huynh, B. Fung and Stuber, G. (2012) The Changing Landscape for Retail Payments in Canada and the Implications for the Demand for Cash. Bank of Canada Review (autumn): 31–40 Retrieved [May 5, 2017]

Archer, N. (2012) Consumer identity theft prevention and identity fraud detection behaviors. Journal of Financial Crime; London19.1 (2012): 20-36.

Bitti, M. (2016) Passion and Purpose. CPA Magazine, Connecting and News. Sep.1 2016 Retrieved [June 1 2017] from [www.cpacanada.ca/en/connecting-and-news/cpa-magazine/articles/2016/september/passion-and-purpose].

Brett H. (2015) Case Study: The Home Depot Data breach. Jan 2015. Retrieved [May 15 2017] from; [www.sans.org/reading-room/whitepapers/breaches/case-study-home-depot-breach-36367]

Broverman, A. (Mar 2107) Canadian credit card, debit card and debt statistics. Retrieved [April 20, 2017] from; http://canada.creditcards.com/credit-card-news/canada-credit-card-debit-card-stats-international-1276/

Button, M. (2012) Cross-border fraud and the case for an "Interfraud". Policing: An International Journal of Police Strategies & Management35(2) January 2012, Volume35, Issue 2, page p.285-303.

Canadian Banking Association. (2016) Debit and Credit Card Fraud Statistics. Retrieved [April 1, 2017] from; [www.cba.ca/credit-card-debit-card-fraud-statistics]

Canadian Securities Administrators (2017) Disclosure of Cybersecurity Risks and incidents. Multilateral Staff notice 51-347, Jan 17, 2017. Retrieved [May 31 2017] from [www.osc.gov.on.ca/documents/en/Securities-Category5/20170119_51-347_disclosure-cyber-security.pdf]

Casey, L. (2017) Cross border investigation leads to arrests in alleged identity theft ring: police. Retrieved [May 10, 2017] from; [https://www.theglobeandmail.com/news/national/cross-border-investigation-leads-to-arrests-in-alleged-identity-theft-ring-police/article34936213/]

COBIT 5 ISACA. New framework for IT Governance, Risk, Security and Auditing. An Overview. Retrieved [June 7, 2017] from; www.qualified-audit-partners.be/user_files/QECB_GLC_COBIT_5_ISACA_s_new_framework_201303.pdf

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2016) Retrieved [June 7, 2017] Sept 29, from [www.coso.org/Documents/COSO - Fraud-Risk-Management-Guide-Executive-Summary.pdf]

Cotton, D., Johnigan, S., Givarz, L. (2016) Fraud risk Management Guide: Executive Summary. Committee of Sponsoring Organization of the Treadway Commission, COSO. Retrieved [June 7, 2017] from [www.coso.org/Documents/COSO -Fraud-Risk-Management-Guide-Executive-Summary.pdf]

Debenham, D. (2016) Big Data Analytics, Big Financial Institutions, and Big Money Fraud. Litigation Banking & Finance Law Review; Scarborough 32.1 (Nov 2016): Retrieved [May 30 2017] [http://search.proquest.com.myaccess.library.utoronto.ca/docview/1843836009?OpenUrlRefId=info:xri/sid:summon&accountid=14771]

Dingman, S. (2016) Watchdog slams Ashley Madison over privacy failures. The Globe and Mail, Aug 23. Retrieved (May 17, 2017) From [https://www.theglobeandmail.com/report-on-business/company-behind-ashley-madison-agrees-to-improve-security-after-massive-hack/article31508144/]

EMVCo. (2017) Worldwide EMV Deployment Statistics. Retrieved (May 17, 2017) From https://www.emvco.com/about_emvco.aspx?id=202

Fung, B., Huynh, K., and Stuber, G. (2015)The Use of Cash in Canada. Bank of Canada Review. Spring. Retrieved [May 2 2017] from; [www.bankofcanada.ca]

Greiner, L. (2017) Cyber Security Guard. CPA D&A Vol IV No 1.

