A COMPARISON OF UNITED STATES AND UNITED KINGDOM CREDIT CARD SECURITY STANDARDS

by

Miguel G. Thornhill

A Capstone Project Submitted to the Faculty of

Utica College

May 2015

In Partial Fulfillment of the Requirements for the Degree of Master of Science in Cybersecurity

Abstract

According to Heggestuen of Business Insider, the cost of United States payment card fraud grew by 29% to a staggering $7.1 billion. The $7.1 billion figure accounts for losses on purchase transactions for acquirers, issuers, and merchants. Inherent security flaws, massive data breaches, compromised consumer Personably Identifiable Information (PII) and escalating card fraud highlighted and expedited change in the United States payment card industry. The United States payment card industry has been using the legacy magnetic stripe card that was introduced in the 1960s. As a result, the U.S. payment card industry continues to outpace the rest of the world, accounting for 47.3% of payment card fraud. Like the United States, the payment card industry in the United Kingdom once boasted high financial losses due to fraudulent card transactions. However, since implementing the Europay MasterCard and Visa (EMV) standard between 2003 and 2006, card present (the consumer is using the physical card at a merchant) fraud losses have dropped significantly in the United Kingdom. Card present fraud, has dropped by 64% since EMV was introduced in 2003 (Ray, 2013). However, EMV is still vulnerable and is not a sole source and enduring solution for payment card fraud. Like EMV, Apple Pay is yet another step in the right direction on the path to thwarting payment card fraud. However, it too has inherent vulnerabilities. The Payment Card Industry may benefit from a NASA-like approach. They may need to end present card payment systems and let competition produce the best of the breed for effective payment card security solutions to be realized.

Keywords: Cybersecurity, Apple, EMV, magnetic stripe, Point of Sale, POS, Christopher Riddell, ECS, RCS.

Acknowledgements

The capstone project signals the culmination of a demanding but rewarding adventure that spanned over two years at Utica College. This conclusion would not be possible had God not given me the ability to endure. Therefore, it is right to give him thanks, thank you God for making this possible. My adventure and the subsequent rewards started from a cold call to Jim Sconnely Throughout my time at UC, I found Jim's interaction and concern pervasive amongst the UC staff.

Although, the first residency was somewhat overwhelming, there was considerable support from everyone involved. That support continued through the entire graduate evolution. From Professor Gloo through Professor Lee, my Professors did an excellent job establishing standards, imparting knowledge and sharing valuable real world experiences. A collective thanks to all my Professors, thank you for your time and the invaluable interaction. To my cohort members, especially Angeo, thank you sharing your collective experiences and considerable talents. It enriched the UC learning experience.

Lalo Munoz, my friend, thank you for your time and the explanations. To my first reader, Professor Riddell, you took the time to get me zeroed in and on target. Thank you for being available, and for the old school tough Navy love. My second reader and mentor, Kevin Sawyer, I cannot thank you enough for your time, encouragement and guidance on this journey.

To my wife, Sonya, our kids, Tori, Kayla, Danyelle, Anthony, Miguel, mom, the rest of the family, and friends thank you. Thank you for putting up with my self-imposed isolation, late hours, "not right nows", and "I can'ts". A lot has transpired these last two years that could have derailed the whole thing. Through it all, when I was tired, your love and support have been amazing and provided the strength that I needed. Thank you all!

Table of Contents

List of Illustrative Materials……………………………………………………………vi

A Comparison of United States and United Kingdom Credit Card Security Standards………..1

Literature Review……………………………………………………………………….8

Current Technologies and Standards……………………………………………………8

Apple Pay………………………………………………………………………..………..8

Near field communications……………………………………………………………10

Apple Pay vulnerabilities……………………………………………………………...10

The history of EMV……………………………………………………………………..11

The EMV standards…………………………………………………………………...13

EMV functionality……………………………………………………………………14

EMV vulnerabilities…………………………………………………………….……..17

The history of the magnetic stripe……………………………………………….……17

The magnetic stripe standards………………………………………………………...18

Magnetic stripe card functionality…………………………………………….……20

Magnetic stripe card vulnerabilities ………………………………………………..21

The lessons learned from the EMV standard…………………………………………22

EMV adoption was slow in the U.S…………………………………………………..25

Fraud protection and reliable telecom hamper U.S. shift to EMV……………….…....28

Financial fraud losses are the tipping point…………………………………….….…..29

The U.S. implementation of EMV and the October, 2015 deadline…………………......31

Discussion of the Findings………………………………………………………….….…...32

Technologies and standards…………………………………………………….………..33

Future Research and Recommendations……………………………………….………..41

References………………………………………………………………………….……47

List of Illustrative Materials

Figure 1: Security of EMV versus Magnetic Stripe Cards. 7
Figure 2: Timeline of EMV chip technology.. 12
Figure 3: Initiation of Computer-Chip Card Payments... 15
Figure 4: Process flow of an EMV transaction.. 16
Table 1: Leading digit in Primary Account Number for major credit card brands……... ……...19
Figure 5: Initiation of magnetic card payments.. 22
Table 2: The Cost of the U.S. EMV roll-out……………..……………………………………..27
Table 3: EMV Fraud Liability Implementation Matrix Timeline.....……………..……………32

A Comparison of United States and United Kingdom Credit Card Security Standards

With nearly 1.4 billion credit cards in circulation, there is no denying the credit and debit card market in the United States (U.S).is mature and highly developed. That 1.4 billion number means almost 77% of the U.S. population or around 181 million persons carry a credit card. "Credit cards are used more than 20 billion times a year with a total transaction volume of $1.9 trillion which is equivalent to roughly 12.9% of the country's GDP" (Kumar Choudhary, n.d., p.1). Further, Choudhary asserted the U.S. reliance on the legacy magnetic stripe card technology and standards have made the U.S. credit and debit cards industry more susceptible to fraud. The U.S. accounts for approximately 47% of global fraud losses although it only accounts for 27% of global volume purchases (Choudhary, n.d., p.1).

The purpose of this research was to compare the security standards of credit and debit card systems of the United States (U.S.) to that of the United Kingdom (U.K.). What are the predominant credit and debit card technologies and standards in use today? What lessons can be learned from the Europay, Mastercard and Visa (EMV) standard used in the United Kingdom? Why has the United States been slow to adopt the integrated chip and pin technology?

Digital currency, specifically in the form of debit and credit products is an increasingly important part of daily life for consumers, businesses, governments and cyber criminals around the world. There is no disputing this when, in 2008 almost 25% of worldwide consumer spending was through some form of payment card, up from 16% in 2003 ("Payment Cards," 2010). Unfortunately, as vital and viable a source of commerce for consumers, businesses, and governments that credit and debit cards are, they are equally vital and viable for criminals across the globe.

Brokering in lost and stolen payment card information is a lucrative business. Hackers who conduct business in the cyber underground produce and sell packages of counterfeit cards from information garnered from lost and stolen payment cards. There have been two major players in the world of counterfeit payment cards. Eleven years ago a Ukrainian known as Maksik was the best-known source for counterfeit cards. Today, another Ukrainian, Rescator is the proprietor of the ill-gotten fraudulent card packages (Poulsen, 2014).

A 2013 Business Insider report showed payment card fraud in the U.S. grew by 29% to 7.1 billion (Heggestuen, 2014). The UKCARDS Association puts card fraud numbers at 388 million pounds that is the equivalent of almost 600 million dollars (UKCARDS, 2013). Although, 600 million dollars is a large sum it pales in comparison to the U.S. losses, $7.1 billion as reported by Business Intelligence (Heggestuen, 2014).

A 2014 Association of Financial Professionals (AFP) survey sponsored by J.P. Morgan concluded that credit and debit card fraud including corporate and consumer cards increased by nearly one-third (J.P. Morgan, 2014). Findings from survey respondents showed exposure to card fraud increased from 29% in 2012 to 43% in 2013 (J.P. Morgan, 2014). Fraudsters prey on credit and debit card systems and their users because they are relatively easy targets (Fahey, 2015). The ecosystem of the credit and debit card industry includes, but is not limited to, the physical cards, point of sale devices, financial databases, network and telephone devices. In order for a single credit or debit card transaction to process, all of those devices must communicate with each other in a secure way. There are two established credit card systems and standards in use across the globe. Although there are similarities between both standards with respect to how credit and debit card transactions are processed there are obvious differences in the intrinsic characteristics of the actual credit and debit card mediums.

The United States credit and debit card security standards involve the use of magnetic stripe (magstrip) cards that transfer static data and are verified by customer signature. International Business Machines (IBM) first introduced this standard in the late 1960s. Very little in the way of security improvements have been made since the late 1960s, however. The lack of security improvements means these type of cards and the ensuing transactions are easier for criminals to hack (Kiplinger's, 2014). The United Kingdom's credit and debit card security standards involve the use of chip-enabled cards that use Europay, MasterCard and Visa (EMV) technology. The EMV standard was introduced in the early to mid-1990s and adopted in the United Kingdom between 2003 and 2006 (Anderson, 2014). Cards equipped with chips use EMV technology, which means each transaction is encrypted and unique when used in conjunction with a terminal set up to accept EMV payments (Kiplinger's, 2014). Further, most EMV transactions rely on the use of pins as opposed to signatures for verification.

There are a plethora of reasons why consumers choose to use credit and debit cards. Consumers use them to make purchases because, credit card issuers offer a number of incentives. Banks, credit unions, and stores lure consumers with signup bonuses, cash back, investment rewards, and frequent flyer miles, as well as additional enticements. Although a number of those lures are attractive, many people use credit cards because of the security and protection they offer the buyer. A Forbes financial professional explains, "credit cards create a barrier between merchants and your own money. If nothing else, credit card companies are good at handling fraud, and they create a line of defense between fraudsters and your money" (Landes, 2013, p. 2).

Consumer personally identifiable information (PII) plays an integral role in the processing of credit and debit card transactions and is a high-value target for fraudsters and criminals. PII includes the account number, expiration date and Card Security Code (CSC) also known as the Card Verification Value (CVV). That is all the information required to process a credit card transaction. If that information makes its way to a criminal, cyber or otherwise, the card's owner is susceptible to fraud being perpetrated against them. That is a synopsis of why credit cards need tighter and evolutionary security standards.

The need for tighter credit and debit card security was highlighted in 2013. Target, a major United States retailer, was the victim of an enormous data breach. The Target data breach exposed the credit card, debit card and personally identifiable information (PII) of 40 million of its customers (Krebs, 2014). Target had its computer network hacked, and subsequently consumer credit and debit card information was stolen by the hackers. ABC News reported the Target breach to be the second-largest retail cyber-attack in history (Zimmerman, 2014). The attackers targeted the data stored on the magnetic stripes of customers' cards (Winchester, 2014). The information stolen during the attack included customer names, card numbers, card expiration dates, card security codes, and debit card PINs. The consequence of such a catastrophic loss is that thieves can easily make and sell duplicate cards that can be used to make purchases as if they were the original cards.

In the 2013 Target breach, it is believed the perpetrators used credentials they stole from the heating, ventilation and air conditioning (HVAC) vendor to install malware that placed the attackers right at the card reader. The malware gave the hackers a unique perspective, almost as if they were standing over the customer's shoulder in the checkout line (Zimmerman, 2014). The persistent attack was perpetrated over several months and was carried out by installing malware into the retailer's security and payment system (Winchester, 2014).

