ANALYSIS OF FRAUD PERPETRATED THROUGH AUTOMATED TELLER MACHINES: STRATEGIC SOLUTIONS THAT WILL ASSIST FINANCIAL INSTITUTIONS IN REDUCING LOSS

by

Lisa Frikker-Gruss

A Capstone Project Submitted to the Faculty of

Utica College

October 2012

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in
Economic Crime Management

ABSTRACT

The global payments industry is currently undergoing a technological shift in security protection. Unfortunately, the United States of America has been lagging behind the rest of the world in implementing standards to enhance protection, such as Chip and PIN authentication in payment cards and biometric validation systems at payment terminals. Payments industry leaders have forced a 2016 deadline for equipment operators to upgrade the technology to either comply with Chip and PIN capabilities or endure increased liability. This initiative is not without warrant, as organized criminal gangs from around the world have moved their operations into the United States. The older technology is thus making this country an easier and more susceptible target. This project focuses specifically on skimming fraud perpetrated at automated teller machines. The Chip and PIN technology used in countries abroad has enhanced user authentication, however, it too has deficiencies and limitations. The vulnerabilities of the random number generator that were identified through a study completed out of the University of Cambridge are reviewed. Additionally, the benefits of using biometrics are highlighted as an authentication tool to implement even after Chip and PIN technology is introduced in the United States.

This project demonstrates the strengths of predictive analysis as a detection tool by measuring a customer's demographic and behavioral metrics and discovering the commonalities that exist within legitimate and fraudulent transactions. The goal is to offer strategic solutions for financial institutions to customize into their organization. To achieve effective operational risk management, multiple layers of user authentication and transaction verification should be analyzed and implemented.

Keywords: Economic Crime Management, Ray Philo, vein, pattern, recognition, ATM, EMV.

ACKNOWLEDGMENTS

I want to thank the faculty of Utica College's Economic Crime Management program for affording me the opportunity to develop both academically and professionally through the insightful and rigorous coursework. I especially want to recognize Raymond Philo, Joseph Giordano, Christopher Riddell, Suzanne Lynch, and Dr. R. Bruce McBride for their guidance and assistance through the challenges. I appreciate John Stacy's leadership, as he provided me with the foundation to develop the concepts outlined within this project and the opportunity to create new insights. I am grateful for the encouragement that Lucy Sharp gave me, both through direct assistance and by living as an example for how I envision my career path. I am thankful to Bradley Gruss for his support in fulfilling his commitment to encourage my dreams and adventure into the unknowns that life will bring us. Lastly, Taylor Frikker has inspired my life-long journey of both learning and teaching. Her curiosity, determination, and enlightening sparkle that shines when she completes a challenge or makes a new discovery is encouraging.

TABLE OF CONTENTS

LIST OF ILLUSTRATIVE MATERIALS

Introduction

Automated Teller Machines, also known as ATMs, have been utilized in the financial industry domestically and internationally since the 1960s (ATMIA, 2010). ATMs serve as a convenient option for personal and business banking, where an individual can access his or her funds through a machine at various locations any hour of the day, any day of the week. Furthermore, the owner of the ATM does not have to be connected with the specific financial institution the customer banks with, leading towards increased spending. As ATMs continue to evolve, they are increasingly becoming the main touch point between the financial institution and the customer. The ATM Industry Association reported that a new ATM is installed every three and half minutes, with 2.1 million ATMs in existence worldwide. The size of the global ATM industry in U.S. currency is estimated between $14 and $15 billion dollars (ATMIA, 2010).

Banking transactions no longer need to occur inside a physical branch building between branch employees and customers. The typical cost of branch operations is budgeted at 75% of the total financial institution's expenses, making this line of business very costly. Based on the continued decrease in the amount of customer traffic, it is imperative that financial institutions identify more efficient service channels (CHOICE Savings & Investments, 2012). With the popularity of ATMs, a variety of other customer touch-points have evolved, such as online banking, mobile banking, and social media. Technological advances have enabled ATMs to adopt enhanced service capabilities similar to that of retail bank branch operations, thus leading financial institutions to consider them to become a primary channel of service delivery. Service enhanced ATMs offer reduced costs in real estate and human capital expenses. The "2012 ATM Software Trends and Analysis" identified that 70% of participants believed that the ATM was projected to become either a "more important" or "much more important" customer service

delivery channel within the upcoming years (ATM Marketplace, 2012). From a security perspective, it is essential to consider the increased level of risk that the ATM owner and financial institution will incur as services increase.

The payments industry within the United States of America is currently using magnetic stripe technology to communicate between the ATM terminal and a consumer's ATM card. This technology is the same that is used to communicate with a retailer's point of sale terminal and the consumer's credit or debit card. Conversely, most of the industrialized nations have migrated to using Chip (micro-chip) and PIN (personal identification number) technology, also known as EMV. Magnetic stripe technology is antiquated and holds various vulnerabilities for criminals to take advantage of, while Chip and PIN technology offers unique user authentication features that are more difficult for a criminal to replicate. Therefore, the organized criminal enterprises that perpetrate crimes in ATM fraud, particularly card skimming, have been migrating their operations to the United States (ATM Marketplace, 2012). The use of the PIN that is created by the consumer once offered an additional authentication security layer for the user. However, ATM skimming crimes have incorporated numerous methods to compromise the consumer's PIN and replicate the transaction as if it belonged to the true customer.

To successfully commit ATM fraud, a criminal must compromise multiple layers of security, thus making this crime more difficult to complete than traditional credit card fraud. This project refers to "ATM fraud" as the theft of funds from a victim's bank account, using the ATM as a vehicle to perpetrate the crimes. However, before this can occur, the perpetrator must obtain the data that corresponds to the ATM card number and PIN. It is important to take into account that when ATM fraud statistics are reported by a financial institution or industry association, the incidents of the theft of cash only are typically the only statistic that is reported.

Because the theft of the data and the compromise of the ATM itself are oftentimes unknown, the criminal acts are consequently under-reported. It can be estimated that more ATM card data is stolen but is never used to steal funds from an account. Because the second step of the crime is never completed, the level of theft becomes under-reported. The Global ATM Security Alliance, a special task force of the ATM Industry Association that assists with international organized crime investigations, reported that only 0.0016% of all worldwide ATM transactions are fraudulent (ATM Marketplace, 2012). Even though the percentage of all fraudulent transactions appears low, ATM fraud losses have significant impact on financial institutions because unlike credit or debit card fraud, there are no provisions for transaction disputes with a merchant. Aite Group, a research firm, reported that the average loss at one ATM as a result of skimming crimes is $50,000 (ATM Marketplace, 2012).

The shift in types of risk threats to ATMs is changing due to newer technology that was introduced globally, known as EMV. EMV is also referred to as the Chip and PIN technology that further authenticates that information captured on the microchip of the card belongs to the cardholder. Historically, the United States experienced relatively low levels of payment card fraud. Therefore, the United States government had not originally instituted mandatory conversion guidelines. However within recent years, international conversion to EMV has been occurring more aggressively. In 2011, 98% of financial institutions in European nations were in compliance, along with 75% in Russia and 65% in Canada (ATM Marketplace, 2012). In September 2012, MasterCard issued a deadline to ensure EMV compliance on all ATMs by October 2016. ATM owners who do not convert the machines by the deadline will incur liability costs if the machine is compromised (American Banker, 2012).

Proposed Strategic Solutions

The purpose of this project is to offer strategic fraud- risk based solutions for financial institutions to incorporate as an effort to reduce losses to due ATM fraud. The risk-based solutions offered include methods of both detection and deterrence of criminal behavior. The strategies are ubiquitous and can be incorporated into any financial institution's risk management plan. The research identifies and outlines the business risks inherent with ATM usage. The research identifies risks for financial institutions that both own their own machines and those who do not, as consumers are welcome to use any ATM within the world. The project will identify both physical risks to the ATM terminal as well as intellectual risks to the cardholder's data. The research will highlight the negative impact of when both factors are compromised; financial losses are incurred by the consumer and ultimately the financial institution.

