**Case Study: Is Chip Technology Really More Secure Than Swipe Technology?**

**Dayana Fernandez**

**Towson University**

**AIT 710**

**Prof. Friedman**

**December 7, 2017**

Table of Contents

I. Abstract 2

II. Introduction 2

III. Background and Related Work 3

IV. Similarities and Differences 5

V. Risks and Vulnerabilities 8

VI. Safeguards 12

VII. Impact of Identity Theft 16

VIII. Company Usage and Consumers 23

IX. Future of Credit Cards and Related Technologies 27

X. EMV Questions and Answers 29

XI. Conclusion 36

XII. Bibliography/Reference 36

### I. Abstract

This case study focuses on the comparison of credit card technologies between chip and swipe mechanisms. The main question being addressed is whether chip technology is more secure than swipe technology. Furthermore, the case study also researches identity theft associated with credit cards. Moreover, it details the vulnerabilities identified and the future direction of credit cards, as well as other technologies being used.

This case study is important because credit card use is essential for any modern economy and will only become more rampant as technology continues to be used to conduct business transactions. This case study will help clarify any misconceptions that may exist about security concerns using this technology. Literature reviews and analyses of existing studies will be used to complete this project.

## II. Introduction

This case study focuses on the comparison of credit card technologies between chip and swipe mechanisms. The main question being addressed is whether chip technology is more secure than swipe technology. This work details the similarities and difference between the two technologies, as well as providing a look into risks, vulnerabilities and safeguards. Furthermore this paper examines the impact on identity theft and company usage and what this means for consumers and how they are impacted. Moreover, the future of credit cards and related technologies is also detailed. Lastly, this paper answers common questions about EMV technology.

## III. Background and Related Work

American consumers are familiar with swipe credit card technology, in which card data is statically encoded on a magnetic stripe (magstripe) that is then run through POS systems. Typically, users must supply their swipe card and PIN or their card and a signature. The problem is that the data on these cards can be easily copied using inexpensive reader machines, allowing criminals to duplicate credit and debit cards. To address this issue, Europay, MasterCard and Visa (EMV) developed a new standard: chip cards. These cards come with an embedded micro computer chip and magstripe. The chip must be inserted into a compatible POS machine, at which time it is dynamically authenticated. First, the card is checked to ensure it is activated and hasn’t expired. Then, a set of unpredictable numbers is generated to encrypt the transmission of card data to the relevant financial institution. The bank or credit card company then authenticates the transaction and sends back an encrypted approval. The biggest benefit of chip cards is reduced fraud, since chips are much harder to duplicate and it is impossible to manually enter card numbers or use carbon-copy paper alternatives. [1]

Europay, Mastercard and Visa (EMV) use international standards to provide interoperable methods for processing credit card transactions. An EMV card is also known as a smart card, chip card or integrated circuit card (ICC). It is a plastic card with an embedded computer chip that stores information and does calculations. EMV cards are already standard in many parts of the world, and the United States is starting to catch up and requiring companies to use this standard. EMV credit cards made up only 10% of the market in 2014 but are projected to reach 95% by 2018. Also the number of EMV-capable terminals is projected to grow to more than 90% in the United States by 2018. The migration to EMV is an industry-wide effort involving card issuers, merchants, card processors, merchant acquirers, and payment networks. [2]

EMV is the latest weapon to combat identity theft in the United States, but according to the Federal Bureau of Investigation, chip card technology is vulnerable, and a transaction security expert added that the new cards would not do very much to stop billions of dollars of credit card fraud over the next few years. “With technology advances and the significant increase in data breaches and identity theft from computer intrusions, we continue to see significant increases in credit card theft/fraud,” a representative from the Federal Bureau of Investigation’s Criminal Investigative Division Financial Crime Section told The Washington Times. “The new EMV chip cards were designed to help curtail credit card fraud; however, there are still vulnerabilities with these cards.” [3]

Both types of cards come with fraud-prevention technology — embedded chips that assign unique IDs to each individual transaction, making cloning almost impossible. The credit card must be physically present when making in-store purchases. Both allow the shopper to insert his or her own card into the terminal — instead of having the cashier swipe the plastic on behalf of the customer (this may require some additional employee training. Both types of cards are readable by the majority of EMV machines, although some EMV terminals only accept chip-and-PIN cards. Both usually come with magnetic strips on the back — in addition to embedded chips on the front. However, these “magstripes” are slowly being phased out and both types of cards are becoming increasingly mandatory worldwide. [4]

With chip-and-signature credit cards, customers must sign their name on the receipt in order to complete the transaction. This step is identical to the swipe-and-sign process normally associated with older, magnetic credit cards. With chip-and-PIN credit cards, customers must key in a personal identification number (PIN) to authorize payment. Anyone can theoretically forge a signature, but without this unique code, the transaction cannot move forward. So while both types of credit cards offer added protection, the chip-and-PIN option is arguably more secure. After adopting chip-and-PIN credit cards back in 2004, the United Kingdom saw fraudulent losses plummet from $356 million a year to fewer than $100 million just four years later. [4]

## IV. Similarities and Differences

Most people are accustomed to magnetic stripe cards. They’ve been used for decades, but these cards are very simple and full of security risks. Magnetic stripe use the same technology used to put music on cassette tapes, which means that data on the card can only be updated once, which means the card is very easy to copy or counterfeit. Stealing credit card data from magnetic stripe cards is easy and extremely common, as thieves only have to swipe the card in order to steal it. [5]

EMV cards feature a small metal square on the front of the card. This square is a contact plate, which connects to a small microprocessor chip with an RFID (Radio Frequency Identification) tag. When the contact plate touches an EMV compatible reader, the reader transfers power to the card, allowing the microprocessor to communicate data, including accessing bank information, making payments, checking a balance, or making a purchase. In some cases, this will also include an NFC (Near Frequency Communication) chip, which allows for contactless payment. More importantly, because the chip communicates with the bank, it can more easily verify that the card is legitimate, preventing easy copying and reproduction of the card. [5]

EMV cards offer a number of advantages over magnetic stripe cards including security, speed, and point-to-point encryption. Security Protocols – EMV chip cards store security protocols, which protect data from theft. The most important of these protocols is the creation of unique transaction codes that are only valid once. This means that the common technique of stealing data using a card skimmer in an ATM or fake ATM does not work, because transaction data only works for that purchase. This process is known as Dynamic Data Authentication (DDA), which uses paired authentication keys for every transaction. Because this data is on the card and never shared, a hacker can never steal it. [5]

P2PE –  EMV cards use P2PE, or Point-to-point encryption, which is a PCI-certified form of end-to-end encryption (also known as E2EE). Data is encrypted as it enters the Point of Sale terminal and decrypted by the payment processor. This reduces cybersecurity risks for business owners, because in the event of a breach, any data that is stolen by hackers will be encrypted and difficult to use. Pin – While Magstripe relies on the consumer’s signature to verify identity, EMV cards often use a pin code which is more difficult to emulate, and prevents the card from being used if it is not correct. Chip and signature cards are also popular, but are less secure. [5]

Tokenization – In some cases, chip and pin cards also use tokenization, or two-step identification, for online purchases. This reduces the risk of data being stolen online, and ensures that stolen data is less usable. Speed – RFID is about 53% faster than Magstripe, allowing you to process payments more quickly. Overall, EMV offers significant advantages over Magstripe in that it is more difficult to steal data, and more difficult to use data when breaches do occur. In October 2016, a year after integration began, merchants saw a 43-54% reduction in counterfeit fraud costs, thanks to the difficulty of stealing chip cards. Because more than 70% of all credit card fraud involves counterfeit cards, and MasterCard has historically seen a 77% increase in fraud year over year, this drop is unprecedented. [5]

While EMV cards offer more data security and reduce the risk of fraud, many small business owners do have concerns over integration. New Readers – The primary concern for many small businesses is the cost of integration. You must invest in new Point of Sale devices or readers to become EMV compliant and, for a small business with a tight budget, this can be daunting. However, readers are a relatively low-cost investment, typically starting in the double digits. For more complex, integrated systems, the cost can range in the thousands of dollars. [5]