Unfortunately for retailers, in addition to the weak security of the physical magnetic stripe card, magnetic stripe POS systems contain at least three additional vulnerabilities. Those vulnerable locations or states of data are as follows.

1. Data in Memory—A number of operations happen with the payment card data in the memory of the hosting computer when a payment application processes an authorization or settlement. The operations typically happen in the RAM of the POS machine.
2. "Data at Rest—The payment application stores data, either temporarily or for the long-term, on the hard drive
3. Data in Transit—The payment application sends and receives data to and from other applications and devices." (Gomzin, 2014, p. electronic)

Data in memory, data at rest and data in transit all represent opportunities for hackers to gain access to sensitive customer information. In the case of the Target breach hackers accessed customer information via malware that was used to infect the POS terminals. The malware was activated each time a customer swiped their legacy magnetic stripe debit or credit card. Once swiped, the compromised card's information was then stored on a server which the hackers had gained access. During a subsequent investigation, it was also discovered the attackers had gained access to customers' pin numbers, encrypted within the cards' data (Winchester, 2014).

Although the Target data breach was an elaborate hacking scheme, which required the use of malware, magnetic stripe cards can be compromised with more rudimentary skimmers. Credit and debit card skimmers are devices that thieves install at point of sale (POS) devices that copy account data from the magnetic stripe on the back of consumer cards. In some instances, the skimmer can obtain the consumers pin as it is inputted to the device (Krebs, 2014).

The magnetic stripe technology in use in the United States credit card industry is four decades old. Many security and technology advancements happen in forty years. Although some U.S. credit card companies and banks have made a halfhearted attempt to upgrade their credit cards standards with chip and signature cards, the preponderance of credit card companies still use the magnetic stripe and signature standard. Magnetic stripe equipped cards in use in the United States are too easily compromised and duplicated (Sullivan, 2013). The ease of magnetic stripe counterfeiting is in stark contrast to the EMV, chip-enabled cards in use in the U.K.

Cards with an embedded computer chip such as those used in the U.K. to render payments have many more capabilities than magnetic-stripe cards. Computer-chip cards are intrinsically more difficult to compromise and duplicate. As a result of the artificial intelligence in the chips the cards secure information stored on the chip more effectively, and are capable of thwarting unauthorized intrusions (Sullivan, 2013). Chip cards that adhere to the EMV standard can use encryption to protect sensitive data. The chip cards can validate messages that it receives, and can send messages to issuers that enable the issuers to authenticate transactions more reliably than they can with magnetic stripe cards. If required, computer-chip payment cards are capable of modifying payment data for security reasons (Sullivan, 2013).

The functionality included on computer chip embedded cards provides the payment card the ability to encrypt data, which makes processes such as Dynamic Data Authentication (DDA) and Combined Data Authentication possible (CDA). Dynamic Data Authentication is a "type of Offline Data Authentication (ODA) in which the card uses public key technology to generate a cryptographic value, which includes transaction-specific data elements, that is validated by the terminal to protect against skimming" ("Chip Terms Explained," 2002, p. 3). CDA, an enhanced version of DDA "not only provides the dynamic aspects of DDA (hence protection against cloning), but also ensures the integrity of sensitive data communicated between the card and terminal, hence protecting against complicated wedge attacks" ("Managing Fraud with EMV," 2011, p. 8).

Magnetic stripe cards are incapable of performing those functions because they bear static verification codes that do not change from one transaction to another. Additionally, computer-chip payment cards are capable of producing a distinct verification code for each transaction (Sullivan, 2013). Figure 1 addresses four basic security features and highlights the differences between EMV-compliant cards and magnetic stripe cards. It also covers four security feature flaws of magnetic stripe cards. The flaws consist of the magnetic stripe cards relative ease of access by unauthorized persons. Magnetic stripe cards are more susceptible to skimming, counterfeiting and the associated counterfeit fraud that results from a skimmed card.

Security Feature	EMV-compliant Card	Magnetic Stripe Card	Security Feature Flaw in Magnetic Stripe Card
Card Possession	Cardholder retains possession of contactless EMV chip cards and taps the card on a reader	Cardholders typically give their cards to a sales clerk in all other POS environments	The potential for skimming data from the card increases when the card leaves the cardholder's possession
Card Design	Card is based on highly secure smart chip technology which makes EMV chip card extremely difficult to counterfeit	Magnetic stripe data can easily be skimmed from a card or stolen from non-PCI- DSS compliant data network or storage	Skimmed card data can be used to create a counterfeit card
Transaction Security	EMV chip card transaction produces a unique transaction code that does not allow reuse or replay of transaction data	Magnetic stripe card carries static data	Static data if skimmed or stolen, can easily be used to make a counterfeit magnetic stripe card
Card Authentication	EMV chip card allows authentication of the payment card for both online and offline transactions	No card authentication is possible for ISO standard magnetic stripe cards	Lack of card authentication exposes the magnetic stripe card to counterfeit fraud

Figure 1: Security of EMV versus magnetic stripe cards. Reprinted from EMV compliance in the U.S., by K. S. Choudhary, 2012, "Now is the time to make the transition to EMV," p. 6. Copyright 2012 by Capgemini.

There are a number of reasons why the U.S. Payment Card Industry (PCI) is now transitioning to EMV chip-enabled cards. Though EMV adoption is imminent, does it effectively deal with payment card fraud? Are there alternatives to EMV? Apple introduced Apple Pay, a mobile payment system that uses Near Field Communication (NFC) technologies. Will NFC solutions like Apple Pay, help address and mitigate payment card fraud? Considerable thought and debate need to go into the next evolution of credit and debit card security standards. The current chip and pin standard are certainly more challenging for criminals, but it is now a decade old and will soon be considered a legacy standard.

Literature Review

Current Technologies and Standards.

Kumar Choudhary of Capgemini reports the annual cost of fraud in the U.S. is $8.6 billion. That $8.6 billion figure represents 0.4% of the $2.1 trillion payment card industry. Further, the Capgemini report states U.S. fraud losses are expected to reach $10 billion per year by 2015 (Choudhary, n.d.). The UKCARDS Association puts card fraud numbers at 388 million pounds; that is the equivalent of almost 600 million dollars (UKCARDS, 2013). Why are instances of credit and debit card fraud so much lower in the United Kingdom than they are in the United States? It has been suggested chip cards that are part of the EMV standard offer stronger defenses against fraud, but vulnerabilities will remain (Sullivan, 2013). Should the PCI be looking at technologies like NFC and for solutions like Apple's Apple Pay?

Apple Pay. Apple markets Apple Pay, their mobile payment system as an innovative and easy way to make in store and in applications (apps) purchases.

> Apple Pay will change how you make purchases with breakthrough contactless payment technology and unique security features built right into the devices you have with you every day. So you can use your iPhone to pay in a simple, secure, and private way. (Apple, n.d., para 2)

The technology giant goes on to explain that making payments with Apple Pay is a natural motion that occurs when the phone's owner deploys an Apple device. The ease of use occurs thanks to the NFC antenna included in the iPhone 6. As a result of the NFC antenna, users merely have to hold their phone near the contactless reader while their finger is on the Touch ID (Apple's biometric fingerprint reader). "Once the payment is initiated a subtle vibration and beep alert the phone's owner the transaction was successful" (Apple, n.d., para 3). In app purchase only require the phone's owner to use the biometric scanner to initiate a payment.

Although, Apple Pay is a simple and technologically advanced process it is still tied to the physical credit and debit card. In order for consumers to use Apple Pay, they must have a financial institution issued credit card. Apple's Passbook application is the repository that brokers the information exchange between consumer's credit and debit cards and their financial institutions. Cards are added via the iPhone's iSight camera or, they can enter the card information manually into Passbook. Users add credit card information to Passbook from their iTunes account by entering the card's security code.

When credit and debit card information is added to Passbook, Apple, and the financial institution coordinate to assign and link a unique Device Account Number (DAN) to the card. The linked DAN is inputted into Passbook ("Does Apple Pay," 2014). The assigned DAN is encrypted and stored securely in the Secure Element, which is a dedicated chip in the iPhone. The DANs are never stored on Apple Servers. When the iPhone is used to make a payment, the DAN, and a transaction-specific dynamic security code is used to complete the payment. Actual customer credit and debit card information is never shared by Apple or transmitted during the payment (Apple, n.d., para. 7).

Apple contends that one of the reasons Apple Pay is more secure is because, unlike traditional credit and debit card transactions where users may have to hand over their cards iPhone users will not have to relinquish control of their phones to make payments.

Another security feature that Apple markets about its Apple Pay is the protection that Find My iPhone offers users of lost or stolen phones. With Apple's Find My iPhone, phone users can put their device into lost mode, which will automatically suspend Apple Pay. For added peace of mind, device owners can completely wipe their iPhone. Additionally, Apple claims Apple Pay does not store payment transaction information. Instead, Passbook only keeps recent purchase information for user convenience.

Near field communications. NFC is a low-power radio frequency protocol that is capable of setting up communications between two devices, as long as the devices are almost touching. It shares similarity with EMV in that it adheres to ISO 14443 and operates within the globally available frequency of 13.56 MHz. The low power radio frequency communication is both automatic and rapid as long as the devices are within a hypothetical range of about 20 centimeters or eight inches. However, in real world applications the actual distance is about four centimeters, or less than two inches. When an NFC session is started, it is referred to as tapping. NFC has a maximum data rate of 424kbps and is much slower than Bluetooth or Wi-Fi. However, NFC can invoke other protocols to facilitate data-heavy transactions, such as biometrics (Wood, 2012)

Apple Pay vulnerabilities. Although Apple Pay has been touted as the next generation for secure payments, it has already become the subject of unwanted attention from fraudsters. Tokenized DANs and biometric fingerprint readers are only effective if all the security protocols are being used as designed. Unfortunately, in the case of Apple Pay all protocols are not being used as intended. Early implementation of Apple Pay is already experiencing fraud. Fraud is being perpetrated because of lax provisioning checks by banks (Heller, 2015).

Heller claims there are reports of criminals configuring iPhones with stolen consumer information, then contacting banks to authenticate the victim's card on a new device. "This is so-called "Yellow Path" authentication, in which a card isn't automatically accepted (Green Path) or rejected (Red Path), but requires additional provisioning by the bank to be added to Apple Pay" (Heller, 2015).

In the event that provisioning is successful, the bank will assign a DAN to be stored on the iPhone's Secure Element chip. Successful provisioning is not an Apple Pay technology flaw. On the contrary, the issue is a two part problem. Apple waited too long to make Yellow Path checks mandatory. Additionally, the bank's Yellow Path processes are lax and inconsistent. Relaxed Yellow Path processes include requiring the last four digits of a consumer's Social Security Number (SSN) (Heller, 2015). As a result of the Yellow Path inconsistencies, there are reports that Apple Pay fraud numbers are roughly $6 per $100 worth of transactions. The PCI had ambitions that Apple Pay fraud numbers would be around $.02 to $.03 per $100 worth of transactions (Heller, 2015).

Apple Pay is a step in the right direction on the path to thwarting payment card fraud. However, Yellow Path verification standards need to be improved and enforced. Additionally, steps need to be taken to mitigate physical limitations of the Apple devices such as dead batteries, lack of retailer infrastructure, and damaged phones. Apple Pay will not work if the battery is depleted and or the device is damaged.