The project will offer unique and specific behavior detection solutions for ATM skimming fraud through data mining and predictive analytics. Predictive behavioral analytics serves as a proactive measure at the transaction level to determine the probability of the individual withdrawing the cash being the true consumer or a criminal. The technology uses metrics based off of the consumer's past behavior to predict typical spending patterns. For example, consumers will typically use the same ATMs, especially those that are located close to home, work, or frequently used shopping centers. They also typically withdraw similar amounts of cash on a schedule that may or may not be routine. Data mining is used to identify these patterns and predictive analytics incorporates mathematical algorithms to review the transactions to determine if they fit within the normal spending patterns. This project will offer examples of trend focused strategies developed from the data. This project will demonstrate that by harvesting this level of intelligence, the financial institution's management team can then best

determine how to settle the transaction with either the customer or criminal, without disturbing the true customer behavior. Compromised cards can be identified faster, ultimately reducing the amount of fraudulent losses.

This research also explores biometric solutions to ATM fraud. Finger and palm vein authentication that Japan is using is reviewed as a hardware countermeasure. The technologies are described, along with explanations of why vein authentication is preferred over fingerprint analysis, iris scan or voice and facial recognition. The technology is not available in the United States, but this research will demonstrate its high level of fraud deterrence in an effort to educate others on the possibilities that this technology can provide.

The research shows the overwhelming consensus that card skimming is ranked globally as the highest threat level to perpetrate ATM fraud. The research also considers that the next threat level of ATM fraud will be handled effectively after skimming is controlled and minimized. Brute force attacks and cyber threats have the next highest threat levels. Operational risk managers need to be cognizant of these threats when developing a strategic risk management plan over several years. Therefore, it is crucial to consider several different components when implementing a strategy to ensure it is versatile to combat various types of fraud. The risk strategy must be stronger than the criminal's next target.

This project does not discuss the impact of fraud from illegal debit card usage at retail point of sale terminals or Internet purchases. This research recognizes that financial institutions and industry associations, domestically and globally, often do not differentiate between the types of loss they are experiencing, as ATM and debit cards are often managed one in the same. In addition to offering specific solutions, this project offers specific recommendations for data

retention and mining practices that would maximize the opportunity to visualize and predict specific crime trends.

Literature Review

ATM industry associations, along with experts within the technology- based and financial institution fields agree that ATM security should be an investment that is strategically implemented. In "The Many Socio-Economic Benefits of ATMs", the ATM Industry Association, a global non-profit trade organization known as ATMIA, highlighted the ATM as a significant invention that enhanced various social and economic benefits within the economy, governments across the world, retailers, consumers, and financial institutions. The ATMIA concludes that the convenience of twenty-four hour, seven day a week service is paramount for society, as extended service hours enhance the profitability of financial institutions and retailers alike. Domestic and global economic stimulation is enhanced through a common network to access cash directly from a consumer's account from any location, thus leading to a habitual spending pattern (ATMIA, 2010).

The ATM Marketplace, in collaboration with KAL ATM Software, conducted the "2012 ATM Software Trends and Analysis" study. The ATM Marketplace reviewed that financial institutions are using multiple channels to reach their customers, such as online banking, mobile banking, ATM, call center and branch level service. The ATM Marketplace has been surveying experts within the global ATM and financial institution industries annually since 2007. The number of respondents has increased significantly, starting at 207 in 2007 and expanding to 797 in 2012. The purpose of the survey was to gauge the needs for ATM software, both with current and future plans for functionality as customers increase the desire for the ATM to become the primary touch point. The findings of the survey coincide with the ATMIA's position of enhancing the focus to be placed on the ATM as a primary customer touch-point. While branches are not the only service delivery method available anymore, 56% of the survey

respondents answered that the branch continues to be the primary service channel, with 40% of respondents who believe the ATM to be the second most important service delivery channel. This finding is an interesting shift in the respondent's answers from 2011 to 2012. In 2011, only 37% of respondents identified the branch as the most important service channel, while 34% of the respondents stated that the ATM was the most important service channel. The respondents indicated that the need for the call center, Internet, and mobile applications remained stable (ATM Marketplace, 2012). No explanation was offered for the shift in differing positions. This trend will be interesting to monitor in upcoming surveys, especially since the former response offers more cost savings options.

Because several financial institutions see the economic value of the ATM as opposed to a retail branch, ATMs are being outfitted to provide all of the services, such as opening new accounts, applying for loans and credit cards, replacing ATM cards, paying bills, and transferring money internationally. Additionally, the ATMs can be equipped to provide video connections to communicate in real-time with customer service representatives (ATM Marketplace, 2012). Financial institutions need to keep pace with the competition, while also maintaining a steady customer traffic flow. If customers become agitated because the additional services create longer wait times, the customers will be more apt to solicit services from another ATM or possibly another financial institution.

The "2012 ATM Software Trends and Analysis" also focused on the capability of the ATM to enhance and personalize the customer's experience. The concept was introduced in the 2007-2008 survey by Peter Kulik, the Technologies Channel Manager for Vantiv. Since financial institutions already house numerous data gathering methods to understand customer spend patterns, by enhancing the technology the financial institution can customize the

customer's options to fit within his or her own specifications. Michael Engel, Head of Software Sales Banking for Wincor Nixdorf, a German based ATM manufacturer, compared the ATM experience to that which is generated on the social media platform, Facebook. Engel stated,

> "If you log onto Facebook, you only see those messages that pertain to you. It should be the same if I use my card at an ATM. For example, here in Germany I always withdraw 200 euros. Why should I have to go through those options over and over again? My bank should recognize me by now and present me with one button" (ATM Marketplace, 2012).

This paper will investigate how Michael Engel's and Peter Kulik's concepts can be considered and developed to further enhance fraud prevention strategies, such as predictive analytics, to determine if a customer's transaction is authentic or if it indicates the possibility of fraud behavior.

The ATM Marketplace, in conjunction with Diebold, a security service industry leader, published "ATM Security" to educate financial institutions and ATM owners about the current threats and how to mitigate the losses. The whitepaper highlighted how the Chip and PIN implementation has shifted the geography of ATM skimming crimes by observing the trends within the converted countries. While crime statistics show ATM fraud losses have decreased within nations who have implemented the conversion, smaller and physically dangerous ATM crimes are developing (ATM Marketplace, 2012).

Additionally, magnetic stripe technology is still present on cards that also have Chip and PIN. So criminals still have the ability to steal the card data and are migrating into the United States to steal the funds. According to Europol, approximately one billion dollars, or 80%, of the ATM card skimming fraud committed outside the European Union using EU payment cards is

committed in the United States (ATM Marketplace, 2012). While the losses cited above are in reference to international financial institutions, the United States has opened the doors to criminal operations that were occurring internationally until the EMV conversion occurred, leaving our citizens and financial institutions at risk.

Benefits and Risks of Chip and PIN Technology

EMV, the term derived from Europay, MasterCard, and Visa, is the global standard for credit, debit, and ATM cards based on embedded chip card technology that was developed in the mid- 1990s. Countries in Europe, Canada, Latin America, and Asia have all migrated to using EMV chip authorization (Smart Card Alliance, 2011). EMV technology is critical in defeating counterfeit ATM card fraud by offering protection for breaches against vestibule door access, external skimmers on the card entry slot, and internal skimmers found on the card reader (Diebold, 2011). However, it is imperative for financial institutions to understand that EMV technology is stronger than magnetic stripe technology, but it cannot protect against all types of card fraud; thus, leading the criminal groups to migrate to areas of opportunity, mainly in cyber-attacks. The areas that EMV cannot protect are: communications from the card reader to the processor, malware, communications between TCP/ IP Host, and the backend infrastructure (Diebold, 2011).

EMV uses a smartcard that incorporates a secure integrated computer chip embedded within the card to store data (Smart Card Alliance, 2011). The computer chip replaces the magnetic stripe. The chip has not yet been cloned by criminals. The chip uses two factor authentication with PIN verification. The technology can support both contact and contactless cards. The security of the transaction is enhanced with three specific additions: card authentication that protects against counterfeit cards, cardholder verification that authenticates

the cardholder and protects against lost and stolen cards, and transaction authorization in which the card issuer collaborates in authorizing transactions (Smart Card Alliance, 2011).

EMV incorporates various levels of authentication and validation dependent upon the type of transaction being authorized. ATM transactions are only approved to use online card authentication, online transaction authorization and online PIN cardholder verification. Online authentication uses a cryptogram to share the secret key. Each transaction generates a new cryptogram; therefore, the cryptogram is unique for each transaction. Since online PIN verification is mandatory for ATMs, terminals will need to be upgraded to support the changes for the various types of cards, in addition to an encrypting PIN pad. Any terminal upgrades must be tested and certified from EMVCo to ensure compliance standards are met (Smart Card Alliance, 2011).