Testing and Certification – Integrating EMV means meeting standards, which requires testing. EMV certification includes three levels of testing, the first two of which are typically performed by the Point of Sale or reader manufacturer. The third will be the business owner’s financial responsibility and requires that the Point of Sale be tested for every type of purchase and security issue. This approval can take 4 to 8 weeks, and will likely cost $500 or more. However, the process can be sped up using the U.S. EMV VAR Qualification Program, which helps pre-qualify businesses before getting started with the certification program. [5]

Liability Shift – The primary concern for small business owners should be the cost of not having EMV, rather than the costs involved with integrating it. In fact, by not integrating EMV technology, businesses are at risk, and can be held liable for card fraud. While the impact of stolen funds typically falls on the payment processor, changes implemented on October 1, 2015, make the least EMV-compliant party liable for the fraudulent transaction. This means that if someone with an EMV card uses it and data is stolen through magnetic stripe because the business is not EMV compliant, the business owner is liable for the stolen funds. While this liability shift is important, many retailers remain unaware of it, and continue to maintain magnetic stripe-only point of sale systems. Importantly, businesses are not liable for any fraud relating to online purchases. [5]

The Payments Security Task Force estimates that 98% of all cards in the United States will be chip enabled by the end of 2018. This makes EMV integration even more important, as cards with dual Magstripe and chip and pin capabilities are now being phased out as well. By not integrating EMV, businesses also reduce the security of Point of Sale transactions. [5]

The new chip is intended to make in-person purchases safer, and, in a matter of seconds, works as follows: During each transaction, the chip creates a one-time code. The payment terminal then sends the code to the bank over a network like Visa or MasterCard. The bank matches it to an identical one-time code and sends verification back to the terminal. [6] EMV cards are primarily designed to prevent fraudulent transactions that take place when someone physically swipes a counterfeit card at a payment terminal. Chip card technology has been proven to work because in countries that have adopted EMV as the standard, certain types of credit card fraud have dramatically declined. [7]

Chip cards are really hard to clone because magnetic-stripe cards are magnetized. When you swipe them, the payment processor reads their magnetic fields and matches them to your bank account information. The problem with this is that the data is static, making it easier for fraudsters to lift your information and clone it onto a new card. In fact, there’s something called a skimmer — which they can get or make for as little as $20 — that can do this pretty easily. [7]

On the other hand, the data on chip cards is constantly changing, making it extremely hard to isolate and extract. To rip it off, someone would have to get into the physical chip circuit and manipulate things to get bank information. Not only is this level of data surgery really difficult, but it also requires a set of high-tech equipment that can cost north of $1 million. [7]

Chip and Pin credit cards have sophisticated encryption. Magnetic-stripe cards broadcast bank information into the payment terminal as-is. Square Reader and Stand keep this information safe by encrypting it as soon as it is received. Chip cards are different in that they have sophisticated encryption built right into the chip. When a chip card is dipped (it’s a dip instead of a swipe), it talks back and forth with the payment terminal in a secret language to make sure it’s actually the card owner who is paying. [7]

## V. Risks and Vulnerabilities

In an effort to align with global POS technologies and improve [security](http://www.ibm.com/security/?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US), MasterCard and Visa had set an October 2015 deadline for what they termed a “liability shift,” according to the [Wall Street Journal](http://blogs.wsj.com/corporate-intelligence/2014/02/06/october-2015-the-end-of-the-swipe-and-sign-credit-card/). Both companies have put their full support behind [EMV technology](https://securityintelligence.com/emv-chip-cards-a-better-way-to-pay-and-fight-fraud/) in the United States, and liability for fraud was shifted to whichever party — merchant or financial institution — used less secure technology. Thus, if merchants had chip capabilities but banks did not issue chip cards, banks bear the cost. If merchants choose swipe-and-sign chip cards, they’re liable if fraud occurs. The idea here is to compel both banks and retailers to adopt chip cards at the same time and significantly reduce total [credit card fraud](https://securityintelligence.com/synthetic-identity-theft-three-ways-synthetic-identities-are-created/). [1]

However, as discussed by [GeekWire](http://www.geekwire.com/2015/why-critics-call-the-imminent-credit-card-chip-system-in-the-u-s-a-joke/), there is a loophole. While chip cards fall under the new rules, the choice to go chip-and-PIN or chip-and-sign is left up to merchants. Mike Cook, assistant treasurer of Wal-Mart, put it bluntly when he said, “The fact that we didn’t go to PIN is such a joke.” The reason being that signatures are much easier to fake than PINs since they are rarely checked for accuracy. This means a chip card is no defense in the case of a lost or stolen wallet since criminals could simply insert the chip, scribble a signature and be on their way. [1]

There are concerns that chip card technology may not be entirely secure and cannot completely eliminate fraud. In the United Kingdom, for example, EMV was fully adopted in 2006. Counterfeit card fraud is down significantly, but card-not-present fraud, which occurs during online or telephone transactions, is on the rise. According to The Hacker News, chip cards also have several inherent vulnerabilities. First, researchers have been able to predict the pattern of supposedly unpredictable numbers, allowing them to duplicate chip cards and eliminate the ability of banks to detect fraudulent transactions. Security researchers also found a way to perform man-in-the-middle attacks on chip cards by compromising the sub process, which determines the authentication required by a POS terminal. The result is the ability to bypass PIN or signature requirements altogether. Finally, Wired reports that a British team found flaws in some “contactless” Visa chip cards, which allowed the approval of foreign currency transactions up to $999,999.99. [1]

Still, the retail industry and some consumer advocates say that banks and payment networks could do more to prevent fraud. Having a chip and a four-digit pin, as many European merchants are accustomed to, would help validate both the card and the person using it. Most of the new chip cards in the United States will require only a signature. “In security, it’s what you have plus something you know,” said James Wester, a research director with IDC Financial Insights. [6]

In the United States, thieves use fake cards more often than stolen cards, according to data from the Boston-based consulting firm Aite Group. Counterfeit cards make up about 37 percent of all fraud, according to a report from Aite last year, compared with 14 percent for lost or stolen cards. But chip technology will not help with “card not present” fraud, such as online purchases. It also will not help with the kinds of data breaches that have embroiled retailers like Target and Home Depot. [6]

US EMV credit cards are definitely an upgrade over their magstripe counterparts. The US chip-enabled credit cards use a strategy called “Chip and signature,” meaning a pin code is not needed to finish a transaction. Another potential security risk is that if a local store doesn’t have a point of sale that’s chip enabled (meaning there’s no slot for a credit card to be dipped), then the magnetic stripe on the back of the card needs to be used and the chip isn’t activated, which means there is no extra security from the chip. [7]

Weaknesses in the EMV protocol and implementations create vulnerabilities that could be exploited via POS malware and man-in-the-middle attacks. More than one year after receiving warnings from security researchers that there are serious flaws in the EMV protocol used to authenticate credit and debit card transactions in 80 countries around the world, card issuers and ATM manufacturers have failed to patch all related flaws. Cambridge University computer security researchers sounded the warning in a presentation at the IEEE Symposium on Privacy and Security in San Jose, California, in which they detailed two major problems with the EuroPay, MasterCard, and Visa (EMV) standard now used to secure more than 1.6 billion cards worldwide. The researchers said they began exploring EMV security, often referred to as chip and PIN -- "in layman's terms, the chip protects against card counterfeiting, and the PIN against stolen card abuse.” [8]

Reviewing the unpredictable number, however, the researchers found that it was, in fact, often predictable. "Some EMV implementers have merely used counters, timestamps or home-grown algorithms to supply this nonce," they said. "This exposes them to a 'pre-play' attack, which is indistinguishable from card cloning from the standpoint of the logs available to the card-issuing bank, and can be carried out even if it is impossible to clone a card physically." In some cases, obtaining a legitimate ATM nonce on which to base an attack would also be easy. According to the researchers, for example, the UN is printed on all receipts generated in Italy. [8]