Holtfreter, R. E., & Harrington, A. (2015). Data breach trends in the United States. *Journal of Financial Crime, 22*(2), 242-260. Retrieved from; http://myaccess.library.utoronto.ca/login?url=http://search.proquest.com.myaccess.library.utoronto.ca/docview/1676298759?accountid=14771

Khomami, N., Solon, O. (2017) Accidental hero halts ransomware attack and warns: this is not over. Retrieved [May 13, 2017] from; https://www.theguardian.com/technology/2017/may/13/accidental-hero-finds-kill-switch-to-stop-spread-of-ransomware-cyber-attack

Goutam, K., & Verma, D. (2015). Top five cyber frauds. *International Journal of Computer Applications, 119*(7) Retrieved [May 13, 2017] from; http://dx.doi.org.myaccess.library.utoronto.ca/10.5120/21080-3759

La Rose, L. (Feb 2016) More Canadians choosing credit cards, mobile payments over cash, study says. Retrieved [May 2 2017] from; [https://www.theglobeandmail.com/report-on-business/economy/more-

canadians-choosing-credit-cards-mobile-payments-over-cash-study-says/article28545469/]

Lorinc, J. (2017) Eyes Spy. CPA Magazine Mar. 2017

Mastercard Payment Gateway Services. Tokenization (2017) Retrieved May 4, 2015 from; [http://www.mastercard.com/gateway/payment processing /tokenization_solution.html]

McIntosh, E. (2017) Husband and wife among 14 arrested on fraud, money laundering charges. Retrieved (May 15, 2017) from; [https://www.thestar.com/news/gta/2017/02/17/husband-and-wife-among-14-arrested-on-fraud-money-laundering-charges.html]

Northcott, M. (2017) Victims of Crime. Research Digest. Issue No. 5, Feb 02, 2017 Retrieved [May 15 2017] from; [www.justice.gc.ca]

Office of the Privacy Commissioner of Canada (Feb 2017) Appearance before the Standing Committee on Access to Information, Privacy and Ethics (ETHI) on the Study of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) Retrieved [May 18 2017] from; [https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2017/parl_20170216/]

Posadzki, AAA. (July 2016) How Canadian banks are turning to biometrics to use your body to fight fraud. Retrieved [June 1 2017] from; [https://www.thestar.com/business/2016/07/22/banks-turn-to-biometrics-to-boost-security-convenience.html]

PWC (2017) The Global State of Information Security Survey 2017 Retrieved [April 1, 2017] from; [https://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html]

Sudjianto, A.,Yuan, M.,Kern, D., Nair, S.,Zhang, A. (2010) Statistical Methods for Fighting Financial Crimes. Technometrics; Alexandria 52.1 (Feb 2010): 5-19.

The Harris Poll 2017 (2017) CPA Canada Fraud Survey (March 2017) Retrieved [May 15, 2017] from; https://www.cpacanada.ca/en/connecting-and-news/news/media-centre/2017/march/cpa-canada-fraud-survey

Tompkins, M., Galociova, V. (2016) Canadian Payments methods and trends 2016. Payments Canada Discussion Paper N.7 November. Retrieved [May 5, 2017] from; [www.payments.ca/sites/default/files/cpmt_report_english_0.pdf]

Volz D., and Auchard E., (May 2017) More disruptions feared from cyber attack; Microsoft slams government secrecy. Retrieved [June 1 2017] from; http://www.reuters.com/article/us-britain-security-hospitals-idUSKBN18820S

Ward, L. (Feb 2017) Woman working as a fraud detection agent is one of 2 arrested in $8 M money laundering scheme. Retrieved [April 4 2017] from; www.cbc.ca/news/canada/toronto/woman-working-as-fraud-detection-agent-is-one-of-2-arrested-in-8m-money-laundering-scheme-1.3988351

Wrobel-Konior, S., (Nov 27, 2017) Payment Trends in 2017: Will Mobile Payments Be A Game-Changer? Retrieved [May 10, 2017] from; http://www.business2community.com/mobile-apps/payment-trends-2017-will-mobile-payments-game-changer-01713765#opzjkyY11OjDYt2g.99