Five researchers based out of the University of Cambridge, in the United Kingdom, conducted a study released in September 2012 based on suspicions of the legitimacy in the Chip and PIN program's safeguards. The study, detailed in "Chip and Skim: Cloning EMV cards with the Pre-Play Attack", looked into the possibility of system programming vulnerabilities. The research began as a result of complaints from a bank customer who was refused refunds from his financial institution for ATM transactions that he claimed he did not transact. The researchers then investigated many claims since the integration of EMV where customers made claims of fraudulent ATM transactions. In many instances when customers requested transaction logs, financial institutions either deleted or refused to provide evidence of the transactions (Bond, et al, 2012).

For the transaction logs that were provided, researchers observed specific mathematical patterns with the "UN", or unpredictable number. The unpredictable number is used during the

transaction authentication phase, where a supposed randomly generated number is assigned to a transaction. The researchers identified through testing transactions that based on the initial programmer, some systems used either counters, time stamps, or amateur written algorithms to generate the random number. The researchers concluded that the random number was predictable and followed a particular sequence. This vulnerability leads to pre-play attacks, which can be carried out by organized criminal organizations. The card does not have to be cloned in order for the criminal to predict the transaction. The research found up to fifty unpredictable numbers for each ATM that was tested (Bond, et al, 2012).

The researchers identified some limitations for a criminal to successfully carry out a pre-play attack, such as the perpetrator must chose the victim country, specific date and amounts all in advance. The authors concluded that if EMV included the terminal ID with the authentication of the transaction, this type of attack would not be possible. The challenge lies in where the liability falls for this error. While the cost of fraud is the responsibility of the issuing financial institution and the customer, the cost to fix the issue is the responsibility of the acquiring bank and ATM vendor (Bond, et al, 2012).

Vein Pattern Recognition

Biometrics is a concept that utilizes features from a person's body to authenticate his or her identity. This security measure is not utilized in financial institutions in the United States, however financial institutions in Japan have been using both finger and palm vein pattern identity verification since 2005 (Hitachi, 2006). Hitachi and Fujitsu are the industry leaders in developing and adapting the technology to be useful for financial security. Hitachi developed its original concepts between 1997 and 2000. Between 2002 and 2003, the concepts were enhanced and placed into production, with the first product of light transmission authentication used for

physical access control in 2002. In 2004, Hitachi further enhanced the scope of the technology to include ATMs, with the product becoming available for commercial use in 2005 (Hitachi, 2006). The timing of the product release was in response to the Japanese government's demand on financial institutions to respond to the organized ATM theft crime rings and to compensate victims for losses. Currently, there are 80,000 ATMs in Japan that use biometric verification systems from Hitachi and Fujitsu, along with leading financial institutions in Brazil, Poland, and Turkey who have recently adopted the technology also (Strickland, 2012).

Hitachi's and Fujitsu's products are developed from the concept that the patterns of a person's veins are unique within each finger and for each person. Both companies study the blood flow patterns and ability of light to adapt to the hemoglobin within the veins through light transmission and reflection techniques. Hitachi's light transmission technology illuminates a person's vein pattern as the lights passes through the surface of the skin. The light is transmitted from a LED, also known as a light emitting diode, source. The LED source is transmitted through the finger and is absorbed by the hemoglobin in the blood. When the light rays are absorbed, the veins appear dark and can be replicated into an image through the use of a camera. Figure 1, found on page 14, shows an image produced by Fujitsu of the veins in the palm once it is illuminated. A camera processes the pattern into an image that is digitized and stored as a template. The template image is used in conjunction with pattern recognition, which uses mathematical algorithms to match against a sample image and authenticate its ownership (Hitachi, 2006).

Fujitsu's light reflection method differs from the light transmission in that the intensity of the reflection in the pattern requires a larger area. To a manufacturer's standpoint, this technique is easier to design. This method offers high accuracy rates, however, the device may be too large

and not user friendly (Edgington, 2007). Hitachi combined the light transmission and light reflection methods into a side illumination technique, which scatters the light throughout the finger. The image is captured on the opposite side of the finger, thus leading to a more applicable product design.

Hitachi developed a finger vein recognition system, while Fujitsu produced a palm vein recognition device, as seen below (Strickland, 2012). Fujitsu's palm reader is the image in the top right corner, while Hitachi's finger vein device is the image in the bottom right hand corner.

Figure 1: Fujitsu image of veins through a palm image (Left), Fujitsu palm vein reader (Top Right), Hitachi finer vein reader (Bottom Right) (Strickland, 2012).

The Japanese financial institutions, along with Hitachi and Fujitsu, have developed a system that stores the pattern recognition image on a microchip on a person's ATM smartcard, rather than in a database. Therefore, the data on the card itself is matched against the image being presented with the card. The smartcard is still authenticated with the PIN, in addition to the image of the vein. The smartcards are designed to not accept incoming data from the ATM; therefore, hacking into and retrieving the image through theft of the card is not possible (Strickland, 2012).

Vein recognition is not the only biometric method on the market, however, the benefits of using finger and palm vein recognition are vast and the attributes outweigh all other authentication devices available. The other biometric methods currently in use are iris scanning, fingerprint analysis, voice and facial recognition. Finger vein patterns are a reliable source of data, as they are unique to each finger and person. This is true even amongst identical twins. The patterns remain stable and constant throughout a person's adult life. With the proper camera image processing, the patterns are easily recognizable. Vein recognition is highly secure and resistant to tampering, as the veins cannot be fabricated or forged outside one's body. From an industry standpoint, it is necessary to know that the accuracy rate is based on the performance of the image sensor. If the image sensor is working properly, the false rejection rate is less than 0.01% and false acceptance rate is less than 0.0001%. The method in which the authentication occurs is desirable to the user, as the infrared light is noninvasive (Hitachi, 2006). The speed of the authentication process is desirable, with Fujitsu having the ability to correctly identify patterns within 1.34 seconds after reviewing five million templates. Fujitsu is currently working on enhancing their system to account for the system's growth and accommodate for 10 million customer samples. Fujitsu uses a data merge method for identifying palm and fingerprint samples with three identifiers. The system disregards any data that is dissimilar to the three matches provided (Strickland, 2012).

Practicality and security are often two adverse subjects, as one can often compromise the other. Vein pattern recognition offers both benefits in being feasible to incorporate into a security design, while offering optimal security protection. When compared against fingerprint analysis, iris scans, facial and voice recognition, vein patterns rank the highest when considering security, accuracy, speed, sample enrollment rates, resistance, cost, and size. While voice and

facial recognition may be more convenient for a customer to use than vein pattern recognition, their accuracy is not as high as the vein comparison rate is. One complication was identified with the palm vein reader, as the system uses the reflected light technique. Therefore, the image may not as distinct as the light transmission method. The condition or roughness of the skin may contaminate the quality of the image produced (Edgington, 2007).

Japan has been using biometric technology for approximately seven years and is finding new ways to adopt the products into financial institution security, such as either discontinuing the use of the PIN code or use of the ATM card. As of September 2012, Ogaki Kyoritsu Bank has incorporated Fujitsu's palm vein biometric authentication with a customer's birth date and PIN to access their accounts. The risk lies in that there is no ATM card, so the customer sample templates are stored in a central database. This financial institution recognizes this practice as a benefit in response to the earthquakes, tsunami, and nuclear accident that occurred in 2011. Customers fled their homes and did not have the identification that was needed to access funds from their banks accounts. As a result, honest customers could not access their funds and dishonest people were able to use clever con methods to steal funds (Strickland, 2012).

MasterCard further estimated that using biometric authentication at a retailer's point of sale terminal with a credit card payment would decrease fraud by 80%. MasterCard approved of the combination of smartcard storage of biometric data, as it encouraged privacy and security. In "Biometric Authentication in Relation to Payment Systems and ATMs", Gerik Alexander von Graevenitz discussed disadvantages and differences with prior research of using smartcard based biometrics. Von Graevenitz identified challenges including the size of the image as it cannot be miniaturized like it can be in fingerprint recognition. He provided research that indicated a person's finger vein patterns can change during a person's lifetime. Additionally, he concluded

that the brightness of the image is reliant upon the thickness of a person's finger. Von Graevenitz challenged biometrics as a sole method of authentication and stated,

> "The optical application of biometric authentication in the financial industry still requires at least one more authentication method that combines with knowledge and/ or possession features or that demands two biometric features" (Von Graevenitz, 2007).