Digging further, the researchers also spotted a deeper flaw in the protocol that attackers could use to compromise transactions, even when an ATM generated a cryptographically strong random number. That flaw is due to the ability of attackers to intercept the unpredictable number via a man-in-the-middle attack and replace it with a different pre-computed one, which would likely pass muster with the authorizing bank. Such an attack could be executed via malware installed on POS devices, even if those devices include tamper-resistant EMV modules. [8]

To date, some of the random-number-generator flaws spotted by the researchers have now been patched. But the EMV alliance has yet to address the deeper flaw in the protocol itself. "The banks appear to have ignored this, perhaps reasoning that it is difficult to scale up an attack that involves access to specific physical cards and also the installation of malware or wiretaps on specific terminals," the researchers said. "We disagree. The Target compromise shows that criminals can deploy malware on merchant terminals widely and exploit it to earn serious money." [8]

The researchers added that they know of at least one "likely case" of a related skimming attack in the wild, and warned that "the spread of ATM and POS malware is making it ever more of a threat." In the wake of the Target breach, which occurred after attackers managed to sneak malware onto millions of Target's point-of-sale (POS) systems and steal data pertaining to 40 million credit and debit cards, many card brands and retailers, including Target, announced that they will push for more widespread EMV adoption in the US. To be clear, however, EMV would not have prevented the Target breach. Furthermore, a forthcoming liability shift by Visa seeks to drive more EMV uptake. "The liability shift encourages chip transactions because any chip-on-chip transaction -- i.e., a chip card read by a chip terminal -- provides dynamic authentication data, which helps to better protect all parties," Visa explained. [8]

According to the new research, however, that dynamic authentication system is vulnerable to spoofing. Any related liability, however, would rest with the consumer, unless he or she can prove that attackers subverted the EMV security system. Researchers expressed frustration at the EMV alliance failing to address the flaws they exposed more than one year after receiving related security disclosures. "We are now publishing the results of our research so that customers whose claims for refund have been wrongly denied have the evidence to pursue them, and so that the crypto, security, and bank regulation communities can learn related lessons," the researchers said. They've also called on banking regulators in the United States and abroad to use their muscle to force merchants, banks, and vendors to put related fixes in place. Furthermore, the researchers called on the payment card industry to take responsibility for keeping the EMV system secure. [8]

## VI. Safeguards

Safeguards are important to keep in mind when using cards. No. 1: Do not choose auto-reload. Some merchants offer a feature called auto-reload that allows you to link a gift card or online or app shopping account to a credit card or debit card. When money on that gift card or in that shopping account drops below a pre-selected limit, new funds are automatically added and charged to the linked payment card. Therefore, a thief who hacks you could repeatedly reload the gift card or shopping account and shop until your card is maxed out or your debit card hits zero, says Paul Stephens, director of policy and advocacy for the Privacy Rights Clearinghouse. With auto-reload, you are giving up some security in order to have greater convenience, says John Breyault, vice president of public policy for the National Consumers League. To protect yourself, do not choose auto-reload. If you already have it activated, disable it. If you insist on keeping it, ask some questions: Does the merchant institute auto-reload limits, such as limiting the overall number of transactions allowed, the number of transactions that can be made within a given time period and the dollar amounts that can be charged? If you turn auto-reload off, can anyone who accesses your shopping account simply switch it back on? What is the company's policy and track record with auto-reload fraud? [9]

No. 2: Keep passwords fresh, complex. When you register at a site, do not recycle a username and password from another account, says Breyault. If you do use the same info for multiple sites, a person who hacks you will have the "keys" to other online accounts. Criminals buy and trade names and passwords, then try them at various popular sites, says Ben Johnson, chief security strategist for Bit9 + Carbon Black, a tech security firm. Another important way to protect yourself is to use passwords that are lengthy. "I wouldn't use anything less than a six- or eight-digit password," says Breyault. Skip the easy-to-remember combos like "1234" or "password." Also avoid using details that are easy to guess, such as your birthday, or a favorite pet or college team name. Instead, opt for a string of seemingly unrelated letters and numbers, says Breyault. One cheap but memorable solution: Use the first letters of a book title, song lyric or favorite quote, with a few numbers and capital letters thrown in. You can also employ technology and buy a password manager, says JD Sherry, CEO of Cavirin Systems, which handles security and compliance for cloud and data centers. "I don't even know my passwords, they're so complex," Sherry says. And, for the love of security, change those passwords once in a while. Johnson says experts generally recommend switching every 90 days. However, most consumers can get by with every six months, every year, or when there's a problem with a site or app, he adds. [9]

No. 3: Investigate security first. Anytime consumers consider storing card information on a site or in an app, they "should at least think about it in the same terms that they would to protect their bank account," says Eddie Schwartz, chair of the cybersecurity task force for the Information Systems Audit and Control Association, and president and chief operating officer of WhiteOps, a company that specializes in digital fraud protection. Johnson agrees: "If you're not comfortable or can't figure out how they're protecting your data and your account, you've got to walk," he says. Look for protective features, such as: Lockouts. This feature prevents people from accessing your account if they log in from a different device. It also locks a person out after a certain number of failed login attempts. These tools seem simple, but they hit crooks where they hurt most: the wallet. Locking a thief out after a few failed attempts "even for half an hour changes the economics," says Johnson, making it harder for the crook to grab your account information or access linked cards. Multilevel authentication: With this feature, a simple name and password alone are not enough to get anyone -- including you -- into the account. Instead, you will need at least one more piece of information that will come from a different source. A common option for this extra information is a one-time code the site sends to your phone. Notifications and alerts. If an app or online account offers security notifications, "turn them on," says Schwartz. While sometimes annoying, an alert that someone just used your account to spend a bundle will "wake you up," he says. "It's in real time, and you'll pay attention," Schwartz adds. [9]

No. 4: Say yes to credit cards, no to debit cards. If you are going to store card information on an app or site, make it a credit card, not a debit card, says Breyault. "The protections are better," he says. "And you're unlikely to miss a (mortgage or bill) payment because someone has drained your credit card." With a credit card, the Fair Credit Billing Act limits your financial losses to $50. Many cards exceed federal laws and waive your liability altogether. By contrast, you can be liable for up to $500 -- or even the total amount of your loss --  with a debit card, depending on when you report the fraudulent activity. Select a credit card with a good record of fighting fraud and granting chargebacks, says Velasquez. Those terms and conditions are what sets them apart, but nobody really drills down and reads them," she says. "So know the parameters of your credit card." Use any security tools and alerts the card offers, such as alerts for each online transaction, she says. If you don't have a credit card and want to shop with apps and online accounts, you can often link to one of the retailer's own gift cards, says Velasquez. By linking to a gift card instead of a debit card, you limit potential losses to the balance on the gift card, instead of to the balance of your checking account. [9]

No. 5: Watch those linked cards. If you link a card to an electronic shopping account, keep an eye on the card. "Pay close attention to your statements," says Breyault. "If you see unusual activity, question it right away." Quickly report such activity to your card issuer. Do not rely on a retailer to do it for you. If you believe you have been hacked or had your financial data compromised, consider helping others by filing a complaint with the National Consumers League and/or the Federal Trade Commission, says Breyault. These organizations "will share their complaint with a network of law enforcement agencies," he explains. [9]

No. 6: Amp up your security. Johnson says many of today's phones have virtually become a "point-of-sale system." If your phone is now your wallet, start treating it like a wallet. "You have to be careful about mobile malware and unauthorized access to your phone," Johnson says. For starters, put a password on your phone, says Velasquez: "If it's lost or stolen, someone can't just hit a button and use these apps to make various charges. "Install anti-virus and anti-malware programs for your phone, she says. Some of these programs even feature the ability to assign different security levels to different apps, she says. Also install such software on your home computer. [9]

