EMV: Worth the Cost

February 1

2016

EMV has come to the United States after being used in Europe for 2 decades. It promises reduced fraud and more protection for American consumers and less fraud cost for financial institution. With fraud reaching record numbers in the recent years, a better solution for protection seems to be something that all parties would be interested in, but it has not been widely accepted. This white paper will explore the reasons consumers and financial institutions alike have not bought into the technology and if the upgrade of cards is worth what it costs.

Authors:
Allison Beckham- Lancaster, SC (ArrowPointe FCU), abeckham@arrowpointe.org
Robyn Blaylock- Monroe, LA (Monroe Telco FCU), rblaylock@monroetelcofcu.org
Tina Farris- Rock Hill, SC (Family Trust FCU), tfarris@Familytrust.org
Kevin Langford- Georgetown, SC (Georgetown Kraft CU), klangford@gkcu.org

Second Year Project Workbook

TABLE OF CONTENTS

I. INTRODUCTION

What is EMV?

EMV stands for Europay, MasterCard, and Visa. It is the technical standard for smart payment cards. They are called smart payment cards because instead of the Magstrip there is a chip that contains an integrated circuit. Magstrips were the standard for the back of cards since plastic cards were introduced. EMV cards are commonly dipped cards (meaning they are put into the machine) but can also be contactless (the card would just be held over a receiver instead of put into the machine).

EMV differs from Magstrip cards because Magstrips store information on the card using iron-based magnetic particles (Foundation, Wikimedia). Magstrips are read by swiping the card and the merchant machine translates what is on the strip. EMV chips differ because it uses an encrypted code to release information to the merchant machine and it is not stored on the card. It makes the card harder to duplicate because each transaction is processed by a unique code. This means a person could not duplicate the card because the code cannot be duplicated.

There is still fraud with EMV cards but that mostly comes from the card-not-present transactions or from cards being stolen along with the PIN (uSwitch). Many merchants also have a low limit set on no signature required transactions and that also leads to fraud. EMV does keep counterfeit card fraud down which is a major source of fraudulent charges in the United States (uSwitch).

The chip also lasts longer than the Magstrip (PSCU). Stealing cards from mailboxes has begun to increase in the US. Having cards that can be in circulation longer, without having to mail new cards, will help fight this type of fraud.

EMV allows institutions the ability to mitigate some of the risk associated with credit card fraud and some of the costs that come from replacing cards whether they are stolen or worn out from use. These are important reasons why a big push for EMV has now started in the United States. Many insiders forecasted the implementation because the history of EMV would lead institutions and merchants to that conclusion.

Brief History of EMV

The history of EMV is older than most institutions realize. It has become a hot topic in the United States recently due to regulatory changes and enhanced emphasis on implementing, but it can be traced back to France in the 1980's. (The Fraud Practice) These countries saw an increase in fraud with card present transactions and set out to find a way to stop it. After a decade of research there was considerable progress made on the "chip and pin" technology.

EMV cards started appearing in large markets outside of France in 1995 (Foundation, Wikimedia). These countries saw major benefits in the way the cards handled card present transactions and the standard was pushed forward.

However, many international travelers found that outside the countries they had trouble using their cards in places that didn't accept the transaction type (Gray and Ladig, The Implementation

of EMV Chip Card Technology to Improve Cyber Security Accelerates in the U.S. Following Target Corporation's Data Breach). This led to a demand from travelers in well-traveled areas and in the early 2000's US merchants started accepting the transactions.

In the United States it has been a slow process as the chips have been in circulation for 16 years, but only recently laws changed to move the process along. These laws standardized who is responsible for the fraud and many regulations on liability were put in place in October 2015. Later in the paper the changes will be expanded on and detailed.

Introduction to Statement

With the history of the EMV cards truly established through decades of use in Europe, the United States is now migrating towards the card. The slowness of implementation was due to a couple different factors: there was no incentive to change and the price to change for both the merchant and financial institution seemed high. With the liability shift of 2015, an incentive for switching to EMV was given making the least secure party, between the financial institution or merchant, responsible for the fraud (PSCU). Now the only downside is the cost of the technology.