ATM Crime Typology

The United States Secret Service is the government's law enforcement agency responsible for investigating all ATM fraud crimes. Title 18 of the United States Code, Section 1029, applies to crimes involving access devices. Access devices include debit cards, automated teller machine cards, and personal identification numbers, all of which are required to perpetrate ATM fraud. Title 18 of the United States Code, Section 1028, refers to identity crimes, such as the misuse of personal or financial identifiers to gain something of value. Identity crimes consist of access device fraud, also known as skimming, bank fraud, false identification fraud, and identity theft (www.secretservice.gov, 2012).

Definitions of Terms

As defined by the European ATM Security Team, Smart Card Alliance and the ATM Marketplace.

ATM- Automated Teller Machine that disperses cash and conducts banking transactions.

ATMIA- ATM Industry Association, a global non-profit trade organization.

Card Authentication Method- Used in Chip and PIN technology to determine that the payment card being used is not counterfeit.

Card Skimming- The card details and PIN are captured at the ATM and used to produce counterfeit cards for subsequent fraudulent cash withdrawals. The customer sees a normal transaction and retains the card. Multiple cards are compromised in one attack at one ATM.

Card Trapping- The card is physically captured at the ATM, and the PIN is compromised. Later the card is used to make fraudulent cash withdrawals. One card is compromised in each attack.

Card Verification Code/ Card Verification Value Number (CVC / CVV)- Terms used by MasterCard and Visa for the security codes used for credit and debit transactions to protect against card fraud.

Cardholder Verification Method (CVM)- Used in Chip and PIN technology to authenticate that the person presenting the card is the valid cardholder. There are four types: offline PIN, online PIN, signature verification, and no CVM. Online PIN is the only CVM available for ATM transactions.

Chip Card- Card that includes an embedded secure integrated circuit. The card can connect with a reader through either direct contact or using radio frequency interface (contactless). Cards have the ability to store large amounts of data and interact intelligently with a reader through authentication and encryption.

EAST (European ATM Security Team)- Non-profit industry association that works with ATM deployers and networks in multiple European countries and territories to disseminate security issues.

EMV (Europay, MasterCard, Visa)- Global standard for credit, debit, and ATM cards based on embedded chip card technology developed by Europay, MasterCard and Visa.

Jittering- Process that controls and varies the speed of movement of a card as it is swiped through a card reader, making it difficult, if not impossible, to read card data.

Magnetic Stripe Card- Plastic card that uses a band of magnetic material to store data.

Online PIN- In an EMV transaction, the process of comparing the cardholder's entered PIN with the PIN stored on the issuer host system. The PIN is encrypted by the POS terminal PIN pad before being passed to the issuer host system.

PIN- Personal identification number used by the cardholder to authenticate identity.

Risks to the ATM Terminal

In the second quarter of 2012, the ATM Industry Association, ATMIA, conducted a survey of ninety-four participants to determine the top two current threats to the ATM. The participants responded online from various countries around the world. The chart below highlights the results of the 152 responses for two questions asking the top threats currently with ATMs.

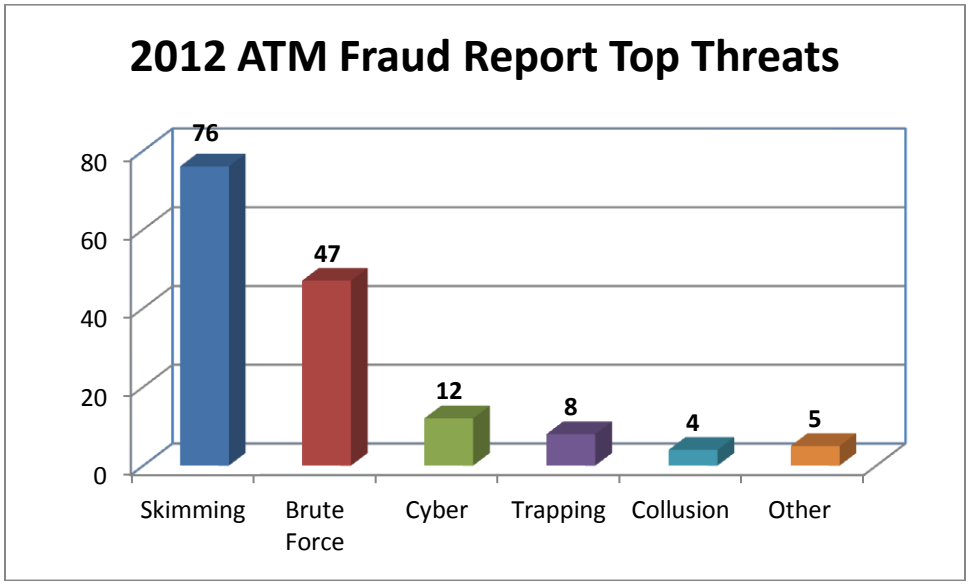

Figure 2: Participant Responses to Top ATM Threats as per the 2012 ATM Fraud Report completed by the ATM Industry Association (ATMIA, 2012).
Note: Brute force attacks consisted of ram raids, burglary, gas/ explosive attacks, vandalism, and cash in transit robbery. Other threats consist of money laundering, terminal master key fraud, denomination fraud and bogus bank official scam.

The results heavily indicated that most financial institutions believe skimming is currently the greatest threat. Skimming occurs when a small electronic device is installed on or in an ATM terminal to read the magnetic stripe coding of the card, thus providing the criminal with the sixteen digit card number. The card data is contained on multiple tracks and depending on the sophistication of the device, the card verification value numbers, known as CVV, can also be stolen. Skimming devices are designed to appear exactly as the ATM would look. Figure 3,

below, shows an example of a full ATM front panel that fits on top of the actual terminal. The card slot contains a feature that reads and stores the magnetic stripe coding.

Figure 3: An ATM skimmer panel that fits directly on top of the real ATM (Krebs, 2010).

ATM skimming is more complex than that which occurs at a merchant point of sale terminal. ATM transactions require dual authentication, which includes the sixteen digit card number and the customer's personal identification number (PIN), typically consisting of four digits. Therefore, the criminal must compromise the customer's individual PIN to successfully commission the theft of cash. The challenge for the criminal is to match the card data to the customer's PIN. PINs are stolen often using a hidden camera to record the numbers or with a fictitious keypad that is placed over the real one, recording and stealing the keystrokes. Additionally, Bluetooth technology can be incorporated into the operation, where criminals remotely steal the data with no need no return to the ATM to retrieve the recording or pin capture devices (ATM Marketplace, 2012). The data gathered is used to clone a separate card and steal the cash from an ATM.

Criminals are identifying clever ways to gain access to the customer's PIN. Figure 4, below, portrays an authentic PIN capture device. The device was placed over the actual PIN pad and used to record the individual key strokes that the customer inputted as his or her PIN.

Figure 4: ATM PIN capture overlay device pulled back to reveal the legitimate PIN entry pad (Krebs, 2010).

Organized skimming attacks are reported to have the largest rate of financial loss. Skimming crimes are typically perpetrated by organized criminal gangs, rather than sole operations. The gangs use proceeds from their theft to fund further research and development of technology designed to overcome the industry's defenses (ATM Marketplace, 2012). For countries who have converted to using EMV technology, EAST reported an increase in perpetrators visually stealing the PIN through shoulder surfing. This action was then followed by direct theft of the ATM card, typically through distracting and targeting elderly people. It has been identified that EMV technology will reduce fraud losses by dollar value; however, the constant number of thefts will still occur, becoming more personal in nature. The schemes are moving towards card trapping, where the card is physically captured at the ATM and the PIN is compromised typically by a by-stander. Only one card can be compromised in each attack, thus decreasing the speed of each attack.

The criminals are rapidly adjusting to the technological advances to incorporate into the schemes. EAST reported an increase of using skimming devices attached to MP3 and MP4 players, on ATMs that have been outfitted with anti-skimming devices (ATM Marketplace, 2012). Figure 5, below, shows an audio device that was confiscated from a Diebold manufactured ATM. The audio device is used to steal the PIN code by listening to and deciphering the keystrokes.