## VII. Impact of Identity Theft

While merchants face some obstacles in EMV adoption, consumers are getting smarter about protecting their information, and fraudsters aren’t wasting time. Being aware of how chip cards are impacting fraud can help your financial institution implement the solutions and best practices that protect your cardholders and meet their expectations for a secure banking experience. Consumers are more aware of fraud. High profile data breaches first drew consumers’ attention to the threat of fraud, but EMV chip card issuance brought it home. According to the Gallup 2015 Crime Survey, card fraud and identity theft are the types of crime consumers are most concerned about. Educating consumers about the increased security features of EMV chip cards has brought greater awareness of the threat of card fraud. Issuing EMV chip cards provides an opportunity for your institution to reiterate its commitment to securing payment transactions for your customers. [10]

There is a sense of shared responsibility. A consumer survey conducted by Vantiv and Socratic Technologies revealed that 72 percent of consumers and 70 percent of card companies feel that they are equally responsible for protecting themselves against credit and debit card fraud. Card controls and other security monitoring practices give financial institutions a means to share this responsibility with their cardholders. Account monitoring tools like MobiMoney from Vantiv put cardholders in control of their cards and help ease the burden of fraud protection for financial institutions, merchants, and consumers alike. [10]

On the other hand, other types of fraud are increasing. Fraudsters road blocked by EMV are finding other ways to get their job done. During the first half of 2016, more than half a billion data records were compromised in 974 publicly disclosed breaches worldwide. Since EMV only protects against counterfeit card present transactions, fraudsters are increasing going online and targeting card-not-present opportunities. Additionally, account takeover and identity theft are becoming more common. Thieves are going after unprotected personally identifiable information, targeting healthcare and government organizations in particular. Automatic Fuel Dispensers (AFD) have the potential for being a target for fraudsters. In addition to being difficult and costly to upgrade, AFD operators have more time to prepare to accept EMV chip card payments in order to avoid counterfeit fraud liability. Another area of concern is non-received issue (NRI) fraud, in which delivery of a consumer’s card is stolen or intercepted. However, financial institutions typically have practices and precautions in place to prevent this type of fraudulent activity. No doubt, the EMV migration will have a permanent impact on card payments and financial institution offerings. Being aware of this technology’s impacts on fraud and across the consumer experience can put your institution in a competitive position to meet cardholder expectations now and into the future. [10]

IBM touts holistic approach to cyber-security, counter-fraud, and compliance efforts. The best way to thwart digital theft and fraud is to use a holistic, connected approach that takes advantage of the latest technologies and applies advanced analytics to vast data sets. It's an approach IBM touted at a mid-March event in New York where it brought together more than 100 security, compliance, and risk-management professionals. [11]

IBM promoted new software and services designed to support this approach. Experts, including a former White House CIO and executives from banks, insurance companies, security firms, and government agencies, offered tips and best practices for moving beyond security, fraud, compliance, and risk silos. The stakes are higher than ever, with increasingly sophisticated and global digital criminals now responsible for some $3.5 trillion in losses each year, according to the Association of Certified Fraud Examiners. [11]

The most important advice is to break out of departmental silos. It's not that you should consolidate separate departments that address, for example, cybersecurity, fraud, and anti-money-laundering compliance efforts. But these separate groups should collaborate, with shared data, measures, goals, and coordinated incentives. "If you start sharing information and thinking through processes across that data, it will help you to bust out of those silos," said Theresa Payton, who served as White House CIO from 2006 to 2008. Payton cited two organizations that created working teams across physical security, cybersecurity, anti-money-laundering, fraud, and risk departments. Collaboration helped one of these organizations, a defense contractor, spot a shell company posing as a supplier. As a result, the firm avoided a $500,000 wire transfer tied to a falsified purchase order, according to Payton. [11]

Once you can span silos and share data, the next step is to apply advanced analytics to spot crime. Last year Atlanta-based SunTrust Bank was able to work across departments, pool information, and apply big data analyses to foil a sophisticated deposit-fraud scheme. "These fraudsters knew more about our bank than some of our own people knew about how we post money to accounts," said speaker Aaron Glover, a senior analyst at SunTrust. "We discovered that we could work better together by establishing protocols for information sharing across anti-money-laundering, corporate security, and the fraud unit." [11]

The upshot was that SunTrust was able to pool a variety of data sets, develop deep analyses to uncover the fraud patterns, and institute procedural changes to thwart the fraudulent deposits. "As a result we were able to save $5.8 million within one year," Glover said. The New York State Department of Taxation and Finance uses advanced analytics and case-management capabilities -- core components of the Counter Fraud Management Software that IBM introduced -- to thwart $350 million in fraudulent tax refunds per year. Internal auditors who recovered an average of $500,000 per auditor per year a few years ago are now recovering $2.5 million per year due to case-management workflow automation and analytics that flag suspicious returns, said Nonie Manion, the department's executive deputy commissioner. Other steps experts suggest include identifying and prioritizing the assets you must protect, holding "doomsday" drills to determine how departments will handle an incident, reviewing security policies and procedures with all employees, and working with law-enforcement and security groups to get ahead of cybercrime and fraud schemes. [11]

All security, fraud, risk, and compliance departments and initiatives within your organization should be aligned and connected, sharing reports on the latest security incidents and fraud attempts. Criminal activities are often connected. Denial-of-service cyber-attacks, for example, are sometimes used by criminals as a diversionary tactic as they attempt to infiltrate and steal data from corporate backend systems. Stolen data is then used to perpetrate fraud. Money stolen through fraud is invariably laundered through otherwise legitimate accounts and transactions. Working together lets you see the bigger picture of interrelated activities. "Fraudsters can potentially hide in plain sight within the data, especially if the data is not interconnected or you're not taking an analytical approach," said Bob Griffin, Vice President of Counter Fraud Solutions at IBM. "By combining the data, it's possible to spot early-indicator events and interrelated activities that you would not spot looking at data in isolation." [11]

The New York State Office of Medicaid has lots of separate departments, admits Medicaid inspector general James Cox, but by organizing oversight teams along business lines the agency has eliminated overlapping efforts and aligned activities. "The silos haven't gone away, but it has been a very successful program that has helped us detect abuse and fraud much more quickly," Cox said. Once cybersecurity, transaction-security, fraud, and risk-and-compliance teams are collaborating, the next step is to institute shared measures, goals, and incentive-compensation plans. "What gets measured gets done, so do you incent people to interact with each other and pursue shared goals?" asked Theresa Payton, former White House CIO and now CEO of risk, fraud, and security firm Fortalice. "If the fraud team reaches its goals, but anti-money-laundering doesn't, should the fraud team get bonuses? Yes, but they should also have shared goals." [11]

Theresa Payton advises corporations and agencies to identify their POTUS- (President of the US) and VP-level priorities. It might be customer information, intellectual property, or financial transaction security. "There are a lot of critical assets, but all constituents should meet to determine the top-two assets that must be protected from a fraud perspective," said Payton. Corporate communications or marketing people might be the best choice to run such a meeting, Payton advises, as departmental bosses are likely to try to sway the assessment. A clearer understanding of the top priorities will help you budget time, talent, and technology investments accordingly. [11]

Make use of the latest technologies. Just as security, fraud, risk, and governance teams should work together, so too should their technologies, advises IBM. The vendor has acquired multiple security technologies in recent years, including SRD entity analytics, i2 social-network and geospatial-analysis tools, and Trusteer malware protection and endpoint management systems. The new [IBM Counter Fraud Management Software](http://www-03.ibm.com/security/counter-fraud/) integrates these formerly separate technologies to support a coordinated, cross-enterprise approach. IBM says existing security, fraud, risk, and compliance tools and systems can be tied in to its counter-fraud platform. Uniting components include advanced analytics and reporting from SPSS and Cognos, and business rules, alerting, and case-management technologies from iLog, FileNet, and IBM Business Process Manager. "We're bringing everything together so we can help our clients move from being reactive to being proactive," said Bob Griffin. [11]

Make use of the data. Data are the most valuable assets in the fight against fraud, yet many organizations leave valuable information untapped in production database tables, according to Aaron Glover, senior analyst at SunTrust Bank. "What we need to be doing, through a chief data officer or data custodian role, is putting this asset into a useful, consumable form on which you can build fraud-risk models and perform link analysis so you spot the bad actors," said Glover. SunTrust used advanced analytics to uncover a sophisticated scheme in the Atlanta metro area tied to a 200% increase in deposit-fraud losses at the bank. A data-analysis breakthrough brought a $5.8 million reduction in deposit fraud in one year. [11]