Appendix A

CANADIAN BANKERS ASSOCIATION — Public

Credit Card Fraud and *Interac* Debit Card Fraud Statistics - Canadian Issued Cards

For the Years Ending December 2008, December 2014, December 2015

	2008	2014	2015		2008	2015		2008	2015	
Category: Credit Card - (American Express Canada, MasterCard Canada, Visa Canada)	Fraud Losses in $CAD	Fraud Losses in $CAD	Fraud Losses in $CAD	% chg [1]	No. of Accounts	No. of Accounts	% chg [1]	Average Loss per Account	Average Loss per Account	% chg [1]
Lost	$16,505,213	$10,796,687	$11,175,980	-32.29%	23,022	25,194	9.43%	$716.93	$443.60	-38.13%
Stolen	$32,293,078	$16,721,787	$20,611,211	-36.17%	47,546	37,014	-22.15%	$679.20	$556.85	-18.01%
Non Receipt	$13,239,049	$5,281,885	$6,029,168	-54.46%	4,352	4,592	5.51%	$3,042.06	$1,312.97	-56.84%
Fraudulent Applications	$11,013,923	$19,207,672	$18,698,208	69.77%	3,625	6,819	88.11%	$3,038.32	$2,742.07	-9.75%
Counterfeit Domestic	$162,239,525	$51,315,783	$37,713,677	-76.75%	130,765	64,299	-50.83%	$1,240.70	$586.54	-52.73%
Counterfeit Cross Border	$33,824,482	$73,843,710	$78,143,135	131.03%	27,738	87,879	216.82%	$1,219.43	$889.21	-27.08%
Card Not Present (Fraudulent e-commerce, telephone and mail purchases)	$128,362,477	$360,314,006	$537,243,970	318.54%	210,430	730,945	247.36%	$610.00	$735.00	20.49%
Account takeovers & Other	$9,662,029	$10,664,621	$16,866,829	74.57%	2,844	5,109	79.64%	$3,397.34	$3,301.40	-2.82%
Total: Credit Card	$407,729,739	$548,200,152	$726,482,179	78.18%	450,322	961,851	113.59%	$905.42	$755.30	-16.58%
Category: Debit Card - *(Interac* Association - Not including other Debit Card Fraud from other Payment Network Sources)	Fraud Losses in $CAD	Fraud Losses in $CAD	Fraud Losses in $CAD	% chg [1]	No. of Accounts	No. of Accounts	% chg [1]	Average Loss per Account	Average Loss per Account	% chg [1]
Total: Counterfeit	$104,500,000	$16,200,000	$11,800,000	-88.71%	148,000	24,795	-83.25%	$706.08	$475.90	-32.60%

Source: American Express Canada, MasterCard Canada, Visa Canada and Interac Association

(1) Percentage change from 2008, when chip and PIN technology was introduced to the Canadian market, to the current year

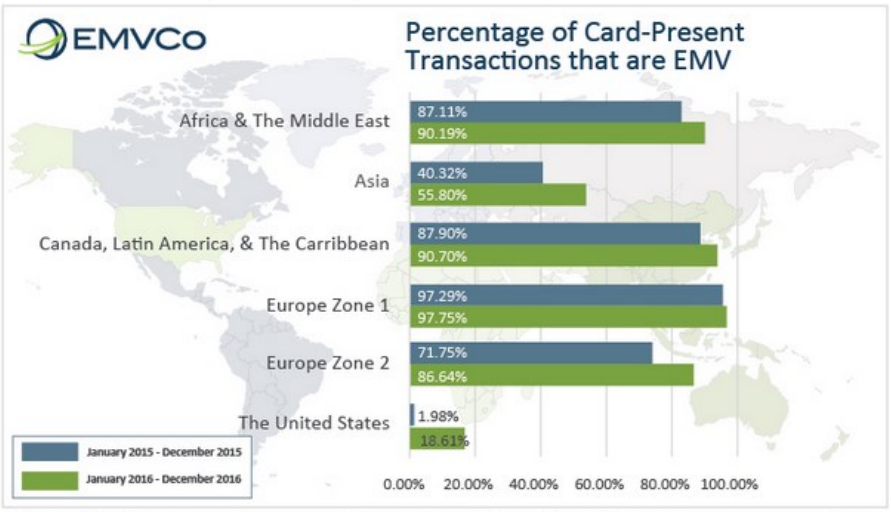
Canadian Banking Association. (2016)