Figure 5: Audio skimmer for Diebold ATMs identified by five European nations (Krebs, 2010).

Anti-Skimming Hardware Solutions

ATM owners can outfit the terminals with various mechanical solutions to defeat criminal efforts. One solution is known as jittering. This is a "process that controls and varies the speed of movement of a card as it is swiped through a card reader, making it difficult, if not impossible, to read card data" (ATM Marketplace, 2012). Jittering is an internal mechanism that is becoming outdated, due to the varying types of ATM terminals. Consequently, jittering is not able to be implemented into dip or swipe style card readers (ATM Marketplace, 2012).

Similarly, a plastic insert or object detection device can identify if a skimming device is added either inside or on top of the machine. Once detected, the insert will alert the machine to disable its service. The ATM owner can incorporate video surveillance to monitor the activity once the alert is activated. The alerting software and video surveillance can be enhanced to remotely monitor the activities, taking into consideration distances and hours of availability (ATM Marketplace, 2012).

Compromising the card number completes only half of the skimming attempt. It is critical for ATM owners to consider security measures to protect the PIN pad. The foreign object detection can accomplish this through the alert and deactivation system. Additionally, ATM owners can install PIN shields to guard the customer's keystrokes from being observed either directly by criminals or through installed cameras (ATM Marketplace, 2012). An easy solution is for ATM owners to post signage reminding customers to cover their hands as they enter their PIN.

This section described some hardware solutions that ATM owners can purchase to protect their equipment and the integrity of the terminal. It is crucial to remember that while the compromised ATM is the first breakdown in controls, it is very often not where the financial losses are impacted. The financial losses are incurred by the financial institution that issued the ATM card that was compromised. Therefore, privately owned ATM terminals may not be as willing to invest in this type of technology, as they are not being held liable for the losses. As cited earlier, MasterCard's 2016 EMV compliance mandate will strengthen the liability concerns in favor of the issuing financial institution, as all ATMs will be required to adapt to the technology.

Methodology

Creation of a Strategic Fraud Data Management Program

The onus and liability of financial losses due to fraud sits with the financial institution that issued the ATM card and holds the customer's accounts. Therefore, it is the issuing financial institution's responsibility to implement detection and prevention measures to reduce and mitigate fraud losses. Comprehensive risk management consists of a multi-strategy approach, as no one method is particularly robust enough to defeat all forms of ATM fraud. This project suggests options for detection and prevention strategies.

Predictive analytics is a tool to engage consumer behavior through mathematical expressions. This is best achieved by using examples of past behavior to predict present and future behavior. Oracle defined the purpose of predictive models as, "finding the causality, relationships, and patterns between explanatory variables and dependent variables, focusing on specific variables" (Oracle, 2010). This concept can be applied to studying and predicting patterns of fraud through understanding the predictors of habitual consumer behavior.

Understanding the standard behavior predictors can be useful in eliminating the vast majority of transactions, mostly legitimate transactions. It is possible that fraudulent transactions may appear to be standard behavior. Through the elimination process, the predictors can then focus in on the transactions that are outliers to the typical behavior. This practice serves a dual purpose: investigative resources can be allocated to research the outliers developed through the analytics, while those transactions that are deemed fraudulent and fit within the typical parameters can be investigated individually. The caveat is that there will be some transactions that will fit within both the parameters that decide legitimate transactions and the assumptions of fraudulent behavior that will create a false positive. It is essential to create a program that will

limit the exposure of fraud losses, while at the same time not causing an inconvenience to the customer. It is understood that not all fraudulent transactions will be identified using predictive analytics, as new trends and behaviors constantly develop. Therefore, the financial institution's investigative team will still need to continue responding to customer inquiries of fraud in a reactionary mode. However, the design of this plan is to minimize reactionary loss and maximize prevention efforts.

The predictors of behavior can be indicated through examining variables such as days of week, times of day, calendar dates, ATM terminal identification numbers, zip codes, and amounts of withdrawals. All of these predictors hold value in the typical consumer's life, as their behavior generally falls within a certain range. Note that consumers who travel extensively for work and/or pleasure should be studied individually and uniquely, as their behaviors will not be as predictive as those who do not travel frequently. Consumers who regularly travel can be identified through a historical transaction analysis.

The first step is for a financial institution to understand and identify the data that is useful in determining what variables to use as predictors. This can be accomplished through a process known as data mining. It is imperative for a financial institution's analytics team to identify the data can be accessed in a pure form, meaning that there should be minimal opportunities for error. Data that is derived from multiple sources should be heavily scrutinized and tested, as this process may show weaknesses and raise doubts of integrity. It is vital to implement a quality assurance protocol to ensure that the data is reliable and free of errors.

The variables are tested through mathematical expressions that can be generated using Microsoft Excel formulas. More sophisticated and enhanced tools can be purchased to fit within the financial institution's needs. Basic functions and macros can provide explanations of the

data supplied from the ATM terminal and transactional hosting platform. The mode, average, maximum and minimum value of the variables can be tested to determine which transactions are most likely the legitimate ones. This historical data can be continually recalculated with new transaction data that is not suspected to be fraudulent. The outputs generated will then be used as examples to develop rules through logical expressions. The rules will trigger once the transaction is activated within real-time. The rules can trigger two functions on suspected fraudulent transactions: either a transaction block or a transaction alert.

Creation of the Data Set

Appendix B includes an attached spreadsheet of the raw data created for 250 sample customers' ATM usage for the duration of six months. This data set is specific to ATM PIN-based transactions only. The ATM card can serve as a dual purpose debit card at merchant point of sale terminals, using both PIN-based and signature based transactions. However, for the purpose of scrutinizing specific data sets, this project does not include retail sales. It can be advantageous for a financial institution to include debit and credit card transactions into the history when conducting this type of analysis, so as to enhance the intelligence developed through the customer's profile.

The data set was created as a sample and is not representative of any factual industry based data set. However, the logic developed is versatile and can be replicated to fit within any financial institution's ATM consumer base. This data set corresponds with customers of "Fictitious Bank A", a Philadelphia metropolitan regional financial institution. "Fictitious Bank A" has twenty-six ATM locations. The study included 154 ATM locations from a total of twenty-six individual financial institutions. The following sections, along with Appendix A and

B, explain the contents of the Microsoft Excel spreadsheets, in addition to the logic used in creating the sample data set.

Raw data tab.

The Raw Data tab consists of four different types of information to base the fraudulent assumptions on. Data gathered at the time of the transaction is found in Columns A, B, D, E, F, and I. This data consists of a customer number, date of transaction, time of transaction, ATM terminal ID number, amount of the withdrawal and the zip code of the ATM. This is the typical data that a financial institution may record on a per transaction basis. The second type of data is that which is known of the customer at the time of the transaction. Financial institutions are held to the Know Your Customer due diligence through the Bank Secrecy Act. This data can be gathered from the customer at the time of the application for the new account and updated once per year. Columns G and H, zip code of home and work addresses, fit within this category. The third type of data consists of the results of the calculations based on the demographic and behavioral metrics. These results were calculated on a per transaction basis. Columns C, J, K, L, M, and N fit within this category. This data consists of the day of the week of the transaction, distance by mileage of home and ATM, distance by mileage of work and ATM, distance by mileage from previous transaction, time since previous transaction in hours, and number of transactions within the same day. The final data element is the status of the transaction, found in Column O, indicating if this particular transaction was fraudulent, suspected of fraud, or legitimate. This field has been and can be continuously updated after the transaction has been investigated.

Customers were assigned a number between one and two hundred fifty. The amount of customer transactions was manually generated based off of an assumption of how many

transactions a customer would conduct within a six month time frame. Each row represents a unique ATM withdrawal. Both the Customer number and the number of withdrawals that correspond to the specific customer are found in Column A in the Raw Data tab. Next, a list of dates between January 1, 2012 and June 30, 2012 was randomly created. The sorted list of dates is found in Column B. Appendix A describes the sequence of how all of the data was generated and the calculations used to create the spreadsheet.

Fraudulent Behavior Predictor Hypothesis

The following are assumptions to predict whether regular and irregular behavior patterns will predict ATM fraud. The assumptions are based off of professional experience investigating losses due to ATM and debit card skimming.