The history of the EMV. Like magnetic stripe technology, the chip card technology used in the EMV standard is decades old. However, EMV technology does receive periodic and substantial functional and security upgrades. France was the first country to conduct mass deployment of chip cards for payment by the banking industry. The high instances of fraud were due to lost or stolen magnetic stripe cards being counterfeited. The French banks conducted field trials of microprocessor chip cards embedded in plastic bank cards in 1984 (EMVCo, 2015). The new chip embedded payment cards stemmed the counterfeit card problem for the French. However, chip-enabled cards did not receive widespread European and eventual global exposure until a decade later with the introduction of the EMV standard (Sullivan, 2013).

The beta version of the specification titled EMV 96 Integrated Circuit Card Specification for Payment Systems was released in 1996. After testing the beta, the first production version of the EMV Chip Specifications, version 3.1.1 was made available in 1998. Version 4.3, published in 2011 is the current version of the EMV Chip Specifications (EMVCo, 2015). Figure 2, which is being used from EMVCo.com shows the timeline of chip and EMV technologies. Figure 2 covers the history of EMV from the inception of the first credit card through the magnetic stripe card, the first memory card and covers the timeline of the various versions of the EMV standard.

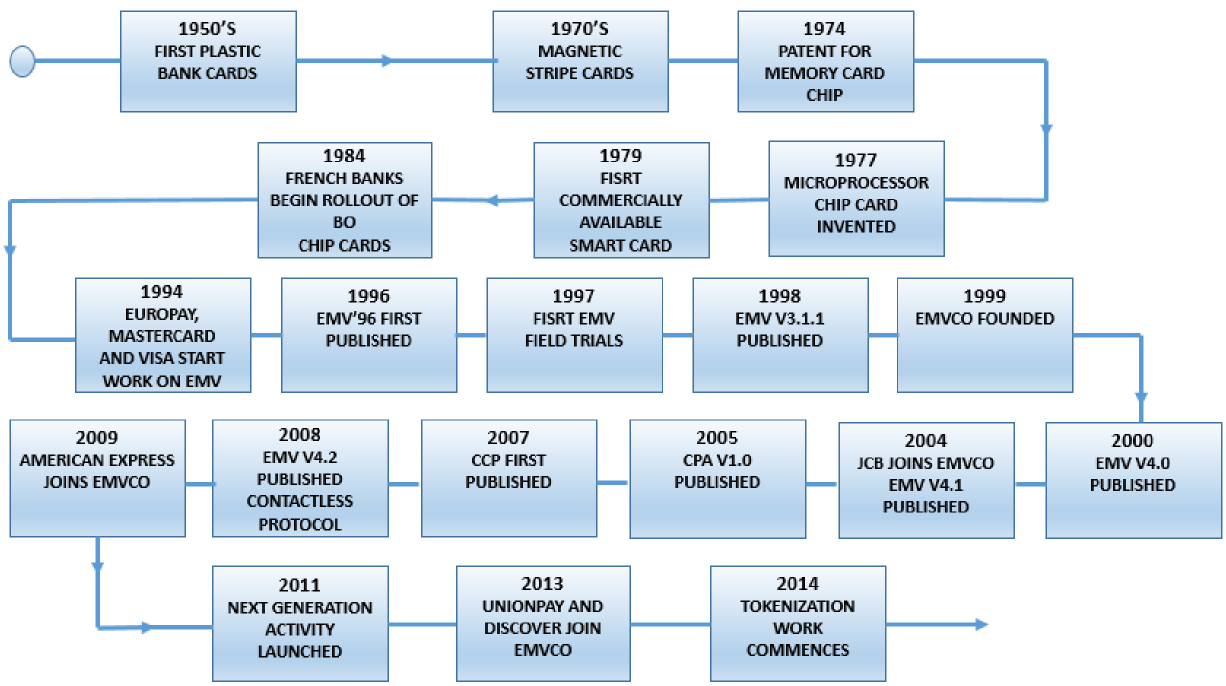

Figure 2: Timeline of EMV chip technology. Reprinted from "A Guide to EMV Chip Technology," by EMVCo, 2014, Version, 2, p.8. Copyright 2014 by EMVCo, LLC.

The EMV standards. According to EMVCo, EMV are Integrated Circuit Card Specifications for Payment Systems. Additionally, EMV are global payment industry specifications that describe the requirements for interoperability between chip based consumer payment applications and acceptance terminals to enable payment (EMVCo, 2015). EMV is the technology used for substantiating credit and debit card payments at smart chip-enabled terminals in the United Kingdom. The name and initials EMV represent the founding organizations from the 1994 European credit card payment standardization venture. The founding organizations were Europay, MasterCard, and Visa. As of 2009 the 1999 EMV trademark is now owned by all of the equity owners of EMVCo: American Express, JCB, Discover, MasterCard, UnionPay, and Visa. Today, EMV refers to the collective specifications, test procedures, and compliance processes managed by EMVCo (EMVCo, 2015).

The EMV Specifications are based on International Organization for Standardization (ISO) guidelines. EMV utilizes standards such as ISO 7816, ISO 14443, and ISO 8583, which define the physical, electrical, data and application levels for financial payment transactions (EMVCo, 2015). The basic premise of ISO 7816, ISO 14443 and ISO 8583 are follows:

- ISO 7816 is a multi-part global standard broken into fourteen parts. With respect to credit and debit cards, ISO 7816 is the worldwide standard for integrated circuit cards (universally known as smart cards) that use electrical contacts on the card, as well as cards that communicate with readers and terminals without contacts, as with radio frequency (RF/Contactless) technology (Nguyen, para. 8. 2015).
- ISO 14443 defines the interfaces to a "proximity" contactless smart card, including the radio frequency (RF) interface, the electrical interface, and the communications and anti-collision protocols. ISO 14443 dictates that compliant

cards operate at 13.56 MHz and have an operational range of up to 10 centimeters (3.94 inches) (Nguyen, para. 9. 2015).

- ISO 8583 is a three part standard and offers an outline for generating protocols for the interchange of financial transaction messages. The outline specifies a common interface by which financial transaction card created messages may be exchanged between acquirers and card issuers. Message structure, format and content, data elements and values for data elements are dictated by the outline ("ISO 8583-1:2003," n.d.).

EMV functionality. Credit and debit cards that utilize EMV contain an embedded microprocessor or smart chip. EMV embedded smart chip credit, and debit cards put the power of a computer onto the payment cards. Smart chip embedded cards give the credit and debit cards the ability to store and process data securely (EMVCo, 2015). That artificial intelligence provides an additional level of security against credit and debit card skimming and the production of counterfeit cards. The smart chip can provide additional security because it takes advantage of features such as data authentication, PIN entry and cryptographic technology (EMVCo, 2015).

The EMV smart chip cards have significantly more capabilities than magnetic stripe cards and interact with point-of-sale devices to accomplish very important security functions (Sullivan, 2013). Smart chip embedded cards are capable of ensuring the card is valid. Chip cards can validate that the card being utilized belongs to the person using it. Smart chip technology adds layers of security and is virtually impossible to duplicate (Sullivan, 2013).

Cards that have smart chips are capable of encrypting sensitive data. Smart chip cards can authenticate received communications, and can transmit messages to issuers that enable the issuers to validate transactions more reliably than can be accomplished with magnetic stripe cards. An additional security feature of computer-chip payment cards is they can modify payment data for security purposes (Sullivan, 2013). Figure 3, is a graphic representation of how the information flows through the three stages of processing a computer-chip card payment.

Figure 3 shows the information flow and process required to initiate a computer-chip card payment. There are three steps in the process. The first step in the process is card presentment. Card presentment begins with the dynamic verification code (DVC) being transmitted to the POS terminal. The second step is authentication and screening. During authentication and screening, the transaction data and DVC are sent to the card issuer. DVCs combat fraud because they change from transaction to transaction. Fraudsters cannot steal the card information and replay a static verification code to commit fraud (Sullivan, 2013). The third step is the decision to approve or reject the transaction. If approved, the cardholder can then enter a PIN and or signature to authorize the transaction.

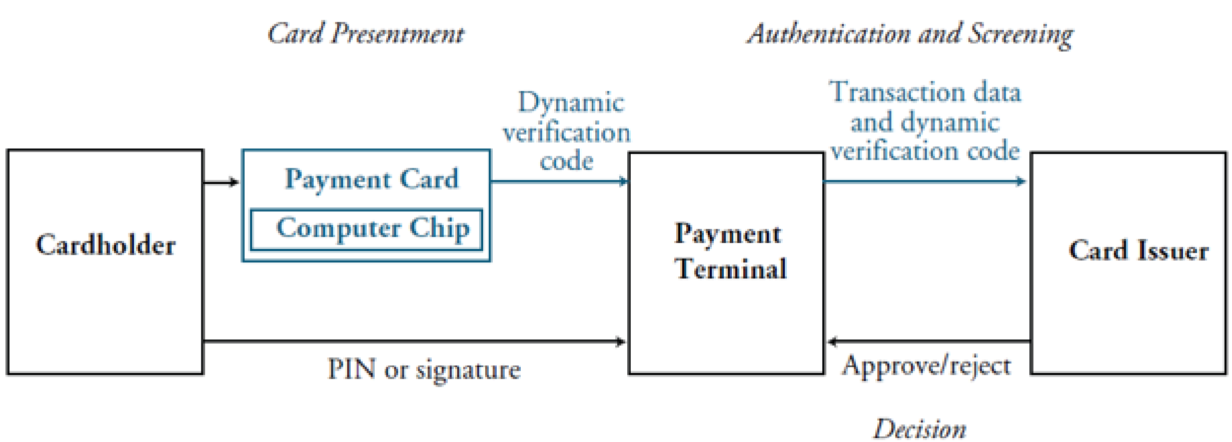

Figure 3: Initiation of computer-chip card payments, Reprinted from "The U.S. Adoption of Computer-Chip Payment Cards: Implications for Payment Fraud," by R. J. Sullivan, 2013, Economic Review, First Quarter, p. 69. Federal Reserve Bank of Kansas.

Choudhary reinforces Sullivan's assertion that the chip cards used in the EMV standard adds more security to credit and debit card transactions. According to Choudhary (2012), Enhanced security is the main driver for the global adoption of the EMV standards. Features of the EMV standard include card authentication, cardholder verification, and transaction authorization, all which are argued to constitute an extremely secure payment standard (Choudhary, 2012).

Figure 4 outlines and explains the nine stages of an EMV transaction. Application selection and initiation of selected application is the process where the card and terminal negotiate the application that will be used by the card holder. Card authentication verifies whether or not the card is legitimate. Check for processing restrictions utilizes ensures the chip is capable of performing the transaction selected. Cardholder verification validates the cardholder's identity and protects against identity theft. Terminal risk management is used to conduct predefined floor limit checks based on the transaction size. Floor limits are rules used to determine the requirements for payment approval (Sullivan, 2013). Terminal action analysis and card action analysis are user defined rules that are used to authorize the transaction. The final step is completion and script processing.