Appendix B

Worldwide EMV Deployment Statistics

EMV Card-Present Transaction Percentage

The statistics below, most recently reported as of Q4 2016, show the percentage of card-present transactions that are EMV. The reported data represents the most accurate possible data that could be obtained by American Express, Discover, JCB, MasterCard, UnionPay, and Visa. It should be noted that, globally, 52.4% of transactions are EMV.



Figures represent the percentage of all card-present transactions processed by each member institution that are EMV transactions (Contact or Contactless). The reported data (blue bar) is from the twelve months of January 2015 through December 2015 and (green bar) the twelve months of January 2016 through December 2016; the data represents the most accurate possible data that could be obtained by American Express, Discover, JCB, MasterCard, UnionPay, and Visa during this period. To qualify as an "EMV transaction" for the purpose of this methodology, both the card and terminal used during a transaction must be EMV-enabled. Data is reported from the acquirer perspective. These figures do not include offline transactions, "on us" transactions (defined as a transaction handled exclusively by another processor), and/or transactions processed by non-EMVCo-member institutions, such as local schemes.

Download statistics and regional breakdown

Worldwide EMV Chip Card Deployment

The statistics below show worldwide EMV deployment figures as of Q4 2014, 2015, and 2016. The figures represent the latest statistics from American Express, Discover, JCB, MasterCard, UnionPay, and Visa, as reported by their member financial institutions globally. ***

Worldwide EMV Chip Card Deployment and Adoption*

	2014		2015		2016	
Region	EMV Cards	Adoption Rate	EMV Cards	Adoption Rate	EMV Cards	Adoption Rate
Canada, Latin America, and the Carribbean	544M	75.7%	680M	71.7%	717M	75.7%
Asia Pacific	1,676M	25.4%	2,459M	32.7%	3,331M	38.8%
Africa & the Middle East	116M	50.5%	160M	61.2%	184M	68.7%
Europe Zone 1	833M	83.5%	881M	84.3%	921M	84.9%
Europe Zone 2	153M	40.4%	200M	52.3%	243M	63.7%
United States	101M	7.3%	394M	26.4%	675M	52.2%