1) Criminals will maximize the amount of withdrawal to reach the bank's daily spend limit.
2) Criminals will maximize the amount of withdrawal to reach the customer's maximum amount of funds in the account.
3) Customers typically withdraw similar amounts of money when visiting the ATM.
4) Customers typically use a few ATMs, those which are conveniently located to their home, job, travel route, or frequently used stores.
5) Customers typically do not withdraw cash from an ATM multiple times per day.
6) Customers typically do not make consecutive cash withdrawals in multiple cities, often several states away from each other in a short time period.
7) Identifying which ATM terminal was compromised is critical to identifying the full scope of the fraud.
8) Criminals and customers alike will conduct a balance inquiry on the cards prior to withdrawals to learn the amount of available funds.

Additionally, research identified that financial institutions in the United Kingdom who use predictive analytic software observed that criminals will conduct a balance inquiry prior to the initial withdrawal, typically just before midnight. They will withdraw the maximum amount for that day and then wait until after midnight to transact another withdrawal for the maximum amount (ATM Marketplace, 2012). Because the data being tested was created, and it is unknown how predictable of a variable the balance inquiry is, the assumption was not formally calculated. It will be referenced to in the Recommendations section.

Findings

The objective of predictive analytics is to determine future behavior by evaluating the past and present behavior. The logic should be designed to look for the unknown and discover what cannot be easily identified. The more expansive the categories of variables are, the easier it will be to create the assumptions. It is imperative to evaluate each variable based on its uniqueness to predicting behavior. When that task is accomplished, each variable can be appropriately weighted to determine how significant the behavior is. It is crucial to know that no one specific behavior can predict fraudulent transactions. Legitimate behavior based on unknown circumstances can make the data appear suspicious; however, there is a legitimate explanation of why the transaction appears that way. The only true verification of the transaction is with the authentic customer's approval.

The raw data was created by randomly generated numbers in Microsoft Excel based on assumptions of customer behavior. While it is unfair to formally evaluate the predictors of fraud based on this data set, the findings were noteworthy and are recommended to be further evaluated using an authentic data set. The data was analyzed at the transaction and customer levels. It was identified that by evaluating predictors of fraud to completely random data, 152 out of 2217, or 7%, of the total population of the transactions was identified as suspicious. There were 152 multiple transactions per day on 58 customers' accounts. Therefore, 23% of the fraud victims could be flagged just by evaluating the time and distance separating the last transaction when reviewing multiple withdrawals in one day. Within the multiple transactions per day, 42 transactions found on 18 customers' accounts were given the "warm card" status, as the time and distance from the previous transactions were not mathematically possible. The distance was greater than one mile per minute, for a total distance of less than 200 miles. This indicates that it

is not possible to drive from ATM to ATM within the time elapsed. To investigate matters such as these, one must first confirm the validity of the data, and then investigate the scenario based on the usage of a cloned card. When different modes of transportation are a likely scenario, multiple factors should be tested. It is vital to stress that results leading to suspicious transactions were generated off of random data. The power that each of the parameters holds can only increase when using an authentic data set that contains actual behavior to measure.

The Historic Data Summary evaluated the transactions according to the customer's prior behavior. This evaluation reviewed the amounts of the minimum and maximum withdrawal and calculated the mode and average of withdrawal. Distances of travel were also compared using the minimum and maximum distances from ATM to home and ATM to work and calculating the averages of both. The average time in between transactions was also calculated in hours.

The Historic Data Summary acts as a customer reference guide. The analytics system should have the ability refer to the customer reference when evaluating the current transaction's criteria. The system should be designed so that if the transaction in question falls outside of the historical thresholds, it should be flagged for inquiry.

Recommendations

This study provided a framework for a financial institution to design a strategy plan. Each financial institution must consider unique parameters that are outside of this study to effectively manage their own risk, such as the needs of the customer base, geographical footprint, budget guidelines, software and hardware capabilities, and adaptability to changing technology. ATM fraud is expected to persist as long as ATMs are expanding, however, the methods of fraud will evolve as EMV is introduced into the United States.

Financial institutions need to be able to understand where fraud is particularly impacting the business. This knowledge will allow risk management professionals to identify what prevention and detection measures will be most effective to implement. It is common practice for financial institutions to issue debit cards that have the ability to be used at ATMs, in addition to retail point of sale terminals. It is essential for a financial institution to categorize the transactions at a retailer separately from the transactions at an ATM terminal. The retail data can be analyzed with the ATM data to help identify possible fraud more quickly. The confirmed fraud transaction data can then be used to determine behavior patterns and trends of crime rings. ATM data is often handicapped because ATM transactions are coded as PIN based, while it is also possible for a consumer to conduct a PIN based transaction at a retailer. A financial institution is not gaining an adequate perspective of what the data reads by combining two different transaction types into one metric. Therefore, it is essential for financial institutions to properly retain and categorize transaction data.

Financial institutions can also provide customers the option of adding security controls to their specific accounts. Many customers will only withdraw funds at an ATM from a specific account. By allowing the customer the option of which account or accounts to connect the ATM card to, fraud losses can be minimized. If a customer opts to never access funds through specific accounts, controls can be added to block those accounts at the ATM. It is essential to make business as convenient as possible for the customer. So, it would be advantageous for the financial institution to allow the customer the add-on option at anytime, only after identity authentication can be established. It should also be explored to allow customers the option of lowering the amount of allowed withdrawals. If the daily withdrawal limit is $1000.00, but a

customer chooses to never withdraw more than a few hundred dollars at a time, the customer should be given the option of lowering the daily withdrawal amount threshold.

It is crucial for risk managers to uphold security at the same time of maintaining customer satisfaction. Therefore, blocking transactions at the time of withdrawal without completing authenticating the identity of the customer is not recommended. The strategies outlined in this study use mathematical expressions that are reliable. However, the expressions should be regarded as highlighters, instead of confirmations. The only confirmation that the financial institution can receive is that which is directly from the customer. Financial institutions can incorporate communication standards into the withdrawal process. It is crucial for the financial institution to do this without negatively impacting the time it takes to complete the transaction. So, the communication would have to occur afterwards. The financial institution can send text alerts to the customer outlining any activity that falls outside of the parameters set forth with the Historic Data Summary. The adoption of mobile payments into our culture will enhance this practice. Mobile devices can assist with tracking transactions through the global positioning systems, if authorized to by the customer.

The financial institution's logic team can design the analytics system based on practicality. The financial institution can choose to adopt rules, similar to mathematical if/ then statements, to alert on any irregular transactional behavior. If/ then statements can be designed to uniquely adapt to the organization. An example of an if/ then statement that was relevant to this data set is "If distance equals greater than one mile per one minute, then flag transaction to be reviewed." This type of evaluation is more suited towards a single variable leading to a high probability of fraud.

The logic team can also decide to use the metrics studied here, in addition to others developed through debit card activity, to design a transactional model that could evaluate each transaction. Each variable can be weighted differently. Multiple conditions increase the probability of a fraudulent transaction. Therefore, each condition can have a point value and transactions exceeding a specified score for the transaction would be listed as a suspect transaction to be investigated further. The logic team can also set up different responses for transactions with different score ranges. Examples of conditions to be tested can include:

- Amount of withdrawal with respect to historical mode, average, maximum value, minimum value (can lead to a test transaction)
- Time frame in between transactions relative to the historical average
- Amount of withdrawal compared to ATM withdrawal limit
- Amount of withdrawal compared to account daily limit
- High crime risk zip codes
- Previously used ATMs that resulted in fraudulent withdrawals throughout the customer base
- Previously used ATMs by other customers who had fraudulent transactions at a later date
    - This could lead to where the data was compromised. This data should be combined with a time frame gained from intelligence on the compromise.

By adding additional data fields on a per transaction basis, financial institutions can improve fraud detection. One example, as previously discussed from the observations in the United Kingdom, is it would be beneficial to record balance inquiries with the transaction. Financial institutions could also find value in calculating the percentage of the withdrawal

amount to the available balance on a per transaction basis. Predictive analytics is dynamic and can be continuously updated with additional data fields and new rules or responses based on the results or changes in technology.

These strategies will assist in minimizing losses by identifying possible fraud early and preventing continued fraudulent transactions on that particular account. Industry experts are finding value in using mathematical logic to predict fraud. In June 2012, FICO was granted seventeen patents by the United States Patent and Trademark Office. Fifteen of the seventeen are for inventions in either predictive analytics or fraud solutions (ABA Banking Journal, 2012).