Review processes and make "doomsday" plans. It's not enough to implement technologies. You have to walk through plausible security scenarios and do disaster drills in order to be prepared. Communication and response plans should be in place before your most important assets are compromised, said Theresa Payton of Fortalice. Lay out the chain of command, escalation plans, action options, key contacts, and recovery steps. Develop media communications plans and consider scenarios in which you may be uncertain as to whether, say, data was accidentally exposed or intentionally stolen. IBM's Smarter Counter Fraud Center of Competency provides industry-specific consulting services that will identify a client's program strengths and weaknesses, and design and implement strategies for detecting, responding to, and investigating fraud. [11]

Train everyone on security policies and procedures. Security and fraud prevention aren't just for related departments. Companies should review security policies and procedures with *all employees* on an annual basis. Topics might include the applications that are acceptable to use and various types of data covered by confidentiality and privacy agreements and laws. Go over safe download, email, thumb-drive, mobile-device, and device-retirement practices. Make sure your organization has clear and consistently enforced policies on patching operating systems and software, the use of passwords and timeout features, data encryption, data-sharing, and system access among partners and suppliers. Target's recent data breach was traced back to a third-party contractor that unintentionally opened a pathway for malware that was exploited to steal credit card data, according to John O'Neill, SVP of fraud investigations at Bank of America. "You have to consider what data and systems your vendors have access to," he said. [11]

Work with law enforcement and security groups. Don't wait for an incident before you get acquainted with law enforcement and security groups. Regional FBI offices and national and global security organizations can tip you off on emerging and active threats that may have infiltrated your enterprise without your knowledge. Fraudsters are taking advantage of every advance in technology, so it's incumbent upon businesses and government agencies to band together to fight cybercrime, said Maria Vello, CEO of the National Cyber-Forensics and Training Alliance (NCFTA). The NCFTA has collected 12 years' worth of data on malware and cybercrime, and it works with law enforcement and security organizations in the US, Australia, Canada, Korea, and Japan to spot new forms of malware, data theft, and fraud. The nonprofit shares this insight with members to thwart attacks. It also helps build legal cases against perpetrators. IBM shares data with security professionals through IBM X-Force, a team that offers quarterly updates on malware and phishing attacks and trends. Last week IBM introduced IBM Red Cell, which will share similar intelligence on fraud. [11]

Collaborate across industries. Look beyond the silos within your own organization and consult with organizations in other industries, advises Jim O'Neill, senior VP of fraud investigations at Bank of America. Bank accounts, for instance, are routinely used by criminals as a destination for deposits tied to fake auto auction sites and falsified tax refund requests. But banks don't have all the data needed to spot this activity within their four walls. "Without a complete picture, you're guessing, so you need to work with other companies to complete the picture," said O'Neill. Telecom companies, Internet access providers, and email providers, for instance, hold the data on phishing scams aimed at defrauding bank customers. Banks and other organizations have to cross organizational boundaries, perhaps with the aid of law enforcement or security organizations, in order to forge alliances. [11]

Strike a balance between security and customer experience. It's possible to lock down business activities so tightly you can virtually eliminate theft and fraud, but you'll ruin the customer experience in the process. Banks, insurance companies, and government agencies want to make it as easy as possible to open accounts, obtain policies, file claims, and secure justified returns and benefits. "Competitive banking has brought us online account-opening and mobile-deposit options that used to require a branch or ATM visit," said Aaron Glover of SunTrust. These new options have introduced new opportunities for fraud, "but we don't want that to affect the way we do business with honest customers." Businesses such as car dealerships and money transmitters that have higher instances of fraud deserve and get extra scrutiny, said Glover, while customers with ordinary customer profiles can open accounts and start depositing and withdrawing money entirely online. [11]

## VIII. Company Usage and Consumers

Companies like Amazon, Chase, PNC, Bank of America, Wells Fargo and other companies are implementing chip technology by updating their credit cards and debit cards and requiring customers to upgrade to the new cards. While on one hard they insist that these are definitely more secure, there is a downside. A credit card war has erupted between large retailers and credit card companies.  The culprit:  chip-embedded credit cards.  Over the last year, credit card issuers have been sending consumers new cards that have a chip embedded in them. Allegedly, these new “smart” cards made your use of a credit card safer. But did it really? Not according to Home Depot, Walmart and a number of other retailers.   In fact, these new cards may have given the Visa and Mastercard a new way of overcharging consumers. [12]

Recently, Home Depot filed an anti-trust suit against MasterCard and Visa in Federal court for allegedly forcing consumers to use unsecure credit cards raises the question. A central issue in Home Depot’s lawsuit is the retailer’s accusation that Visa and MasterCard are conspiring to prevent adoption of more secure technology in order to maintain market dominance and profits. “For years, Visa and MasterCard have been more concerned with protecting their own inflated profits and their dominant market positions than with the security of payment cards used by American consumers and the health of the United States economy,” Home Depot states in its 138-page lawsuit.  This follows a similar lawsuit filed by Walmart and [a group of smaller retailers](http://www.law360.com/articles/769244/retailers-hit-visa-mastercard-banks-with-antitrust-suit) earlier in 2016.  In fact, Walmart Canada also announced that its stores will boycott Visa cards, citing high fees for transactions. [12]

Remember that Chip-and-PIN cards operate just like the checking-account debit card you have been using for years. Entering a PIN connects the payment terminal to the payment processor for real-time transaction verification and approval. However, many payment processors are not equipped with the technology needed to handle EMV chip-and-PIN credit transactions. So it is not likely you will have to memorize new PINs anytime soon. A vast majority will be issuing chip-and-signature cards, which aren’t all that different from how credit cards work now.  Again, as with a magnetic-stripe credit card, you sign on the point-of-sale terminal to take responsibility for the payment when making a chip-and-signature card transaction. [12]

But the failure to require a PIN turns out to be very expensive. Credit card fraud is now a $16 billion a year problem in the United States alone, and every hour, thieves with skimmers are stealing Americans’ credit card numbers. Again, while chip-enabled cards offer an extra layer of security beyond the chip itself, by not requiring the user to enter a four-digit PIN, there’s not real benefit because “Signatures can be copied or forged, and cashiers are not handwriting experts trained to identify forged signatures.” As a result, Home Depot claims United States consumers and merchants such as the Home Depot pay fraud-related costs that are “unrivaled in the rest of the industrial world.” [12]

In fact, the lack of PIN requirements in the United States could lead to even greater fraud in the future, as more transactions shift to online payments, where no physical card is presented  The answer is yes, the new cards were supposed to improve security. However, the Home Depot suit and a similar one recently filed by Walmart against Visa claim that the system was executed poorly, leaving credit card transactions vulnerable to fraud.  Unfortunately, the PIN is only good if hackers can’t get it and that is precisely the problem. Two high-profile data breaches at Target and Home Depot occurred because hackers used malware to collect customers’ credentials, including PINs, from the retailers’ systems. Those breaches affected 56 million cards in the Home Depot breach and 40 million in the Target breach. [12]

The newspapers make it sound like the battle is over PINs vs. signatures but in fact all the evidence suggests that this is a battle between retailers and credit card companies about fees. Many retailers have pointed to the fact that consumers’ card transactions are routed over Visa’s or MasterCard’s signature debit networks, where merchant fees are often more than double what they are on comparable pin debit networks, according to data compiled by the Federal Reserve. “Visa and MasterCard have pushed consumers to use payment card technology that Visa and MasterCard know is defective and subject to fraud and have colluded with each other and with the banks that issue debit and credit cards to do so,” it reads. As a result, Home Depot is charged higher fees by the card issuers, the suit claims. “The Interchange Fee on signature transactions is markedly higher than the fee on PIN transactions,” Home Depot’s complaint alleges. “According to data from the Federal Reserve Board, as of 2009, the average Interchange Fee for signature debit was 56 cents per transaction (or 1.53%) while the average fee for PIN debit was just 23 cents (0.56%).” [12]