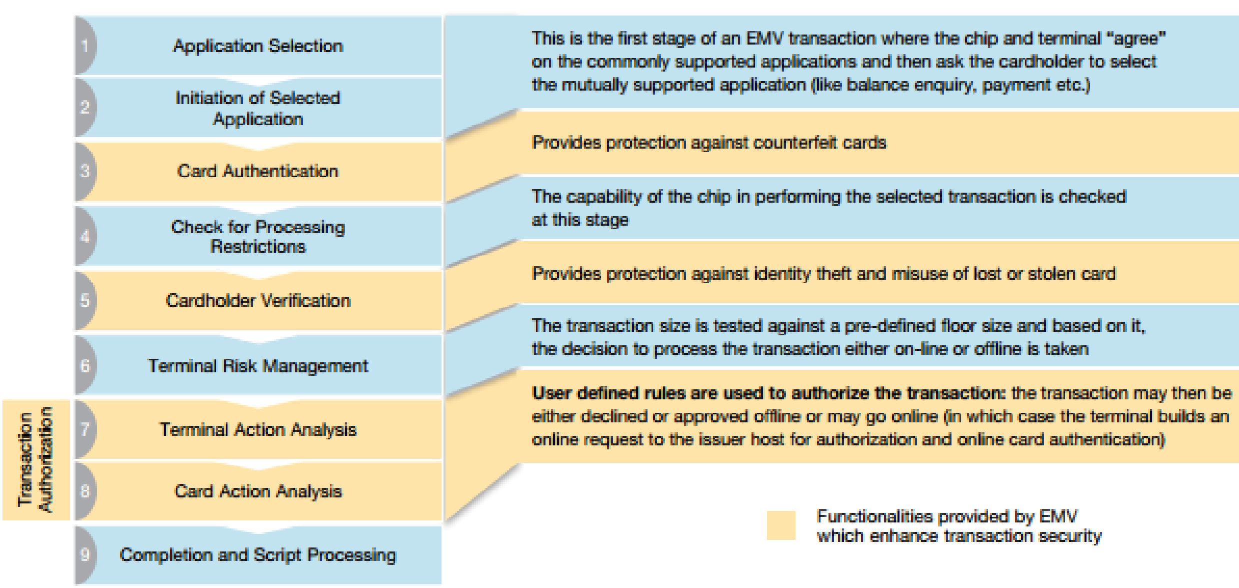

Figure 4: Process flow of an EMV transaction. Reprinted from EMV compliance in the U.S., by K. S. Choudhary, 2012, "Now is the time to make the transition to EMV," p. 9. Copyright 2012 by Capgemini.

EMV vulnerabilities. EMV standards are more secure than magnetic stripe standards. However, the EMV standards still have vulnerabilities that can be exploited by fraudsters. Chip and PIN cards used in the EMV standard are susceptible to PIN harvesting, counterfeiting, and the No-Pin attack.

1. PIN Harvesting is accomplished by using a fake credit card loaded with malicious software that is capable of reprogramming POS terminals. Fraudsters insert the fake card into the POS terminals and reprogram the terminals to store transaction information. Once the terminal is infected, the criminals can return at a later time with a second fake card to retrieve the information (Owano, 2012).
2. Chip and PIN cards that still have magnetic stripes to support backwards compatibility are still vulnerable to counterfeiting.
3. The No-PIN attack is used by criminals in possession of stolen credit cards when they do no not know the Chip card PIN. Perpetrators in possession of lost or stolen cards can place a small electronic device between the ill-gotten card and use any PIN (Anderson & Murdoch, 2014). The electronic device manipulates the card into thinking it is performing a chip and signature transaction while tricking the terminal to believe the PIN that was entered was accepted by the card.(Anderson & Murdoch, 2014)

The history of the magnetic stripe. U.S. credit card issuers and merchants are still using magnetic strip credit cards with signature verification as means of validating transactions (Sullivan, 2013). International Business Machines (IBM) engineer Forrest Parry pioneered the magnetic stripe system in the early 1960s ("Magnetic Stripe Technology," n.d.). Parry and IBM were the pioneers of the modern plastic credit card ("Magnetic Stripe Technology," n.d.).

Not only did one of IBM's Engineers create the magnetic stripe cards used by major credit card companies, IBM also played an expanded role in the creation of the credit card payment system ("Magnetic Stripe Technology," n.d.). IBM and other leaders of electronic payments teamed to create open compatibility standards. Working with the banking and airlines industries, IBM helped develop the approach that was adopted as a U.S. standard in 1969 and an international standard two years later in 1971. That meant that anybody could use their magnetic stripe credit or debit card anywhere in the world ("Magnetic Stripe Technology," n.d.).

Current U.S. magnetic stripe credit card technology was developed over four decades ago. As a result, it makes sense that cyber criminals target the U.S. credit card industry to perpetrate cyber crimes and credit card fraud (Fahey, 2013). Magnetic stripe credit cards store cardholder information directly on the magnetic stripe. The process to extract that information from the magnetic stripe is relatively straight forward for seasoned criminals. Once extracted the information is sold to criminals who encode the information onto new fraudulent cards (Krebs, 2014).

The magnetic stripe standards. Magnetic stripe credit cards transfer static data from the card and are verified by customer signature. IBM first introduced the magnetic stripe card in the late 1960s. The magnetic stripe embedded on the back of the credit card houses important data about the cardholder's bank account in the magnetic code. Each magnetic stripe is a plastic-like film made up of minute iron-based magnetic particles. The particles are extremely tiny bar magnets about 20 millionths of an inch long. Static information can be written to the magnetic stripe because the bar magnets can be magnetized in either a North or South Pole direction.

There are three tracks in each magnetic stripe. The tracks are:

- Track 1, which is the International Air Transportation Association (IATA) contains cardholder specific information. Track 1 contains the cardholder name, Primary Account Number (PAN) as well as other optional data. A PAN is up to 19 digits. Table 1 shows the four major credit card companies accepted in the U.S. and the first leading digit in their PANs (Gomzin, 2014).

Table 1

Leading Digit in Primary Account Number for Major Credit Card Brands.

Card Issuer	**PAN Starting Number**
American Express	3
Visa	4
MasterCard	5
Discover	6

Note: The table represents the major U.S. credit card issuers and the first digit of their issued card PANs.

- Track 2, which is the American Banking Association (ABA), is the track that is read by Automatic Teller Machines (ATM) and point of sale machines. The specifications found in this track were designed by the ABA, and the specifications are an international banking standard. Track 2 contains the cardholder's PAN, encrypted Personal Identification Number (PIN) as well as other optional information. Track 2, which is a shorter version of track 1 was implemented to improve performance of old dial up POS terminals (Gomzin, 2014, p. electronic).
- Track 3, defined by the Thrift industry (THRIFT-TTS) has a layout similar to tracks 1 and 2. However, it is seldom used.

The act of swiping the card is the catalyst that enables a card reader to read the static information contained on the card's magnetic stripe. Magnetic stripe card readers decipher the information contained on the three track stripe. The four and a half decades old magnetic stripe card specifications adhere to but are not limited to ISO 7810, ISO 7811-1-6 and ISO 7813 to ensure read reliability and worldwide acceptance.

- ISO/IEC 7810:2003 "is one of a series of standards describing the characteristics of identification cards. It is the purpose of ISO/IEC 7810:2003 to provide criteria to which cards shall perform and to specify the requirements for such cards used for international interchange. It takes into consideration both human and machine aspects and states minimum requirements" ("ISO/IEC7810," n.d., p. 1).
- ISO/IEC 7813:2006 stipulates the data structure and data content of magnetic tracks 1 and 2, which are used to begin financial transactions. ISO 7813 takes into account both human and physical aspects and states minimum requirements of conformity. It references layout, recording techniques, numbering systems, registration procedures, but not security requirements ("ISO/IEC7813," n.d., p. 1).

Magnetic stripe card functionality. Magnetic stripe credit cards rely on static encryption techniques for security. A key part of the magnetic stripe authentication process occurs during the time the card transmits encrypted information between itself and a POS terminal (Sullivan, 2013). Card issuers use cryptographic processes to write and store static verification codes into the magnetic stripes of cards they manufacture. The static code is verified each time a cardholder swipes the magnetic stripe card at a POS terminal. Once the magnetic stripe credit or debit card is swiped, the terminal transmits the verification code stored on the card to the card's issuing authority. The transmitted code is read by the issuer to verify its authenticity. Issuers ensure the code received is consistent with the PAN and has a valid expiration date. If fraud is suspected, the transaction will be declined. The static verification code stored on the magnetic stripe does offer merchants some level of assurance the transaction may be legitimate (Sullivan, 2013).

Magnetic stripe card vulnerabilities. Magnetic stripe cards are inherently vulnerable because of the static nature of their verification codes. The static nature of the authentication protocols used in magnetic stripe card transactions can be exploited in a number of ways to include sending false signals to card issuers (Sullivan, 2013). False signals include signature forgery, PIN harvesting, counterfeiting and use for Card Not Present (CNP) transactions.

1. Signature forgery is possible because card holders sign their credit cards as a means of verifying their identity. Fraudsters can forge cardholder signatures based on the signature on the lost or stolen card.
2. PIN Harvesting is accomplished by using a fake credit card loaded with malicious software that is capable of reprogramming POS terminals. Fraudsters insert the fake card into the POS terminals and reprogram the terminals to store transaction information. Once the terminal is infected, the criminals can return at a later time with a second fake card to retrieve the information (Owano, 2012).
3. Lost and or stolen magnetic stripe cards are more easily counterfeited than Chip and PIN cards because the information contained on magnetic stripe cards is accessible via a skimmer or card reader. A counterfeiter only needs a computer, new card and a magnetic stripe reader and writer to encoded and create counterfeit cards (Sullivan, 2013). This method is successful because criminals can make the counterfeit card seem legitimate by replaying the static card data from the original card (Sullivan, 2013).

Figure 5 depicts the process required to start a card payment. Magnetic stripe payments occur in three stages. The process begins with the card being presented for payment and the static verification code being transmitted. Next, the card and transaction will undergo authentication and screening. The third step in the process is the final decision to approve or reject the transaction.

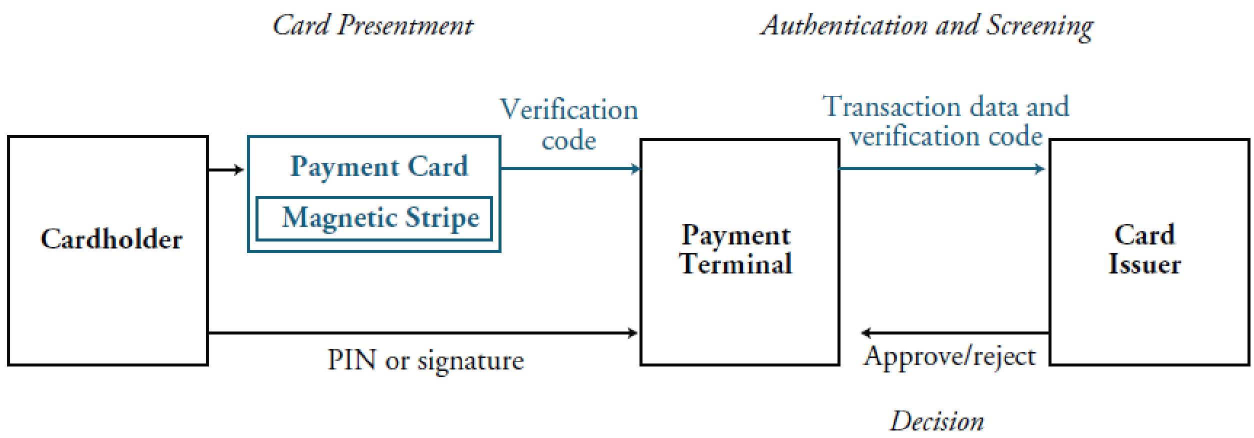

Figure 5: Initiation of magnetic card payments, Reprinted from "The U.S. Adoption of Computer-Chip Payment Cards: Implications for Payment Fraud," by R. J. Sullivan, 2013, Economic Review, First Quarter, p. 64. Federal Reserve Bank of Kansas.