Conclusion

This project reviewed the prevalence and anticipated increase of ATM skimming fraud within the United States of America. Countries around the world have adopted unique security measures, such as Chip and PIN authentication and biometric identity validation through vein pattern recognition. These measures have readily been in use since the mid- 2000s, while the United States is still using outdated magnetic stripe technology. The antiquated systems are enabling our financial institutions and customers to become more susceptible targets.

Financial institutions can incorporate predictive analytics software solutions into their fraud strategy. The Marketing and Sales departments can also find value in introducing predictive analytics into their development strategies. Predictive analytics is useful for investigating ATM fraud, but can be also incorporated into credit and debit fraud, mortgage and loan account fraud, and deposit account fraud investigations. It is imperative for a financial institution to recognize that customers can withdraw money from any ATM terminal; therefore they can be victimized from any ATM terminal. The issuing financial institution is ultimately the bearer of the fraud losses. Therefore, incorporating a multiple strategy approach would be most beneficial. It is also imperative to recognize that the solution incorporates other methods of ATM fraud, while considering the potential future vulnerabilities. The technology must adapt to the scheme. Ultimately, the true customer must verify that the transaction was indeed completed by him or her. It is the role of the financial institution to make the verification process as timely, efficient, and seamless as possible. Predictive analytics can be continually updated to improve effectiveness, as well as to conform to new technology making it a versatile, long-term tool against fraud.

REFERENCES

ABA Banking Journal. (2012, June). *17 Patents Awarded in predictive Analytics, Credit Scoring, and Fraud Detection.* Retrieved from http://www.ababj.com/tech-topics-plus/17-patents-awarded-in-predictive-analytics-credit-scoring-and-fraud-detection-3027.html

A Free Zip Code Database + Latitude and Longitude. (2012, January). Retrieved from http://federalgovernmentzipcodes.us/

Adams, John. (2012, September). MasterCard pressures ATM owners to accept EMV. *American Banker.* Retrieved from http://www.americanbanker.com/issues/177_177/mastercard-pressures-ATM-owners-to-accept-emv-1052579-1.html

ATM Marketplace. (2012). *2012 ATM Software Trends and Analysis 5th Edition.* Sponsored by KAL ATM Software. Retrieved from http://www.atmmarketplace.com/whitepapers/5071/2012-ATM-Software-Trends-and-Analysis

ATM Marketplace. (2012). *Anti-skimming Technology and EMV for the ATM.* Sponsored by TMD Security. Retrieved from http://www.atmmarketplace.com/whitepapers/1793/Anti-skimming-Technology-and EMV-for-the-ATM

ATM Marketplace. (2012). *ATM Security.* Sponsored by Diebold. Retrieved from http://www.atmmarketplace.com/whitepapers/4976/ATM-Security

ATMIA (2010). *The Many Socio-Economic Benefits of ATMs*. *A Whitepaper by ATMIA, the Global Nonprofit Trade Organization for the ATM Industry*. Retrieved from ATM Industry Association website: https://www.atmia.com/

ATMIA. (2012). *ATM Fraud Report 2012.* ATM Industry Association. Retrieved from ATM Industry Association website: https://www.atmia.com/

Bond, M., Choudary, O., Murdoch, S., Skorobogatov, S. & Anderson, R. (2012). Chip and Skim: cloning EMV cards with the pre-play attack. Retrieved from University of Cambridge, UK, Computer Laboratory http://dl.packetstormsecurity.net/papers/attack/unattack.pdf

CHOICE Financial Solutions. (2012). *Bank 2.0: 2012 Trends in Retail Banking.* Retrieved from http://www.choicefs.com/pdf/MIB_Bank_2_0.pdf

Diebold, Inc. (2011). *Battling Card Fraud through Chip and PIN Technology*. Retrieved from http://www.atmmarketplace.com/whitepapers/5397/Battling-Card-Fraud-through-Chip-and-PIN-Technology

EAST. (2012). *ATM Crime & Fraud Information.* European ATM Security Team Ltd. Retrieved from https://www.european-atm-security.eu/ATM%20Crime%20/

Edgington, B. (2007). *Your Quest for the Ideal Biometric: Is It In Vain? Introducing Hitachi's Finger Vein Technology: A White Paper.* Retrieved from http://www.hitachi.eu/veinid/documents/veinidwhitepaper.pdf

Hitachi, Ltd. (2006). *Finger Vein Authentication: White Paper.* Retrieved from http://www.hitachi.pl/veinid/documents/Finger_Vein_Authentication_White_Paper.pdf

Krebs, B. (2010). All About Skimmers [Web log post]. Retrieved from http://krebsonsecurity.com/all-about-skimmers/

Oracle (2010). *Predictive Analytics: Bringing The Tools To The Data.* An Oracle White Paper. Retrieved from http://www.oracle.com/us/products/applications/crystalball/risk-mgmt-analysis-wp-326822.pdf

Smartcard Alliance. (2011). *Card Payments Roadmap in the United States: How Will EMV Impact the Future Payments Infrastructure?. A Smartcard Alliance Payments Council Whitepaper*. (Publication Number: PC – 11001). Retrieved from Smart Card Alliance website:http://www.smartcardalliance.org/resources/pdf/Payments_Roadmap_in_the_US_091512.pdf

Strickland, E. (2012, June). The biometric wallet. *IEEE Spectrum.* Retrieved from http://spectrum.ieee.org/biomedical/imaging/the-biometric-wallet/0

United States Secret Service. Criminal Investigations. (2012, July). Retrieved from http://www.secretservice.gov

Von Graevenitz, G. A. (2007). Biometric authentication in relation to payment systems and ATMs. *DuD: Datenschultz and Datensicherheit.* Retrieved from http://www.esg-consulting.com/uploads/media/Biometric_authentication_DuD_2007.pdf

APPENDICES

Appendix A – Calculations of Raw Data

Date tab.

- Column A & B: Assigned each date between January 1, 2012 and June 30, 2012 a sequenced numeric value between one and 182.
- Column E: Randomly generated a list of numbers between one and 182 using the Microsoft Excel formula =INT(RAND()*182+1).
- Column G: Used the randomly generated number to LOOKUP the corresponding date from the table in Step 1 with the following Microsoft Excel formula: =VLOOKUP(RandomNumber,Sequence#:Date,Date).
    - Pasted the list of dates into Column B Date of transaction on the Raw Data Tab.
    - Sorted the dates per Customer # in Column A.

Raw data tab.

- Day of week of transaction in Column C corresponds to the actual date of transaction, such as 1 = Sunday, etc.
- Microsoft Excel formula =WEEKDAY(Column B)

Time Tab.

- Created five groups of randomly generated numbers to create the minutes of the day using Microsoft Excel formulas. Note: 360= Number of minutes of the day.
- Column B: 06:00 to 09:00 =INT(RAND()*181+360)
    - 181= Amount of minutes within the time range + 1 (Mathematical expression to ensure whole number is generated)

    - 360= Value of starting time in minutes
- Column C: 11:00 to 14:00 =INT(RAND()*181+660)
    - 181= Amount of minutes within the time range + 1 (Mathematical expression to ensure whole number is generated)
    - 660= Value of starting time in minutes
- Column D: 16:00 to 20:00 =INT(RAND()*241+960)
    - 241= Amount of minutes within the time range + 1 (Mathematical expression to ensure whole number is generated)
    - 960= Value of starting time in minutes
- Column E: 00:00 to 24:00 =INT(RAND()*1440+0)
    - 1440= Amount of minutes within the time range
    - 0= Value of starting time in minutes
- Column F: 16:00 to 20:00 =INT(RAND()*241+960)
    - 241= Amount of minutes within the time range + 1 (Mathematical expression to ensure whole number is generated)
    - 960= Value of starting time in minutes
    - Note: This equation was repeated to emphasize assumption of heavier usage of ATM withdrawals in the evening hours.
- Column A: Randomly generated group number from one to five =INT(RAND()*5+1)
- Column G: Group number (Column A) was used to pull one of the time groupings from the five groups previously described in the same row and placed into Column G to determine the calculation for the time.
- Column H: =(Minutes from Column G) / 1440

    - Converts minutes to time per the Microsoft Excel format
    - Results in Column H were pasted into Column D (Time of Transaction) in the Raw Data tab.