The implementation of EMV requires all cards to be replaced and for all credit unions the price is high. For small credit unions, it can seem unreasonably high with no way to offset the cost. Institutions will still see fraud in card-not-present transactions and online fraud. That leads to many small credit unions willing to deal with fraud to avoid the cost of upgrading.

Are they making a mistake by avoiding the implementation? Even with the liability shift, nothing is forcing credits unions to change. They simply absorb any fraud like they have done since credit cards were invented. This paper examines both sides of the cost; the cost of establishing the standard and the cost of fraud should the credit union chooses to stay with the Magstrip. **Is the protection of EMV worth the cost of upgrading?**

II. RESEARCH

Important dates in US History

It's already established how old the technology of EMV is, but the US has finally started making strides in the chips in the past 4 years. Starting in October of 2012, Visa extended the Technology Innovation Program (TIP) to merchants (Javanovic). This gave the merchants a way to skip annual PCI compliance audits if at least 75% of the merchant Visa Transitions were from EMV chips.

On December 31, 2012, Discover introduced Fraud Liability Shift for Diners Club International. This gave an insight into what was needed for Visa and Mastercard to make the same type of surge in usage.

In April of 2013, credit card acquirers and processors were required to be able to support EMV transactions. This was very important because the EMV chip had now been the standard in Europe for a decade and there were still travelers who would find their cards denied at most

merchants in the United States (PSCU). There was also a mandate in the same month for cross border Maestro ATM to shift liability to the non-EMV ATM.

Target (one of the biggest retailers in United States) had a major breach in November 2013 (The Fraud Practice). Personal information, including names, mailing addresses and phone numbers, were stolen from 40 million customers. Almost everyone who shopped at Target during the holidays was exposed to the fraud. The fraud was met with serious repercussions for the EMV implementation. In December of 2013, executives from Target met with US Justice Department officials to determine how the fraud happened and how it would affect the US economy.

In 2014, innovators and early adopters started pushing towards EMV implementation, mainly due to the Target breach but also because of other security lapses in other merchants. This led to law makers introducing liability shifts for point of sale transactions starting in October 2015. That shift did not include fuel pumps.

The future has some important dates as well. In October 2016, Mastercard will extend the liability shift to ATM transactions at US Terminals and in 2017 all fuel merchants will have the liability shifted to them.

Chip Cards by the Numbers

There are 37.9 billion debit card users in the United States. These users performed 1.4 trillion dollars in transactions from 2009 to 2012 (Miller, Berg and Stroud).

The United States is responsible for 47% of the credit card fraud in the world (The Fraud Practice). About 31.8 million US consumers had their debit card breached in 2014. The average breach was $12.75 per card. 37% of the fraud was from counterfeit cards (The Fraud Practice), which is what EMV targets specifically. 237.64 million cards were part of breaches at places in the United States, such as Home Depot, Michael's, Staples, Domino's and Target.

Breaches of nationwide merchants could lead to even more fraud if the cards were not closed out and reissued. Most of the fraud was from counterfeit cards. The breaches were all performed by a security flaw in the merchants credit card system and would not been breached if the machines had EMV (PSCU). This is why the liability shift is an important process in the move to EMV cards.

III. LIABILITY SHIFT OVERVIEW

What exactly does the Liability Shift mean for institutions? This is a broad term that can be used for many different aspects of changes, but it has a tangible meaning as to what will be changing and why those changes are coming. In general terms, the liability shift means that the least secure institution will be responsible for the fraud. It takes the responsibility for the fraud from the financial institution (should they choose to implement it) and moves it to the less secure merchant. This opens up a line of accountability for merchants and other point of sale locations to upgrade technology that would help its customers avoid credit and debit card fraud that was not present before the liability shift.

What Liability actually means

During a normal practice of fraud, a fraudster would create a card and present it as the real card at a merchant. The merchant should then take the card and check the signature. However, most merchants do not check the signature and on small dollar purchases the signature or PIN isn't required by law (The Fraud Practice). This fraud is considered card present fraud and is the main fraud that EMV is meant to eliminate.

Since fraud was then passed on to the financial institution, merchants had no incentive to upgrade their equipment. This would lead to a financial institution having an EMV card but the merchant not having a reader for the card. The member would be forced to use the Magstrip on the back to make their purchase, bypassing all EMV safeguards put in place by the technology.