The lessons learned from the EMV standard.

EMV chip-card technology that is currently being deployed in the United States has been in existence since the 1970s. It has been in use in the United Kingdom since the early 2000s. Prior to the adoption of the EMV standards, credit, and debit card fraud in the UK was higher than other developed nations (King 2012). Higher instances of fraud in the 1990s caused the Association for Payment Clearing Services (APAACS) to commission a study to determine the cause of systemic payment card fraud across the UK (King, 2012). King suggested transaction authorization was one of the major drivers behind card fraud in the UK. In the 1990s UK card transactions relied on offline authorizations. Unlike offline authorizations, online authorizations, allows issuers to refuse payments as soon as they become aware the card in question has been lost or stolen.

A solid telecommunications infrastructure is required to facilitate efficient online authorizations. Unfortunately, during the 1990s telecommunications in the UK were not as robust as required to support online transaction authorizations (Sullivan, 2013). As a result of the APAACS study, the EMV standard, also referred to as chip and pin, was adopted and deployed in the U.K. between 2003 and 2006 (Anderson & Murdoch, 2014). In the UK, all EMV transactions regardless of purchase or withdrawal require a pin hence, the moniker "chip-and-PIN" cards (Sullivan, 2013).

Chip and PIN cards, or EMV is a fraud-reducing technology that is capable of protecting both businesses and customers from loss. The credit and debit card industry began to see a return on their investment in EMV standards by 2005. By 2005 the benefits of EMV payment cards were apparent because fraud losses due to lost or stolen cards began to decline (Sullivan, 2013). The EMV standards and technologies provided increased fraud protection because of the computer chip and the required use of a PIN. Those two additions successfully limited the use of lost or stolen cards by unauthorized users (Sullivan, 2013).

Although instances of payment fraud declined in areas where the EMV standard was in place, fraudsters were not out of business. Fraudsters moved operations and concentrated on UK markets with weaker authentication. Weaker markets constituted those still using magnetic stripes and those that used Internet, mail order, and telephone order (IMOTO) purchases (Sullivan, 2013). The initial rollout of EMV cards in the UK was ill conceived. In order to facilitate backward compatibility during the transition, it was not uncommon for new EMV payment cards to have both computer chips and magnetic stripes. Unfortunately, those dual purpose cards represented a loophole and were the weak link in the new EMV standard (Sullivan, 2013).

Dual-purpose cards could still be counterfeited and used at facilities and in countries that still accept magnetic-stripe payment cards. Although the new EMV standard provided increased security, the credit and debit card industry in the UK experienced a spike in fraud related losses. The new fraud losses were still attributed to the counterfeit cards. UK fraud losses grew from £97 million ($176 million) in 2005 to £170 million ($312 million) in 2008 (Sullivan, 2013). How were counterfeit cards being used as part of the EMV standard? IMOTO transactions were not accounted for by the initial EMV standard and therefore remained unchanged. Therefore, IMOTO transactions enjoyed increased attention by fraudsters and increased rapidly, from £183 million ($333 million) in 2005 to £328 million ($602 million) in 2008 (Sullivan, 2013).

Fortunately, as the EMV ecosystem in the UK matured and became more robust fraud losses from counterfeit cards and on IMOTO transactions declined by 2008 (Sullivan, 2013). The decline in fraud numbers was attributed to two main factors. By 2008 more Automatic Teller Machines (ATMs) and merchants were equipped to handle transactions initiated with credit and debit cards from the EMV standard. The second reason was businesses in the UK were adopting 3 Domain Server (3D) Secure systems to service IMOTO transactions (Sullivan, 2013). 3D Secure is an Extensible Markup Language (XML) based protocol that is designed help prevent and reduce fraud by providing an additional security layer for online credit and debit card transactions ("3D Secure explained," 2014). There are three parties involved in each 3D Secure transaction. The parties involved are the merchant, the acquiring bank (the merchant's bank) and Visa and MasterCard (the card issuers). 3D Secure is led by the credit card schemes and is designed to make online shopping transactions safer by authenticating a cardholder's identity at the time of purchase. Verified by Visa (VBV) and MasterCard SecureCode (MSC) are the only members of this fraud prevention collective ("3D Secure explained," 2014).

EMV standards have done a lot to stem card present debit and credit card fraud in the UK. A 2014 ACI Universal Payments worldwide study found that from 2012 to 2014 credit card fraud in the UK fell from 31% to 25% of all respondents (Inscoe, 2014). Although it is working to prevent forms of credit and debit card fraud, EMV is not stopping it. As the U.S. works toward adopting the EMV standard criminals realize the days of the easy prey magnetic stripe are numbered. Criminals have already implemented new strategies to circumvent the security features of the EMV chip and pin or chip and signature cards.

EMV adoption was slow in the U.S.

The cost has been a driving factor behind the slow transition to the EMV standard in the U.S.; the upgrade and transition to the EMV standard will be $8.65 billion (Bose, 2015). Though the cost of transitioning to the EMV standard is expensive, the price of inaction will soon surpass the cost of the transition. The annual price of fraud in the U.S. is $8.6 billion. That $8.6 billion figure represents 0.4% of the $2.1 trillion payment card industry. Further, the Capgemini report provides that U.S. fraud losses are expected to reach $10 billion per year by 2015 (Kumar Choudhary, n.d.).

Upgrades and transitions are costly. However, the associated costs and subsequent processes are more tolerable when they offer holistic solutions to common problems. While the shift to the EMV standard addresses many aspects of U.S credit and debit card fraud, it does not address them all. According to Bose (2015), analysts predicted that card present fraud at physical retail locations will fall after the EMV chip standard is adopted in the U.S. However, instances of online fraud will follow the trend of increasing as was seen during other EMV roll outs (Bose, 2015). It has also been suggested that U.S. online fraud will reach as high as $6.6 billion by 2018 (Bose, 2015). That $6.6 billion figure is double that of what experts believe the number will be in 2015 (Bose, 2015). In light of the partial EMV solution, U.S. businesses have put off upgrades and transitions until they were deemed necessary. For U.S. businesses necessary is October 2015. October 2015 is the deadline credit card companies have established for the transition to the EMV standard.

After analyzing the tasks and associated costs to transition to EMV Javelin Strategy and Research, reported the numbers and dollar amounts in Table 2. The graphic in Table 2 is used courtesy of paymentsleader (researching the source) the single largest expense will be point of sale (POS) devices which are estimated to cost $6.75 billion. In order to be compliant with the October 2015 deadline, businesses are required to transition to new POS devices that can read chip-enabled cards. If businesses choose not transition or are slow to do so, they will be held liable for any fraudulent transactions that occur at the legacy terminals. The U.S. credit card industry will spend an estimated $1.4 billion to issue the new chip-enabled cards. Banks will absorb the cost associated with upgrading ATMs.

Table 2

The Cost of the U.S. EMV Roll-Out.

Item	Volume	Estimated Cost to Replace
POS Devices	15,000,000	$6,750,000,000
ATM's	360,00	$500,000,000
Credit/Debit Cards	1,126,800,000	$1,400,000,000
TOTAL:	1,142,160,000	$8,650,000,000

Note: Reprinted from Will retailers be ready for EMV by Oct 2015, by payments leader, 2013, Retrieved from http://www.paymentsleader.com/will-retailers-be-ready-for-emv-by-oct-2015/, Copyright, 2013 FIS and/or its subsidiaries.

Depending on the features desired, upgrading a single payment terminal to chip-and-PIN capability costs between $500 and $3000 (Bose, 2015). Additionally, the U.S. deployment of the EMV standard will require the installation of 15 million payment terminals that will carry a price tag of approximately $6.75 billion. The $6.75 billion price will require banks to spend some $1.4 billion to issue new cards and another $.5 billion to upgrade their Automated Teller Machines according to Javelin Strategy & Research (Bose, 2015, p. 1).

Upgrading to and or transitioning to the new EMV technology could be a major investment for banks and businesses, and it does not guarantee complete fraud protection. In light of the lack of guarantees, some business have opted out of EMV adoption and will assume the liability for fraudulent transactions as they await more proven fraud protection standards (Bose, 2015). While many retailers are aware of the push to upgrade to the new EMV standard by October, 2015, there are some who remain unaware of the EMV adoption. Smaller retail businesses have hardly been the victims of credit card fraud. Therefore there has been little incentive for them to learn about, let alone transition to the EMV standard. Retailer response to the October, 2015 EMV deadline has been mixed.

Though many support the impending U.S. PCI shift to EMV, others are concerned with what will come next. Like magnetic stripe standards, EMV standards are also old. What will the next standard be? Will it include point-to-point solutions (P2P)? “P2P works by encrypting cardholder data at one point (e.g., a payment terminal), transmitting the data through a network, and then decrypting the data at an endpoint (e.g., an acquirer or processor)” (Knopp, 2013, p.1). If the next standard relies more heavily on P2P, there will be additional cost associated with that upgrade. Security experts, estimate it would cost between $1000 and $4000 to install a point-to-point encryption terminal (Bose, 2015). Those figures represent a potential $500 to $1000 increase per terminal that merchants would have to invest.

Fraud protection and reliable telecom hamper U.S. shift to EMV. Unfortunately, the United States PCI has one of the best fraud protection systems in place, and that is yet another reason the shift to EMV has been slow (“EMV: America,” 2014). While the U.S. fraud problem has been significant, historically, it has been amongst the lowest rates of highly developed economically-mature nations (“EMV: America,” 2014). The use of online, real-time authentication used in the U.S. is credited for the low fraud numbers. The U.S. has one of the most highly developed and robust telecommunication networks in the world. Therefore, U.S. telecommunications support real-time authentication (Sullivan, 2013). Real-time authentication helps combat payment fraud at the POS terminal, which payments leader states is the best place to stop fraud (“EMV: America,” 2014).

The telecommunications network in the U.K. is not as robust and reliable. Therefore, the U.K. payment card transactions rely on offline authentication. In the offline authentication model, credit card transactions are grouped together at specific times. Normally, the grouped transactions are processed and then batched over to the card issuers for authorization at the end of the business day ("EMV: America," 2014). The time between when the transaction was made to when it is authenticated was significant enough that it left a window of opportunity in which fraudsters could commit undetected fraudulent acts.

Financial fraud losses are the tipping point. Financial fraud is believed to be the main driver behind the U.S. migration to the EMV standard ("Will Retailers be,"2014). It has been argued the magnetic stripe card standard used in the U.S. is weaker and has allowed international criminal elements to use counterfeit, lost, and stolen cards in the magnetic stripe ecosystem (Sullivan, 2013). Unfortunately, those international acts of cyber-crime can present significant international legal issues. Though global law enforcement agencies try to manage the acts of fraud, global losses have risen steadily ("Will Retailers be,"2014). Therefore pressure to find a global solution to card fraud is mounting. Payments leader puts the annual costs of card fraud in the U.S. alone at an estimated $8.6 billion per year. If the transition to chip card technology is not executed efficiently and expeditiously, experts believe that figure will rise to $10 billion or higher by 2015 ("Will Retailers be,"2014).