Wal-Mart’s lawsuit follows two decades of negotiations, court battles and Congressional lobbying between retailers and payment card networks over billions of dollars in fees paid each year to process transactions. Wal-Mart and other merchants sued Visa in 1996 over a policy called “honor all cards” that forced merchants to accept both credit and debit cards. The case was settled in 2003 on the night before it was to go to trial, with Visa agreeing to pay $2 billion to retailers and lower the fees it charged to merchants for debit-card transactions. [12]

Wal-Mart also sued Visa in 2014 for more than $5 billion over card fees charged to merchants, known as “interchange.” The companies settled the case last year. Retailers nationwide reached a $5.7 billion settlement with Visa and rival MasterCard in 2012 over allegations that they illegally fixed fees for credit cards through restrictive rules that prevented merchants from passing along the costs or even disclosing them to customers.  However, in late June, an appellate court rejected the settlement on the basis of attorney conflict of interest and sent it back to the lower courts.   In the interim, 8,000 retailers, including Wal-Mart, dropped out of the settlement, claiming the accord wasn’t big enough and that it allowed card firms too much freedom to raise rates in the future. Wal-Mart filed its own suit against Visa seeking at least $5 billion in damages, but did not pursue claims against MasterCard. The case has been settled for an undisclosed amount, according to Visa company filings.  Retailers also successfully lobbied for limits on debit card fees, passed as part of the 2010 Dodd-Frank financial reform legislation. The result is that debit card fees have dropped by roughly two thirds. [12]

The new Chip and PIN technology threatens the relative monopoly on processing “signature-based” verification for Visa and MasterCard transactions. According a recent press accounts, Visa makes about five cents more per signature transaction than it does for those transactions that involve a PIN. To be clear, the data shows that a couple very large credit card companies profit by using an outdated credit card verification process that is more susceptible to fraud, which pushes avoidable costs to merchants. When merchant costs go up, so do consumer prices. In other words, the big credit card companies win and everyone else loses. [12]

The credit card companies counter this, claiming that requiring shoppers to memorize a PIN would discourage them from using the cards.  Not all issuers were implementing a PIN; therefore, any card requiring a PIN was at a disadvantage in the competition to be ‘top of wallet’.  Also, the costs to issuers to implement PINs for credit cards is significant.” Switching the world’s largest, most distributed, and most fragmented credit card market to a chip-and-PIN plan would have been horrifically complex and expensive, they claim. [12]

## IX. Future of Credit Cards and Related Technologies

The foundation of the future of credit card processing will be based on two pillars: speed and efficiency. The companies that are staying ahead of the trends in the payments ecosystem have realized that these two factors are paramount for consumers. The Huffington Post notes that 25% of organizations stopped accepting cash altogether in 2015. And given that more individuals are managing their finances electronically, it's natural that more companies will become cashless. [13]

To that end, mobile payments will be the wave of the future. Apple Pay, Samsung Pay, Chase Pay, Android Pay, Microsoft Wallet, Walmart Pay, Kohl's Pay, and more will all become habitual for shoppers, who will reach for their phones instead of their wallets. BI Intelligence forecasts that mobile payments growth will be slower than anticipated, but volume will pick up significantly by 2020 to hit $503 billion, up from $75 billion in 2016. And more than half of the United States population will at least try a mobile wallet by 2020. [13]

Mobile payments are typically frictionless, which is a problem that EMV cards have in spades. These chip cards certainly provide extra security, but they are slow to process thanks to their two-step procedures and often frustrate shoppers on the checkout line. This could spur more users to try mobile wallets, which often involve a simple tap of the screen to process the payment. As a result, more merchants would need to invest in mobile wallet readers, even inside their brick-and-mortar stores. As consumers more frequently expect rapid payment processing, merchants will need to meet that desire or risk losing their customers to other stores that do. [13]

Apple will expand in multiple directions as it attempts to boost adoption of its service. Apple claims it is adding one million Apple Pay users per week, while Juniper Research says 148 million global consumers will use contactless services like Apple Pay this year. Apple is pushing hard to introduce the service in more territories, particularly in Europe and Asia. “We’re working rapidly in Asia and also in Europe, our goal is to have Apple Pay in every significant market Apple is in,” Jennifer Bailey, VP of Apple Pay, recently told TechCrunch. Apple’s recent launch in China will be seen as especially significant and India is also a key market, Apple CEO, Tim Cook, recently disclosed. Beyond the inevitable introduction of Apple Pay for online payments and the potential then for in-app payments, enabling, for example, secure online shopping via an Apple TV, there are many other key opportunities the company can explore. [14]

Mary Meeker’s Internet Trends Report looked closely at mobile payment services and noted that messaging services like WeChat, and social networks like Facebook and Instagram are growing popular payment services, particularly in the APAC, where WeChat is already more popular than some debit cards. Alibaba’s AliPay generated over $1 trillion in payments in 2015. This integration between messaging and payment services makes it an utter no-brainer to predict Apple Pay support for payments through Messages is on the way. This is of wider strategic consequence, given the move dovetails so well with Apple’s recent Didi investment and Apple Car plans. The Wall Street Journal confirmed these plans last year and an Apple patent shows its potential as a Messages feature. Banks are developing cash machines with NFC support and these will demand both a biometric element and passcode in order to protect against theft, but one day you will inevitably be able to withdraw cash from any ATM anywhere just by waggling your Apple Watch above the machine. [14]

Operator billing is popular in some countries. It’s a system in which your carrier allows you to pay bills and services via your mobile phone, recouping costs from your bill. Such services are highly popular in developing economies where smartphone users may lack conventional bank accounts. Apple Pay may in future offer something similar. “In India, that is something we are looking at. Operator billing is something, we don’t need in the US. But in India it is something the customer would want and help us move faster,” Cook recently said. Apple Pay may help support emerging economies. [14]

There is huge potential for Apple Pay and Wallet in retail. Forrester recently found 57% of US online adult smartphone users are interested in access to loyalty schemes and rewards within mobile wallets. Apple Pay will soon offer loyalty and discount schemes, replace under-utilized retail apps, and help deliver personalized shopping experiences. Customers should be able to use Apple Pay to purchase things in shops, but they should also see those transactions automatically added to existing loyalty schemes, and receive personalized deals and coupons. [14]

## X. EMV Questions and Answers

1. Why are EMV cards more secure than traditional cards? It is that small, metallic square you'll see on new cards. That is a computer chip, and it is what sets it apart the new generation of cards. The magnetic stripes on traditional credit and debit cards store contain unchanging data. Whoever accesses that data gains the sensitive card and cardholder information necessary to make purchases. That makes traditional cards prime targets for counterfeiters, who convert stolen card data to cash. "If someone copies a mag stripe, they can easily replicate that data over and over again because it doesn't change," says Dave Witts, president of U.S. payment systems for Creditcall, a payment gateway and EMV software developer. [15]

Unlike magnetic-stripe cards, every time an EMV card is used for payment, the card chip creates a unique transaction code that cannot be used again. If a hacker stole the chip information from one specific point of sale, typical card duplication would never work "because the stolen transaction number created in that instance wouldn't be usable again and the card would just get denied," Witts says. EMV technology will not prevent data breaches from occurring, but it will make it much harder for criminals to successfully profit from what they steal. Experts hope it will help significantly reduce fraud in the United States, which has doubled in the past seven years as criminals have shied away from countries that already have transitioned to EMV cards, Conroy says. "The introduction of dynamic data is what makes EMV cards so effective at bringing down counterfeit card rates in other countries," she says. [15]

Counterfeit fraud rates have already decreased in the U.S. as a result of EMV adoption, according to Mastercard and Visa. In March 2017, chip-enabled merchants saw a 58 percent drop in counterfeit fraud compared to a year earlier, according to Visa. Mastercard noticed a difference even earlier: It recorded a 54 percent decrease in counterfeit fraud costs among its EMV-ready merchants from April 2015 to April 2016. [15]