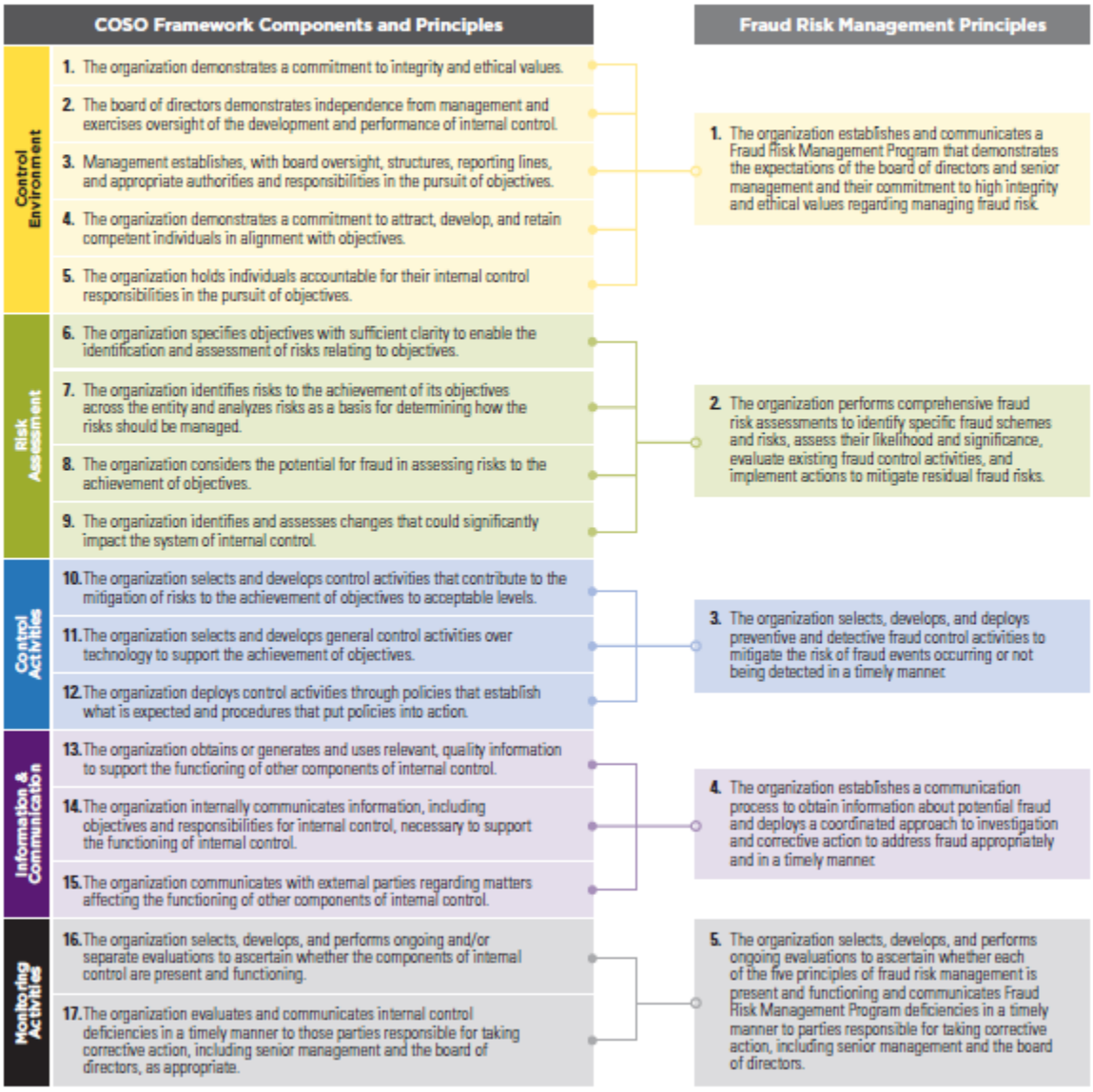
*Figures reported in Q4 of 2014, 2015, and 2016, respectively, and represent the latest statistics from American Express, Discover, JCB, MasterCard UnionPay, and Visa, as reported by their member institutions globally.

EMVCo. (2017)

Appendix C

Relationship Between the 2013 COSO Framework's Five Components and 17 Internal Control Principles and this Guide's Five Fraud Risk Management Principles

COSO revised its 1992 *Internal Control — Integrated Framework* in 2013 to incorporate 17 principles. These 17 principles are associated with the five internal control components COSO established in 1992. This guide's five fraud risk management principles fully support, are entirely consistent with, and parallel the 2013 COSO Framework's 17 internal control principles.[7] The correlation between the fraud risk management principles and the 2013 COSO Framework's internal control components and principles is as follows:



[7] The 2013 COSO Framework's 17 internal control principles have been adopted by the U.S. federal government in the *Standards for Internal Controls in the Federal Government*, issued by the Comptroller General of the United States. The Federal Managers' Financial Integrity Act of 1982 requires federal agencies to follow the Comptroller General's standards. In addition, the Government Accountability Office (GAO) has issued a *Framework for Managing Fraud Risks in Federal Programs*, which was developed based on leading practices as a tool for federal agencies to use in developing Fraud Risk Management Programs. [See gao.gov/assets/680/671664.pdf.]

COSO (2016)