Although there may have been plans to upgrade or shift from the magnetic stripe standard, high profile data breaches that began in 2013 may have been the tipping point for change. In light of the number of high-profile breaches there was concern in the credit and debit card payment industry that the U.S. Congress would weigh in. There was concern Congress would provide guidance on the way ahead for card security standards (Daly, 2014). However, industry executives dismissed that notion because congressional oversight would only slow attempts to upgrade the antiquated standards or move to a new security standard. At a March 26, 2013 Senate Commerce Committee hearing Senator Ed Markey, D-Mass spoke on the topic of the need for new standards. Senator Markey felt there was no need for Congressional mandates to dictate the technologies required for the new standard. However, he did state the credit and debit card industry needed to keep up with technological changes, and if they could not or did not they would be liable for losses (Daly, 2014).

Although, the U.S credit and debit card industry has suffered the consequences of being the juiciest target for criminals looking for financial card information, it has also benefitted from its late adoption of the EMV standard. The U.S. adoption of EMV standards will benefit from years of historical perspective based on EMV roll-outs in other countries. The U.S. roll-out of EMV will also benefit from the fraud protection systems that card networks have already instituted to protect magnetic stripe cards (Groenfedlt, 2014). There are also two U.S. laws that deal directly with credit card fraud and incentivize corporations to offer protections from fraud. The two laws are the Fair and Accurate Credit Transactions Act43 (FACTA) and the Gramm-Leach-Bliley Act44 (GLBA). FACTA specifies merchants must truncate credit card numbers to five or fewer digits, and they should exclude expiration dates from receipts. GLBA addresses a merchants' vulnerability to hacking and requires financial institutions to safeguard sensitive data and explain their information-sharing procedures to their customers (Segal, 2011).

From a financial perspective, the U.S. implementation of EMV will come at significant cost savings. The technology and hardware such as cards and terminals are now considerably more cost effective to purchase (Groenfedlt, 2014). According to Groenfedlt, the aforementioned and the competitive nature of the United States will result in an accelerated migration to EMV in the U.S.

Eliminating fraud is an extremely ambitious goal and may not be realistic. However, thwarting and making the execution of fraud more difficult is attainable. The U.S. credit and debit card industry can help prevent fraud by instituting layers of security. Adoption of EMV is the first step in the way ahead for the United States credit and debit card industry.

The U.S. implementation of EMV and the October 2015 Deadline.

Implementation of the EMV standard in the United States is scheduled to occur by October of 2015. October 2015 is not an arbitrary date, it is the date the card issuers like American Express, Discover, Mastercard and Visa will have completed transitioning their systems and cards to meet the full EMV standard ("Will Retailers be," 2014). Once the major card issuers have completed the transition, they will no longer be held liable for fraudulent transactions if a new chip card is used on a legacy terminal.

The liability shift for fraudulent transactions was one of the driving forces behind the shift to the EMV standard. MasterCard's Carolyn Balfany explained how the liability shift will work to representatives of the Wall Street Journal. According to Balfany the transition to EMV cards places the liability for fraud onto the party with the lowest technology. That means if a merchant does not have the equipment to process an EMV card transaction the merchant would be liable for any fraud that occurred as a result of that POS terminal.

Ms. Balfany also made it clear that if the bank fails to issue EMV cards, leaving clients with traditional swipe-and-sign cards, then the bank would responsible for any fraud ("Preparing for," 2014). Table 3 depicts key dates, retailer incentives and liability shifts that have or will occur as a result of the U.S. transition to the EMV standard ("Will Retailers be," n.d.). Further the figure shows the major card brands have aligned and streamlined key milestones in an attempt to facilitate the EMV migration. The table covers topics and milestones such as the PCI Audit Relief. For Visa and MasterCard PCI Audit Relief occurs if 75% of retailer major payment card transactions originate from EMV-compliant terminals that support both contact and contactless transactions. If this is true, the retailer is relieved of audit requirements for PCI. However, the retailer is still required to be PCI compliant (Medich, n.d.).

Table 3

EMV Fraud Liability Implementation Matrix Timeline.

EMV Deployment Milestones	Key Dates	Visa	MasterCard	Discover	American Express
PCI Audit Relief	October, 2012	Y	Y	N	N
	October 2013			Y	Y
PCI Account Data Compromise Relief					
75%-50%	October, 2013	N	Y	N	N
95%-100%	October, 2015	N	Y	N	N
Acquirer/ Sub-processor Compliance	April, 2013	Y	Y	Y	Y
Counterfeit Liability Shift (excluding fuel dispensers)	October, 2015	Y	Y	Y	Y
ATM Counterfeit Liability Shift	April, 2013	N	Y – cross border Maestro	tba	N
	October, 2016	N	Y – all MasterCard-branded products	tba	N
Lost or Stolen Liability Shift	October, 2015	N	Y	Y	N
Counterfeit Liability Shift for Automated Fuel Dispensers	October, 2017	Y	Y	Y	Y
Lost and Stolen Liability Shift for Automated Fuel Dispensers	October, 2017	N	Y	Y	N

Note: Reprinted from Will retailers be ready for EMV by Oct 2015, by payments leader, 2013, Retrieved from http://www.paymentsleader.com/will-retailers-be-ready-for-emv-by-oct-2015/, Copyright, 2013 FIS and/or its subsidiaries.

Discussion of the Findings

The purpose of this research was to compare the security standards of credit and debit card systems of the United States (U.S.) to that of the United Kingdom (U.K.). What are the predominant credit and debit card technologies and standards in use today? What lessons can be learned from the Europay, Mastercard and Visa (EMV) standard used in the United Kingdom? Why has the United States been slow to adopt the integrated chip and pin technology?

Technologies and Standards.

The legacy magnetic stripe payment card needs to be phased out and eliminated completely. The technology and standards are dated and represent more of a risk to consumers and the payment card industry as opposed to providing a convenient service. The U.S. represented the last bastion of use for the legacy magnetic stripe payment card standard. However, the rising cost of fraud has signaled the end to this dated standard and its supporting technologies. As of 2012, a Nilson report suggests the U.S. accounts for 47.3% of payment card fraud (Heggestuen, 2014). How can one of the world's most technologically advanced nations be the victim of such record breaking fraud losses? One need only look at events in recent history, and the legacy magnetic stripe standards still in use in the U.S. for potential answers.

United States retailer, Target had its computer network hacked, and subsequently consumer credit and debit card information was stolen by the hackers. ABC News reports the Target breach is said to be the second-largest retail cyber-attack in history (Zimmerman, 2014). Winchester of Data Science Central reported the attackers targeted the data stored on the magnetic strips of customers' cards (Winchester, 2014). The Target data breach exposed the credit card, debit card and personally identifiable information (PII) of 40 million of Target's customers (Krebs, 2014).

The Target data breach was not an isolated incident, it was merely one of the most high profile data breaches and highlighted the need to phase out the legacy magnetic stripe payment card and technology. The magnetic stripe technology that has been the primary technology in use in the United States credit card industry is four decades old. The concept of how payments are made and accepted has not changed. There are two main stages in payment card transactions. Those stages are the authorization and settlement. Authorization is the more vulnerable of the stages as it requires sending sensitive authentication data. Unfortunately, the data is often transmitted unencrypted via multiple systems. The static poorly secured information contained on magnetic stripe cards is vulnerable to interception by hackers. Once intercepted the hackers can then use the harvested information to produce counterfeit cards.

Although the magnetic stripe standards were the first to be adopted globally, there was little forethought with respect to technological and security enhancements. Today's magnetic stripe credit cards are a result of an IBM Engineer's desire to combine a strip of magnetized tape with a plastic identity card. IBM Engineer, Mr. Forrest Parry was working on the magnetic stripe embossed identity card for the CIA. He had a difficult time going from the concept to reality. While discussing his project with his wife who happened to be ironing, the Engineer's wife suggested ironing the magnetic strip onto the plastic card. Taking the advice from his wife, Engineer Parry did just that, and it was then magnetic strip technology was born. Mr. Parry and IBM were the pioneers of the modern plastic credit card ("Magnetic Stripe Technology," n.d.).

The beginning of the modern payment card is an interesting story. However, it also illustrates that card security was not native to the card's design. In the 1960s fraud was not as prevalent and the Internet of today did not exist. Therefore, little to no thought was given to making the card secure, or how the physical medium could be upgrade in the future. A lack of vision is part of the reason why the same poorly secured three track magnetic stripe card that Engineer Parry designed is still in use today.

Though the banks and credit card issuers are not the solely to blame for the billions of dollars lost to credit card fraud, they are certainly complicit. When the credit and debit card industry consider fraud loses to be acceptable because they total less than the cost of changing an archaic legacy system they are culpable for the rising payment card fraud numbers.

There is no denying the role that the first credit card standard played in making credit cards and credit card systems what they are today. However, many security and technology advancements happen in forty years. Unfortunately, magnetic stripe cards and their standards where not managed appropriately and as a result must be phased out entirely.

"In 2009, payment card fraud losses in the United States totaled an estimated $3.4 billion" as reported by the Federal Reserve Bank of Kansas (Sullivan, 2013, p. 32). As of 2013, U.S. card fraud numbers continue to rise. According to a 2013 Business Insider report, payment card fraud in the U.S. grew by 29% to $7.1 billion (Heggestuen, 2014). Eliminating fraud is an extremely ambitious goal and may not be realistic. However, thwarting and making the execution of fraud more difficult is attainable. The U.S. credit and debit card industry can help prevent fraud by instituting layers of security. Adoption of EMV is the first step in the way ahead for the United States credit and debit card industry.

The UKCARDS Association puts card fraud numbers at 388 million pounds that is the equivalent of almost 600 million dollars (UKCARDS, 2013). Although, 600 million dollars is a large sum it pales in comparison to the U.S. losses, amounting to $7.1 billion, as reported by Heggestuen of Business Insider. The Javelin Research Group estimates the cost of the U.S. EMV upgrade to be $8.65 billion. With annual fraud losses in the U.S. at $7.1 billion and expected to rise, the $8.65 billion dollar upgrade is needed. From a financial perspective, an investment in EMV technology and standards will result in significant Return On Investment (ROI) for the payment card industry.

It has been argued that chip cards, which are part of the EMV standard offer stronger defenses against fraud, but he also points out they certainly will not put an end to it (Sullivan, 2013). Recent analysis of instances of fraud since the implementation of EMV in the U.K.

support Sullivan's assertion. The United Kingdom's use of EMV has resulted in a significant drop in card present fraud. Card present fraud, has dropped by 64% since EMV was introduced in 2003 (Ray, 2013). Although EMV seems to combat card present fraud, it does not adequately address IMOTO fraud.

A 2013 LexisNexis annual fraud report EMV suggests EMV may prove to be a double-edged sword with respect to addressing and preventing retail fraud. The report details one of EMV's flaws. EMV does a great job of protecting users at the POS with highly secure "chip-and-PIN" authentication ("True Cost," p. 6, 2013). However, in order to be effective the physical card must be present in for this technology to be utilized. The LexisNexis report predicts EMV implementation in the U.S. will follow trends seen in the U.K. and Canada deployments of EMV. According to LexisNexis, "Based on the experiences of merchants and issuers in the U.K. and Canada, POS fraud is likely to decrease while CNP fraud skyrockets after EMV is widely adopted in the U.S" ("True Cost," p. 6, 2013).

In addition to being ineffective for IMOTO transactions, EMV standards still have to contend with vulnerabilities such as PIN harvesting, the no PIN attack and the inherent vulnerability of the included magnetic stripe. The U.S. implementation of the EMV standard will also have to contend with signature based EMV chip cards. Signature based EMV cards introduce the vulnerability of human error. "There is little likelihood that a $9-per-hour checkout clerk is going to bat an eyelash at a thief who signs your name when using your stolen card to buy stuff at retailers" (Krebs, p.1, 2014).