2. How do I use an EMV card to make a purchase? Just like magnetic-stripe cards, EMV cards are processed for payment in two steps: card reading and transaction verification. However, with EMV cards you no longer have to master a quick, fluid card swipe in the right direction. Chip cards are read in a different way. "Instead of going to a register and swiping your card, you are going to do what is called 'card dipping' instead, which means inserting your card into a terminal slot and waiting for it to process," Conroy says. [15]

When an EMV card is dipped, data flows between the card chip and the issuing financial institution to verify the card's legitimacy and create the unique transaction data. This process isn't as quick as a magnetic-stripe swipe. "It will take a tiny bit longer for that transmission of data to happen," Witts says. "If a person just sticks the card in and pulls it out, the transaction will likely be denied. A little bit of patience will be involved." [15]

While chip card transactions may take a bit longer than magstripe transactions, total card processing time will vary between merchants and eventually speed up as the new payment environment is improved. “It will vary depending on the merchant, the equipment and the point-of-sale system,” Ferenczi said. “I think that time lag overtime will be reduced for those longer transactions.” [15]

3. Is card dipping the only option? Not necessarily. EMV cards can also support contactless card reading, also known as near field communication. Instead of dipping or swiping, NFC-equipped cards are tapped against a terminal scanner that can pick up the card data from the embedded computer chip. "Contactless transactions are more consumer-friendly because you just have to tap," said Martin Ferenczi, president of Oberthur Technologies, the leading global EMV product and service provider. "Around the world, there is a move to make EMV cards dual-interface, which means contact and contactless. However, in the U.S., most financial instructions are issuing contact cards." [15]

Dual-interface cards and the equipment needed to scan them are expensive. Right now, the first step is to successfully integrate EMV cards into the U.S. shopping scene. Dual interface will arrive later, although they are in production and rolling out slowly now, according to Ferenczi.

“Dual-interface cards, which in 2016 represented less than 5 percent of total EMV cards in the United States, will have significant growth in 2017,” Ferenczi said. “Issuers want to offer their cardholders the added level of speed and convenience provided by tapping.” [15]

4. Will I still have to sign or enter a PIN for my card transaction? Yes and no. You will have to do one of those verification methods, but it depends on the verification method tied to your EMV card, not if your card is debit or credit. Entering a PIN connects the payment terminal to the payment processor for real-time transaction verification and approval. However, many payment processors are not equipped with the technology needed to handle EMV chip-and-PIN credit transactions. So it is not likely you will have to memorize new PINs anytime soon, according to Conroy. "There aren't going to be many issuers requiring a PIN," she says. "A vast majority will be issuing chip-and-signature cards, which aren't all that different from how credit cards work now." [15]

As with a magnetic-stripe credit card, you sign on the point-of-sale terminal to take responsibility for the payment when making a chip-and-signature card transaction. United States chip-and-PIN cards will be transitioned in slowly, according to Ferenczi. "The card production demand today is really based on chip-and-signature cards," he says. "It will probably take two to three years to fully convert to chip-and-PIN." Despite a slow transition overall, those who get chip-and-PIN cards will be able to use them right away. "If a terminal doesn't have the ability to accept a PIN, it will then step down to accepting a signature," says Randy Vanderhoof, executive director of the Smart Card Alliance. "There will always be a secondary option." [15]

5. If fraud occurs after EMV cards are issued, who will be liable for the costs? If an in-store transaction is conducted using a counterfeit, stolen or otherwise compromised card, consumer losses from that transaction fall back on the payment processor or issuing bank, depending on the card's terms and conditions. Since the Oct. 1, 2015 deadline created by major U.S. credit card issuers Mastercard, Visa, Discover and American Express, the liability for card-present fraud has shifted to whichever party is the least EMV-compliant in a fraudulent transaction. [15]

Consider the example of a financial institution that issues a chip card used at a merchant that has not changed its system to accept chip technology. This allows a counterfeit card to be successfully used. "The cost of the fraud will fall back on the merchant," Ferenczi says. The change is intended to help bring the entire payment industry on board with EMV by encouraging compliance to avoid liability costs. Today, any parties not EMV-ready could face much higher costs in the event of a large data breach. [15]

Until recently, automated fuel dispensers had until 2017 to make the shift to EMV. However, a December 2016 Visa and Mastercard agreement now gives pay-at-the-pump gas terminals until October 2020 to become EMV-compliant. “Given the migration challenges for implementing EMV in the petroleum environment, Visa's and Mastercard’s modification of the liability shift dates will be beneficial to the retail petroleum industry and the U.S. chip migration,” Vanderhoof explained in an emailed statement. So for now, gas stations do not fall under the existing EMV fraud liability shift rules. ATMs still have two fraud liability shift dates: Mastercard’s that passed in October 2016 and Visa’s in October 2017. [15]

6. Since Oct. 1, 2015, is the transition to EMV technology complete? Not yet. Although the deadline was strong encouragement for all payment processing parties to become EMV-compliant as soon as possible, not everyone has made the transition yet.“Most countries that migrated to EMV have four or five banks that issue cards and a couple of acquirers that provide a service to merchants,” said Jason Oxman, chief executive officer of the Electronic Transactions Association. “We have 13,000 financial institutions in the U.S. that issue credit and debit cards, and we have 5 million merchant locations in the U.S. that accept debit and credit cards. So it’s a *massive* undertaking.” [15]

EMV debit cards have rolled out at a slower pace. Approximately 25 percent of U.S. debit cards were issued as EMV chip cards by the end of 2015, according to Mercator Advisory Group’s Sarah Grotta, director of Debit Advisory Service. That ratio rose to 33 percent by the end of June 2016, and today, approximately 60 percent of issuer's debit cards are EMV chip-equipped, according to CPI Card Group estimates. EMV debit cards are slowly being issued because banks have to prep their software to accept those new cards as well, according to Ferenczi. [15]

The majority of chip cards in the hands of cardholders today have come from larger issuers auch as Bank of America and Chase, according to the Federal Reserve Bank of Chicago. The cost of this EMV transition is causing smaller banks to convert their cards more slowly. The EMV credit card rollout, however, is progressing steadily. More than 449 million Visa chip cards have been issued in the United States overall so far, as of June 2017. About 68 percent of Mastercard-branded credit and debit cards have been issued with chips so far, as of Oct. 1, 2016. For all U.S. credit cards, CPI Card Group estimates approximately 85 percent of cards now have chips on them. Overall, 70 percent of cards (debit and credit) have been converted to EMV, per CPI Card Group. [15]

If some of the cards in your wallet have yet to be issued with chips, don't fret. "Different companies have different rollout strategies," says Doug Johnson, vice president of risk management policy for the American Bankers Association. Some will base their actions on card expiration dates; others will work to get chip cards into the consumer's hands as soon as possible.“I think the progress we are seeing today is promising,” said Chiro Aikat, senior vice president of product delivery (EMV) at Mastercard. [15]

7. If I want to use my chip-card at a retailer that doesn't support EMV technology yet, will it work? Yes. The first round of EMV cards -- many of which are in consumers' hands -- will be equipped with both chip and magnetic-stripe functions so consumer spending is not disrupted and merchants can adjust. If you find yourself at a point-of-sale terminal and are not sure whether to dip or swipe your card, have no fear. The terminal will walk you through the process. "For example, if you enter a card into the chip reader slot but the reader isn't activated yet, it will come up with an error and you'll be prompted to swipe the card in order to use it," Vanderhoof says. And vice-versa. "If a consumer tries to swipe a chip card instead of inserting it, an error will appear and they will be prompted to insert the card for chip processing instead," Vanderhoof says. [15]

If chip-card readers are not in place at a merchant at all, your EMV card can be read with a swipe, just like a traditional magnetic-stripe card. "You can still conduct transactions, you just lose that extra level of chip security," Johnson says. While many large retailers, such as Walmart, Target and Costco, have upgraded their POS terminals and have activated them for chip card acceptance, many U.S. retail locations are still *not* EMV-ready. [15]