- Note: The random generator function of Microsoft Excel updates whenever changes are made to a spreadsheet. Therefore, the data on the working sheet may no longer match the data pasted into the Raw Data tab.

Legend Tab.

- Twenty-six financial institutions were created, each named "Fictitious Bank" and then assigned to a letter of the alphabet.
    - Note: The data reflects the assumption that customers are of Fictitious Bank A, as more ATM terminals were created for Fictitious Bank A.
- Columns A, B, & C: ATM Terminal Codes were created using a two character Bank Code and then a sequence number of ATMs, totaling 154 ATMs corresponding to twenty-six financial institutions.
- Column D: ATM Zip Codes were randomly generated between 18500 and 19500 using Microsoft Excel =INT(RAND()*1001+18500).
    - Note: This area corresponds to the Philadelphia metropolitan region.
- Columns E & G: The validity of the randomly generated zip codes was verified against a download labeled "Free Zipcode Database" found on the website "A Free Zip Code Database + Latitude and Longitude" found on http://federalgovernmentzipcodes.us/ to be a standard, active zip code.

Zip Code Worksheet tab.

- Column A: Numbers were randomly generated between one and 154, representing each ATM using Microsoft Excel formula =INT(RAND()*154+1).
- Column C: These values were then copied to Column C due to the formula re-generating random numbers upon every edit.
- Column E: The values in Column C were then used to LOOKUP the ATM codes from the Legend tab using Microsoft Excel formula =VLOOKUP(C2,Legend!A:D,3).
    - The ATM Terminal codes were then copied to the Raw Data tab Column E, titled "ATM Terminal ID#". This column of data indicates the ATM terminal used by the customer for that particular transaction.
    - The ATM Terminal Zip Codes were then copied and pasted into the Raw Data tab Column I, titled "Zip Code / ATM".
- Column H: Randomly generated zip codes between 18500 and 19500 indicates customer's home and work locations using Microsoft Excel formula =INT(RAND()*1001+18500)
- Column J: Randomly generated values were then copied to Column J to verify zip code validity against the Free Zip Code database previously discussed. The corresponding verifications are found in Columns K & L.
    - After the Work Zip Codes were generated and verified, the column was copied and pasted into the Historic Data Summary tab, Column M, titled "Work Zip Code".

    - The Raw Data tab Column H was then populated with the following Microsoft Excel formula =VLOOKUP(A3,'Historic Data Summary'!A:M,13,FALSE) to LOOKUP the work zip code of each customer.
- Column J: Another set of randomly generated zip codes, indicating the Home zip code, was again copied from Column H to Column J and verified for validity against the Free Zip Code database Columns K and L.
    - This was then copied and pasted to the Historic Data Summary tab Column L for the customer's home zip code.
    - The Raw Data tab Column H was then populated with the following Microsoft Excel formula =VLOOKUP(A3,'Historic Data Summary'!A:M,12,FALSE) to LookUp the home zip code of each customer.
- Column P was populated with dollar amounts for withdrawal transactions.
    - Assumption: Withdrawal amounts of $60.00 and $100.00 were strategically repeated to emphasize more common withdrawal amounts, such as the fast cash option and round number amount.
- Column O was created as an index for the dollar amounts.
- Column R has randomly generated numbers between 1 and 102, representing the index values of the dollar amounts, using Microsoft Excel formula =INT(RAND()*102+1)
- The values of Column R were copied and pasted into Column T due to the formula re-generating random numbers upon every edit.

- The randomly generated values from Column R were used to LOOKUP the corresponding withdrawal amounts using Microsoft Excel formula =VLOOKUP(T2,O:P,2)
    - These values from Column U were then copied and pasted into the Raw Data tab Column F (Amount of withdrawal).

Raw data tab.

The calculations with the Raw Data tab were based off of the demographic and behavioral metrics. These results were calculated on a per transaction basis. Columns C, J, K, L, M, and N fit within this category. This data consists of day of the week of the transaction, distance by mileage of home and ATM, distance by mileage of work and ATM, distance from previous transaction, time since previous transaction in hours, and number of transactions within the same day.

The calculations are as such:

- Column J (Distance by Mileage of Home & ATM) & Column K (Distance by Mileage of Work & ATM) calculated using Microsoft Excel formula:

```
=ACOS(COS(RADIANS(90-VLOOKUP(G3,'Zip Code Data'!A:G,6,FALSE)))
*COS(RADIANS(90-VLOOKUP(I3,'Zip Code Data'!A:G,6,FALSE)))
+SIN(RADIANS(90-VLOOKUP(G3,'Zip Code Data'!A:G,6,FALSE)))
*SIN(RADIANS(90-VLOOKUP(I3,'Zip Code Data'!A:G,6,FALSE)))
*COS(RADIANS(VLOOKUP(G3,'Zip Code Data'!A:G,7,FALSE)-
VLOOKUP(I3,'Zip Code Data'!A:G,7,FALSE)))) *3959
```

The formula above is based on the distance formula for the spherical coordinate system using information found on Drexel University's Math Forum website http://mathforum.org/library/drmath/view/51756.html

- Column L:
- Column L (Distance from previous transaction) was calculated based off of comparing the current spherical coordinates to that of the most recent transaction prior using Microsoft Excel formula:
    - =ACOS(COS(RADIANS(90-VLOOKUP(I3,'Zip Code Data'!A:G,6,FALSE))) *COS(RADIANS(90-VLOOKUP(I4,'Zip Code Data'!A:G,6,FALSE))) +SIN(RADIANS(90-VLOOKUP(I3,'Zip Code Data'!A:G,6,FALSE))) *SIN(RADIANS(90-VLOOKUP(I4,'Zip Code Data'!A:G,6,FALSE))) *COS(RADIANS(VLOOKUP(I3,'Zip Code Data'!A:G,7,FALSE)-VLOOKUP(I4,'Zip Code Data'!A:G,7,FALSE)))) *3959
- Column M (Time since previous transaction (Hours)) was calculated by comparing the time of the current transaction to that of the most recent transaction prior using Microsoft Excel formula: =((B4-B3)*1440+(D4-D3)*1440)/60

Historic Data Summary tab- Calculations.

The following statistical calculations were performed on each customer's transactions off of the raw data to gain an understanding of the values generated. The Historic Data Summary categorizes each customer's behavior based on his or her history. The hypothesis is that no significant patterns of behavior indicating fraud can be generated from randomly generated raw data. However, after the data is analyzed to determine the normal patterns, it is assumed that the variations should be addressed as anomalies and investigated. The results are discussed in the Findings section.

1) Maximum Amount of Withdrawal-

   =MAX(IF(RawData!L:L="N",IF(RawData!A:A=A3,RawData!F:F)))

2) Minimum Amount of Withdrawal-

   =MIN(IF(RawData!L:L="N",IF(RawData!A:A=A3,RawData!F:F)))

3) Mode of the Amounts of Withdrawal-

   =MODE(IF(RawData!L:L="N",IF(RawData!A:A=A3,RawData!F:F)))

4) Average Amount of Withdrawal-

   =AVERAGE(IF(RawData!L:L="N",IF(RawData!A:A=A3,RawData!F:F)))

5) Minimum Distance from ATM to Home-

   =MIN(IF(RawData!L:L="N",IF(RawData!A:A=A3,RawData!J:J)))

6) Maximum Distance from ATM to Home-

   =MAX(IF(RawData!L:L="N",IF(RawData!A:A=A3,RawData!J:J)))

7) Minimum Distance from ATM to Work-

   =MIN(IF(RawData!L:L="N",IF(RawData!A:A=A3,RawData!K:K)))

8) Maximum Distance from ATM to Work-

   =MAX(IF(RawData!L:L="N",IF(RawData!A:A=A3,RawData!K:K)))

9) Average Distance from ATM to Home-

   =AVERAGE(IF(RawData!L:L="N",IF(RawData!A:A=A3,RawData!J:J)))

10) Average Distance from ATM to Work-

    =AVERAGE(IF(RawData!O:O="N",IF(RawData!A:A=A3,RawData!K:K)))

Appendix B – ATM Predictive Analysis Raw Data

Refer to the entire contents of the Microsoft Excel spreadsheets within the file ATMPredictiveAnalysis - Random Data.xls.

Appendix C – Raw Data Analysis

Refer to the entire contents of the Microsoft Excel spreadsheets within the file

RawDataAnalysis.xls