Signature based compromises are not the only concern for the U.S. implementation of the EMV standards which will be a combination of signature and PIN. Compromised PINs represent another potential issue. Once EMV is implemented in the U.S., hackers will undoubtedly improve their PIN harvesting techniques and solutions. Payment card fraud represents a significant source of income for fraudsters. Therefore, designing, and implementing more sophisticated skimming and harvesting technologies and schemes are just costs associated with conducting the lucrative fraud business.

Time is not on the side of the U.S. payment card industry. The international community has spoken via their widespread adoption of the EMV standard. The PCI can no longer rely on one of the best fraud protection systems in place as a way to prolong the adoption of EMV ("EMV: America," 2014). The use of online, real-time authentication used in the U.S. is credited for the low fraud numbers. Real time authentication was made possible because the U.S. has one of the most developed and robust telecommunication networks in the world (Sullivan, 2013). Real-time authentication helps combat payment fraud at the POS terminal, which payments leader states is the best place to stop fraud ("EMV: America," 2014). However, as the last bastion of magnetic stripe use in North America it is merely a matter of time until fraudsters overwhelm the real time fraud protection services.

As fraud protection services fail the cost of fraud will increase. At that juncture it would no longer be cost effective for the U.S. payment card industry to maintain the status quo. Increase fraud cost would reduce profits and eclipse the cost of the upgrade to EMV. Additionally, with the magnetic stripe standards banks and card issuers were able to redirect fraud costs to the retailers and consumers. Therefore, card issuers had little incentive to upgrade from the magnetic stripe. With EMV standards retailers will be able to push the cost of fraud back to the card issuers and banks (Jones, 2011). That would mean even lower payment card revenue for the banks and card issuers. From a financial perspective, it makes sense for the U.S. payment card industry to make the shift to the less vulnerable EMV standards.

Regardless of the vulnerabilities inherent in the EMV standards and technology, EMV is a more secure standard than the legacy magnetic stripe. EMV implemented correctly should begin to reduce the rising cost of card present fraud. However, Avivah Litan, a fraud analyst with Gartner Inc has seen recent fraudulent transactions that resulted from improper EMV rollouts (Krebs, 2014). Litan has seen considerable confusion with respect to proper configuration of EMV roll outs. She attributed the confusion to the complexity of a properly configured EMV roll-out.

Litan has also brought attention to another unintended consequence of EMV. That consequence is a false sense of security and feeling that EMV will address all the issues that are currently associated with fraudulent transactions. As a result of those false senses of security about EMV, Litan has seen banks loosen their other fraud measures once they believe they have the EMV standards implemented. The banking institutions release other fraud protection measures without validating their EMV standards (Krebs, 2014).

The implementation of EMV in the U.K. and other international regions provide some valuable lessons that the U.S. can benefit from. One of the most important lessons is the case of the Netherlands and their slow adoption of EMV. The Netherlands payment card industry did not adopt EMV when neighboring European countries did. As a result fraud numbers in the Netherlands increased from 1.5 % in 2005 to 5% in 2009 ("EMV in the USA," 2012). That represents a 300% increase in the rate of payment card fraud. It is time for the U.S. to effectively and efficiently adopt the new EMV standard because neighboring countries like Canada and Mexico now support the standard.

EMV adoption is a complex, staged and methodical process (Ray, 2013). In order to be successful the chip card must be distributed to customers. Customers need to be taught what

EMV is, how it works, and what it can and cannot do. Banks and retailers must install and maintain EMV complaint systems and POS devices. EMV compliant devices must be configured correctly. Fraud protection should not be removed because EMV complaint systems devices are installed. The systems and devices need to be tested at length before a decision is made about removing additional fraud protections safeguards.

In order for the United States payment card industry to realize effective fraud controls with the EMV standards, they have to be implemented correctly. Additionally, the payment card industry has to educate retailers, and consumers on what the standards are and how they work. Fraud affects consumers differently than it does a retail business, bank and or card issuer. At times, consumers endure significant and lasting effects such as lost money, poor credit scores and job loss as a result of payment card fraud (Anderson, 2012). Therefore, consumers need to know what EMV is, how it is supposed to protect them and what recourse they have in the event they are the victim of fraud in the EMV ecosystem.

EMV is not the silver bullet that will eradicate payment card fraud. However, EMV is a good first step toward mitigating the increasing costs associated with fraudulent payment card transactions. Although a good first step, the architects of EMV must realize that is also a dated standard which means fraudsters understand the technology.

Apple Pay is yet another step in the right direction on the path to thwarting payment card fraud. However, Yellow Path verification standards need to be improved and enforced. Now that Apple has released the Yellow Path specifications it is up to the banks to educate their customers and enforce the standard. If full social security numbers (SSN) are required to authenticate customers as part of the Yellow Path verification then banks should put that information out to their customers. Most people are leery of providing their full SSN’s. However, if they understand the reasoning behind the request, they are more apt to comply with the customer service representative's request if they are educated ahead of time.

Yellow Path is not the only issue that Apple has to contend with. Adoption of Apple Pay is being slowed by lack of infrastructure. Apple Pay got off to a banner start as it attracted 11% of all credit card using households. It also converted 66% of iPhone users within the first four months of its October 2014 debut. These numbers are the result of an ongoing study being conducted by firm Phoenix Marketing International of more than 3,000 credit card users (Neagle, 2015).

The survey numbers show the interest in Apple Pay is there. However, customer enthusiasm is not the problem for Apple. Apple lacks the retailer infrastructure to interact with and accept payments from Apple Pay enabled devices. Unfortunately for Apple lack of retailer support is a tow pronged problem. There are retailers who are equipped to support Apple Pay but their staff is not trained on Apple Pay, equipment has either not worked and or took too long to process transactions (Neagle, 2015).

The other issue for Apple is Apple Pay generates revenue for Apple. How is that a problem? Retailers want a piece of the NFC mobile payment revenue pie. The Merchant Customer Exchange (MCX) is marketed as the only merchant-owned mobile business network built to simplify the customer shopping experience across all major shopping verticals ("Merchant Customer," n.d.). MCX is made up of companies such as but not limited to CVS, RiteAid, 7-11, Dunkin Donuts, Lowes and ExxonMobile are boycotting Apple Pay. The MCX is boycotting Apple Pay and developing CurrentC, their own mobile payment technology (Neagle, 2015).

Apple not only has to deal with mitigating the physical limitations of Apple Pay, such as the fact that it only works on Apple devices. Apple Pay will not work if the device's battery is depleted, or the phone is damaged. It also has to contend with limited infrastructure, CurrentC and other NFC based mobile payment systems such as Google Wallet. Those are a few of the potential limitations to widespread adoption of Apple Pay. Regardless of the challenges used in conjunction with other effective fraud control measures such as EMV, Apple Pay will make a difference in loses associated with payment card fraud.

Future Research and Recommendations

Credit card-carrying residents of the United States have unwittingly played the role of targets of opportunity. Cyber criminals and other nefarious individuals choose to exploit United States credit card holders because of the more lax security standards utilized by United States payment card industry. United States credit card holders have been targets of opportunity because magnetic strips are less secure and more easily compromised than the chip technology cards (Fahey, 2013).

The United States banking and credit card industry is now taking steps to improve the outdated magnetic strip technology by introducing the decade old chip technology used in the United Kingdom. Chip and pin technology is considered more secure because it requires the cardholder to utilize four-digit pins that correspond to the information contained on a computer chip embedded in the card. Thanks to NFC technology Apple has introduced Apple Pay as yet another way to make secure payments via tokenization of payment card PANs.

EMV and Apple Pay are steps in the right. Those technologies and standards take payment card processing out of the 1960s. EMV and Apple Pay provide more secure ways to perform payment card transactions. However, they both still rely on the physical medium that was first developed in the 1960s.

Credit card security has to be an evolutionary process. It must change with the times. The companies vying for consumer payment card business need to do a better protecting the consumer. For far too long the payment card industry believed the tangible financial losses associated with fraud were an acceptable risk because of the insurance and other protections afforded to them. Unfortunately, the intangible losses that consumers suffer cannot be quantified.

With the October 2015 EMV implementation deadline looming, it is doubtful that the U.S. retail industry will be in complete compliance by October. During January 2015, ACI Worldwide conducted a survey of 200 retail industry professionals during the National Retail Federation's Annual Convention and Expo in New York. The survey gaged EMV preparedness and looked for feedback on emerging technology trends. The survey results concluded but are not limited to the following:

- EMV readiness—Of the 200 survey respondents almost ¼ of participants are not fully prepared for the EMV migration. Based on responses from 55% of the respondents, 14% are still working on compliance, 19% are not prepared and 22% are still weighing their options ("Retailers not ready," 2015).
- Breaches and payments security—59% of respondents cited costs associated with 2014 data breaches as reasons for limiting their investment in payment in security initiatives. 39% indicated they have already raised investments in payment security. While 20% have taken no action but plan to increase investment in payment security over the next 12-24 months ("Retailers not ready," 2015).

- Mobile wallet war—Apple emerged as the dominant mobile payment technology garnering 47% of respondent votes. Google Wallet followed with 21% and PayPal rounded out the field at 15% ("Retailers not ready," 2015).

Further research needs to be conducted to discern retailer preparedness throughout the EMV adoption process. In April 2015, indications are retailers and subsequently consumers will not experience the full benefit of EMV with respect to card present transactions. As a result of the lack of EMV preparedness fraudsters still have significant fodder in the U.S. payment card ecosystem.

Additionally, the U.S. adoption of the EMV standards will provide valuable lessons learned and may affect the future of the EMV standards. The U.S. adoption of EMV is unique in that it will support both the chip and PIN as well as the signature based chip cards. As a result of the magnitude of this adoption of EMV it represents a good benchmark test. Will chip and PIN prove to be more effective against fraud protection that signature based chip cards?

With attackers honing their craft each day in large numbers and sharing their methods through the Internet costing the consumers and industries billions of dollars each year, the need to increase security at all levels of the financial transaction is necessary. With this in mind, how do credit card companies improve upon the current technologies to increase this security?

As discussed, each of the current technologies is useful and some provide better security benefits than others. EMV offers both contact and contactless cards. Both the contact and contactless cards encrypt the data stored on the card, magnetic stripe was widely used throughout the world, and NFC uses a proximity method to ease the use. While they each have their benefit, they also introduce weaknesses to the transaction process.

Improvements upon current technology are already in progress to include biometrics such as fingerprint scanning, retinal scanning, facial recognition, or voice recognition. Banking and credit card issuing institutions such as the United Services Automobile Association (USAA) and American Express already make effective use of biometrics in their mobile applications. USAA allows members to access the mobile banking app via facial, voice, or fingerprint recognition. To date, the American Express mobile app affords users access via fingerprint scan.

The overall implementation biometric methods would reduce the risk of fraud at the point of sale to include physical location POS and online purchases. The payment card industry needs to take customer security more seriously. The increased use of smart phones will improve the ability to secure these transactions with biometrics by using smart phone fingerprint readers and cameras. In addition, smart phone functionality will assist in moving credit card transactions to use random key generators such as Rivest-Shamir-Adleman (RSA) tokens, which create random pins that refresh each minute. According to Tech Target, “RSA is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet” (Rouse, p.1, 2104). Online game companies such as Blizzard are already using these random number generators to authenticate users when using new systems or making purchases through their online stores.