Visa says 50 percent of U.S. stores, approximately 2.3 million merchant locations, now accept chip cards, as of June 2017. Mastercard has tallied 2.3 million chip-active merchant locations on its network, representing 38 percent of all U.S. merchants back in October 2016. Industry experts expect the merchant migration to slowly continue over the next few years. “I expect to see a slow and gradual increase of merchant moving over, just like we’ve seen up until today, as each merchant makes an assessment if this expenditure makes sense for them and their particular business,” said Mallory Duncan, senior vice president and general counsel at the National Retail Federation. In July 2017, U.S. Payments Forum estimated 45 to 50 percent of U.S. credit and debit card transactions were chip-on-chip. [15]

8. Will I be able to use my EMV card when I travel outside the country? Yes and no. The U.S. is the last major market still using the magnetic-stripe card system. Many European countries moved to EMV technology years ago to combat high fraud rates. That shift has left many U.S. consumers who have magnetic-stripe cards looking for other forms of payment when they travel. [15]

Since many foreign merchants are wary of magnetic-stripe cards, consumers who hold some type of chip card may run into fewer issues than those without one, according to Ferenczi."Just the existence of the chip will likely make European merchants more willing to accept transactions that they wouldn't have likely accepted if a customer presented a mag-stripe card," he say, which is good news for traveling U.S. cardholders. However, chip-and-PIN cards are the norm in most other countries that support EMV technology. So consumers with chip-and-signature cards may find some merchants who are unwilling or unable to process their card, even though it does have an embedded chip. But despite any difficulties in the transition, Ferenczi says the change is a step in the right direction. "Nobody likes to think that his or her card is being secretly used for other purposes," he says. "So I think regardless, there is a level of comfort knowing that it will be far more difficult to counterfeit EMV cards." [15]

The new EMV cards in the U.S. might be called any of the following terms: smart card, chip card, smart-chip card, chip-enabled smart card, chip-and-choice card (PIN or signature), EMV smart card or EMV card. Retailers using mobile payment devices such as Square also have to upgrade their equipment to read EMV chip cards. Square has designed EMV-compatible card readers for Android and iOS devices that can read contactless mobile payments and process dipped chip cards. Merchants can purchase the devices for $49. [15]

Following are some statistics that everyone should keep in mind. 855 million: Estimated number of chip cards issued to U.S. consumers so far, per U.S. Payments Forum estimates. 85%: Estimated percentage of all U.S. credit cards issued with chips at the end of July 2017, per CPI Card Group. 60%: Percentage of U.S. debit cards issued with chips by the end of July 2017, per CPI Card Group. $2-$4: Approximately cost of issuing a new EMV card, per First Data. 15 million: Estimated total number of point-of-sale terminals that have to be upgraded to accept chip cards, per Javelin Research & Strategy. $6.75 billion: Estimated cost of replacing the 15 million POS terminals with chip card-compliant machines, per Javelin Research & Strategy. 50-52%: Estimated percentage of merchant locations currently ready to process chip card payments, per Visa, U.S. Payments Forum and Strawhecker Group estimates. 1.81-2.3 million: Estimated number of U.S. point-of-sale terminals enabled to accept chip card payments, per Mastercard and Visa estimates. [15]

## XI. Conclusion

This work has presented information that will allow consumers to remain informed about credit card technology. Through this case study we now know that chip technology is more secure, although we should always keep in mind that vulnerabilities will always be present, as well as having advantages and disadvantages. Having newer and safer technology will never eliminate all risks but can give us a bit more peace of mind. Lastly, remember that just as technology is expanding and growing at a rapid pace, so too, are cyber criminals, so being vigilant and protecting ourselves as much as possible is critical.

## XII. Bibliography/Reference

[1] D. Bonderud, “Chip Card Security: Past, Present and Potential Future”, SecurityIntelligence, Banking and Financial Services, April 10, 2015. [Online.] Available: <https://securityintelligence.com/chip-card-security-past-present-and-potential-future/>. [Accessed: September 22, 2017].

[2] “What Are EMV Chip Cards?”, Discover, Lifestyle. [Online.] Available: <https://www.discover.com/credit-cards/resources/what-are-emv-chip-cards>. [Accessed: July 3, 2017].

[3] T. Quimby, “Credit card chip technology not more secure than magnetic stripes: FBI warns new chip cards insecure among growing fraud”, The Washington Times, Business and Economy, November 15, 2015. [Online.] Available: <http://www.washingtontimes.com/news/2015/nov/15/credit-card-chip-technology-not-more-secure-than-m/>. [Accessed: June 30, 2017].

[4] “Chip-and-pin vs. chip-and-signature: What’s the difference?” BluePay. [Online.] Available: <http://blog.bluepay.com/chip-and-pin-vs-chip-and-signature-whats-the-difference>. [Accessed: July 3, 2017].

[5] “Chip Card Technology: A Small Business Perspective”, Threat Sketch, January 26, 2016. [Online.] Available: <https://threatsketch.com/chip-card-technology-small-business/>. [Accessed: September 22, 2017].

[6] R. Abrams, “Chip cards will require users to dip rather than swipe”, The New York Times, Business Day, September 28, 2015. [Online.] Available: <https://www.nytimes.com/2015/09/29/business/chip-cards-will-require-users-to-dip-rather-than-swipe.html?mcubz=0>. [Accessed: July 3, 2017].

[7] “Chip Card Security: Why is EMV More Secure?”, Squareup.com, Square, Inc. [Online.] Available: <https://squareup.com/townsquare/why-are-chip-cards-more-secure-than-magnetic-stripe-cards>. [Accessed: June 30, 2017].

[8] M. Schwartz, “Flaws In EMV Chip And PIN Undercut Security”, DarkReading, Vulnerabilities/Threats, May 22, 2014. [Online.] Available: <http://www.darkreading.com/vulnerabilities---threats/flaws-in-emv-chip-and-pin-undercut-security/d/d-id/1269155?page_number=2>. [Accessed: October 11, 2017].

[9] D. Dratch, “6 ways to safeguard cards when shopping electronically”, CreditCards.com, June 22, 2015. [Online.] Available: <https://www.creditcards.com/credit-card-news/6-safeguard-cards-shopping-electronically-1273.php>. [Accessed: September 23, 2017].

[10] “3 ways EMV chip credit cards are impacting fraud”, Vantiv, 2017. [Online.] Available: <https://www.vantiv.com/vantage-point-fi/smarter-payments/emv-chip-credit-cards-impacting-fraud>. [Accessed: September 25, 2017].

[11] D. Henschen, “10 Ways To Fight Digital Theft & Fraud”, InformationWeek, IT Leadership/CIO Insights & Innovation, March 25, 2014. [Online.] Available: <https://www.informationweek.com/strategic-cio/executive-insights-and-innovation/10-ways-to-fight-digital-theft-and-fraud/d/d-id/1127869?image_number=11>. [Accessed: October 11, 2017].

[12] “The Hidden Costs of New Chip-Embedded Credit Cards”, San Diego Consumer Action Network, June 21, 2016. [Online.] Available: <https://www.sandiegocan.org/2016/06/21/hidden-costs-of-new-chip-embedded-credit-cards/>. [Accessed: October 28, 2017].

[13] A. Meola, “Exploring the present and future of credit card processing”, Business Insider, Finance, December 22, 2016. [Online.] Available: <http://www.businessinsider.com/future-of-credit-card-processing-2016-11>. [Accessed: September 22, 2017].

[14] J. Evans, “Here is the future of Apple Pay”, ComputerWorld, News Analysis, June 7, 2016. [Online.] Available: <https://www.computerworld.com/article/3080054/apple-ios/here-is-the-future-of-apple-pay.html>. [Accessed: October 1, 2017].

[15] S. Kossman, “8 FAQ about EMV credit cards: Chip? PIN? Signature? Do old cards work? Answers to frequently asked questions”, August 29, 2017. [Online.] Available: <https://www.creditcards.com/credit-card-news/emv-faq-chip-cards-answers-1264.php>. [Accessed: October 28, 2017].