Like Blizzards others need to follow their lead and use random card number utilities. Each level of validation used in the transaction will increase the security of the process; it will also increase the time to finalize the transaction. A complete solution for credit card security will have to balance the fine line of convenience for the consumer and security for the industry. Addressed in the security model of electronic transactions are how to best handle confidentiality, authentication, integrity, nonrepudiation of origin, and nonrepudiation of receipt. Security is an evolutionary process that needs to be reviewed and improved consistently to ensure the "would be" attackers are deterred from stealing the information of consumers.

Why are retail payment transactions still tied to a physical piece of plastic? The reliance on the physical card seems to be one of the weakest links in the machinery of the retail payment industry. Why do gaming platforms like the ones offered by Blizzard seem to be more secure than credit and debit card transactions? Layered security, such as two form factor authentication would certainly add much needed protection. For example, when a consumer enters their PIN into POS device the device sends a confirmation number to the consumers' mobile device on file. The consumer then has to enter the confirmation number to complete the transaction. Apple Pay offers a level of layered protection with the tokenized PAN. Although Apple is offering viable payment card security solutions it suffers from a lack of infrastructure and is a stove piped solution.

Will Apple explore and entertain the idea of packaging Apple pay so it can be used on multiple mobile platforms? Apple will not be able to convert the general population to Apple devices. Therefore, providing Apple Pay as a service could potentially increase Apple Pay adoption and use. Doing so could derail MCX's upstart CurrentC venture.

Today it appears that technology giant Apple, American Express and banks like USAA are the leading the technological charge to advance the payment card industry and the technologies associated with it. These organizations offer biometric solutions that are convenient and offer more secure access to customer information and finances. The credit card consortium need to take the lead away from Apple, USAA and American Express or risk extinction as a result of a lack of vision.

Unless MasterCard and Visa want to go the way of famous notables such as E.F. Hutton, RCA, Compaq and TWA it would behoove them to take the lead in taking the payment card industry out of the 1960s. If SpaceX founded in 2002 can design, build and launch rockets and spacecraft into outer space; Tesla Motors founded in 2003 can build some of the most sort after electric cars on the market, why don't MasterCard and Visa offer a better alternative to the plastic credit card designed over four decades ago?

Perhaps, the answer lies in the core business of the credit card companies. Credit card companies are financial based and in the business of making money from card membership and various fees associated with the physical credit card. The major credit card companies need to take a closer look at how they safeguard their most prized asset, a loyal customer. The major card brands need to do more than settle for a standard because it is globally accepted and somewhat more secure than the current standard.

Apple is already adapting and promoting card less payment technology. However, at this juncture there are more extreme solutions being considered. Is wearable or ingestible technology the answer to providing enhanced security? The major card issuers need to be at the tip of the spear with respect to the future of payment card technologies in order to remain viable and relevant. Failure to do so could render them unfortunate case studies that future financial, security and technological academics study to determine the cause of their demise.

References

3D Secure explained. (2014). Retrieved from http://www.sagepay.co.uk/support/12/36/3d-secure-explained

Anderson, R. (2012). *Measuring the cost of cyber crime.* Retrieved from http://weis2012.econinfosec.org/papers/Anderson_WEIS2012_old.pdf

Birch, R. (2013, July 1). *Future fraud threat; analysts see card risk rising in 2015*. Retrieved from http://www.cujournal.com/

Bose, N. (2015, March 3). *Costly shift to new credit cards won't fix security issues. Reuters.* Retrieved from http://www.reuters.com/article/2015/03/03/us-usa-cybersecurity-retail-insight-idUSKBN0LZ0GC20150303

Chip terms explained. (2002). Retrieved from https://www.visa-asia.com/ap/center/merchants/productstech/includes/uploads/CTENov02.pdf

Does Apple Pay replace the plastic in your wallet? (2014, September 25). Retrieved from http://www.paymentsleader.com/does-apple-pay-replace-the-plastic-in-your-wallet/

EMV: America, what took you so long? (2014, October 13). Retrieved from http://www.paymentsleader.com/emv-america-what-took-you-so-long/

EMV in the USA: best practices and lessons learned. (2012). Retrieved from https://www.firstdata.com/downloads/thought-leadership/2756-EMV-Best-Practices-WP.pdf

EMVCo. (2015). EMVCo. Retrieved from http://www.emvco.com/about_emv.aspx

Fahey, J. (2013, December 22). *Weak U.S. card security made Target a juicy target.* Retrieved from http://www.usatoday.com/story/money/business/2013/12/22/weak-us-card-security-made-target-a-juicy-target/4165427/

Gomzin, S. (2014). Processing payment transactions. In *hacking point of sale: payment application secrets, threats, and solutions* [Safari]. Retrieved from https://www.safaribooksonline.com/library/view/hacking-point-of/9781118810071/9781118810071c01.xhtml

Heggestuen, J. (2014, March 5). *The US accounts for over half of global payment card fraud.* SAI - *Business Insider.* Retrieved from http://www.businessinsider.com/the-us-accounts-for-over-half-of-global-payment-card-fraud-sai-2014-3

Heller, M. (2015, March 3). *Amid Apple Pay fraud, banks scramble to fix Yellow Path process.* Retrieved from http://searchfinancialsecurity.techtarget.com/news/2240241612/Amid-Apple-Pay-fraud-banks-scramble-to-fix-Yellow-Path-process

Inscoe, S. (2014, June). *Global consumers: Losing confidence in the battle against fraud.* Retrieved from http://www.aciworldwide.com/-/media/files/collateral/global-consumers-losing-confidence-in-the-battle-against-fraud-report

ISO 8583-1:2003. (n.d.). Retrieved from http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=31628

ISO/IEC 7810:2003 - Identification cards -- Physical characteristics. (n.d.). Retrieved from http://www.iso.org/iso/catalogue_detail?csnumber=31432

ISO/IEC 7813:2006 - Information technology -- Identification cards -- Financial transaction cards. (n.d.). Retrieved from http://www.iso.org/iso/catalogue_detail.htm?csnumber=43317

J.P. Morgan. (2014). *2014 AFP payments fraud and control survey.* Retrieved from https://www.jpmorgan.com/cm/BlobServer/2014_AFP_Payments_Fraud_Survey.pdf?bl obkey=id&blobwhere=1320639355606&blobheader=application/pdf&blobheadername1=Cache-Control&blobheadervalue1=private&blobcol=urldata&blobtable=MungoBlobs

Knopp, J. (2013). Point-to-Point Encryption: *A merchant's path to cardholder data environment scope reduction. MasterCard.* Security Matters. Retrieved from http://arm.mastercard.com/securitymatters/compliance/pci-dss/point-point-encryption-merchants-path-cardholder-data-environment-scope-reduction/

Krebs, B. (2014, October 30). *Chip & PIN vs. Chip & Signature*. Krebs on Security. Retrieved from http://krebsonsecurity.com/2014/10/chip-pin-vs-chip-signature/

Krebs, B. (2014, February 12). *Email attack on vendor set up breach at target*. Krebs on Security. Retrieved from http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/

Kumar Choudhary, S. (n.d.). *EMV compliance in the U.S.* Retrieved from http://www.capgemini.com/resource-file-access/resource/pdf/EMV_Compliance_in_the_U.S..pdf

Landes/Forbes, L. (2013, November 6). *Credit card basics: everything you should know*. Forbes. Retrieved from http://www.forbes.com/sites/moneybuilder/2013/06/11/credit-card-basics-everything-you-should-know/

LexisNexis. (2013, September). 2013 *LexisNexis True cost of fraud study.* Retrieved from https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2013.pdf

LexisNexis. (2014, October 10). *Preparing for the transition to EMV chip cards next fall.* Retrieved from http://www.lexisnexis.com.ezproxy.utica.edu/hottopics/lnacademic/?

Magnetic Stripe Technology. (n.d.). Retrieved from http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/magnetic/

Managing Fraud with EMV. (2011). Retrieved from http://www.mastercard.com/us/company/en/docs/Managing_Fraud_With_EMV.pdf

Medich, C. (n.d.). EMV migration. *Driven by payment brand milestones*. EMV Connection. Retrieved from http://www.emv-connection.com/emv-migration-driven-by-payment-brand-milestones/

Merchant customer exchange. (n.d.). Retrieved from http://www.mcx.com/

Moody's Economy.com. (2010, January). *The positive economic impact of digital currency.* Retrieved from http://betterthancash.org/wp-content/uploads/2012/09/moodys-economy-fact-sheet-Visa.pdf

Neagle, C. (2015, March 31). *Broken NFC terminals, lack of retail support stifling Apple Pay usage.* Retrieved from http://www.networkworld.com/article/2904098/opensource-subnet/broken-nfc-terminals-lack-of-retail-support-stifling-apple-pay-usage.html

Owano, N. (2012, July 31). *Chip and pin terminals shown to harvest customer info*. Retrieved from http://phys.org/news/2012-07-chip-pin-terminals-shown-harvest.html

Poulsen, K. (2014, September 26). *The days of credit card fraud are numbered. (Wired UK).* Retrieved from http://www.wired.co.uk/news/archive/2014-09/26/credit-card-fraud

Poulsen, K. (2014, September 25). *Why the heyday of credit card fraud is almost over. WIRED*. Retrieved from http://www.wired.com/2014/09/emv/

Ray, R. (2013, July 13). *Lessons learned from UK's EMV success.* The Verifone Blog. Retrieved from http://blog.verifone.com/security-2/emv-security-2/lessons-learned-from-uks-emv-success/

Retailers not ready for EMV. (2015, February 3). Retrieved from http://www.bankingexchange.com/news-feed/item/5254-retailers-not-ready-for-emv?Itemid=101

Rouse, M. (2014, November). *What is RSA algorithm (Rivest-Shamir-Adleman)? Definition from WhatIs.com*. Retrieved from http://searchsecurity.techtarget.com/definition/RSA

Segal, L., Ngugi, B., & Mana, J. (2011). *Credit card fraud: A new perspective on tackling an intransigent problem.* Fordham Journal of Corporate & Financial Law, 16(4), 743-781 Retrieved from http://search.proquest.com/docview/910125106?accountid=28902

Steiner, S. (n.d.). *The evolution of credit cards*. Retrieved from http://www.bankrate.com/finance/financial-literacy/the-evolution-of-credit-cards-1.aspx

True cost of fraud study. (2013, September). Retrieved from https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2013.pdf

Will retailers be ready for EMV by Oct 2015? (2014, October 16). Retrieved from http://www.paymentsleader.com/will-retailers-be-ready-for-emv-by-oct-2015/

Winchester, B. (2014, July 13). *The Target security breach: What happened and what it can teach us about cyber security*. Data Science Central. Retrieved from http://www.datasciencecentral.com/profiles/blogs/the-target-security-breach-what-happened-and-what-it-can-teach-us

Wood, L. (2012, March 26). *Phones become electronic wallets*. Network World. Retrieved from http://www.networkworld.com/article/2187029/smartphones/phones-become-electronic-wallets.html

Yu, A. (2013, December 19). Outdated magnetic strips: *How U.S. credit card security lags.* All Tech Considered : *NPR.* Retrieved from http://www.npr.org/blogs/alltechconsidered/2013/12/19/255558139/outdated-magnetic-strips-how-u-s-credit-card-security-lags

Zimmerman/ABC news, S. (2014, February 13). *Could Target-style data breach happen to me?* ABC News. Retrieved from http://abcnews.go.com/Blotter/target-style-data-breach-happen/story?id=22483195