The liability shift added an incentive for merchants to upgrade. In October 2015 the shift changed the way the fraud recovery for the member was handled. Now the definition is defined that the least secure institution is responsible for the fraud. This gives both parties reason to upgrade.

To illustrate the shift, here is an example of fraud and how it was handled before and after the liability shift:

Before Liability Shift- A credit union issued EMV cards to their members and a counterfeit card was created through a breach at a merchant. When that counterfeit card was used at a merchant point of sale machine that did not have EMV capability, (meaning the merchant would see that it was a chip card but ask the member to slide using the Magstrip) the ultimate responsible party for the fraud would be the credit union. They would be the responsible party for returning funds and claiming insurance (Medich).

In the example above, the credit union did everything necessary to protect its member from fraud. The card wasn't stolen, it was counterfeited. The credit union had the EMV technology in place, but because the merchant did not have the capability to use the technology the counterfeited Magstrip was used. The merchant did not lose any money on the sale so they did not have a reason to upgrade the technology.

The merchant kept their money, the fraudster received a product through illegal means, and the member had money stolen but returned by the credit union. The only entity in the example that was harmed was the credit union which was actually the most secure party in the entire transaction (they issued the EMV card).

After Liability Shift- Take the same example from above. An EMV card is produced by the credit union, the card is compromised through a merchant breach and a counterfeit card is created. The counterfeit card is then presented at a merchant who does not have EMV technology; the fraudster walks away with $1,000 in illegally purchased goods. When the fraud is detected and brought to the attention of the credit union, the store where the fraud took place reveals they do not have EMV technology, making the store responsible for the fraud. This takes the LIABILITY and SHIFTS it to the least secure party in a transaction. This gives merchants reasons to upgrade their machines.

The credit union does not take a loss in the above example because they were more secure than the merchant. This is a great scenario of why EMV is becoming the standard.

Keep in mind, if the credit union does not have EMV cards and the merchant doesn't have an EMV point of sale machine; it will default back to the credit union. In a situation where the merchant has EMV machines and the credit union doesn't have EMV cards, it would still be the credit union's fraud because they have the least secure system. Below is a chart to explain the shift before and after October's shift.

Date of transaction	**Credit Union Cards**	**Merchant Machines**	**Liability**
Before October 2015	Magstrip Only	Magstrip Only	Credit Union
Before October 2015	EMV Chip	Magstrip Only	Credit Union
Before October 2015	Magstrip Only	EMV Chip Reader	Credit Union
After October 2015	Magstrip Only	Magstrip Only	Credit Union
After October 2015	EMV Chip	Magstrip Only	Merchant
After October 2015	Magstrip Only	EMV Chip Reader	Credit Union

Table 1

As seen in Table 1, the only place that the credit union would see any relief from the fraud is if the merchant was not compatible for EMV. Fraud prevention improves for the credit union more than before the shift because merchants were never responsible for the fraud.

Table of Important Dates for Liability Shift

Date	Significance
February 5, 2011	Law Professor Adam J. Levitin releases study suggesting a two-part system to stem fraud loss. Included in his suggestion is a cap on liability and a regulation that coordinates security measures among all that are involved in payment card networks ((Miller, Berg and Stroud).
August 2012	Visa Announced plans to accelerate chip migration in part to stem the fraud increase including their acceptance of any liability shift with merchants (The Fraud Practice)
January 2012	Mastercard announced a US roadmap to enable next generation of electronic payments including working with law makers on shift
March 2012	Discover announced their own roadmap
June 2012	American express announced their road map.
January, 2013	Card Payment Roadmap for EMV released. In it October 2015 is set as the Liability Shift date for Visa, American Express, Mastercard, Discover transactions
October 2015	Liability shift to least secure vendor in the transactions (POS) only
October 2016	ATM Liability Shift
October 2017	Gas Station EMV Liability Shift

Table 2

Why the shift matters

The shift now gives reasons for merchants to upgrade. Without the shift they would not be responsible for any fraud and had no reason to worry about it. Wal-mart was one of the first major retailers to implement the EMV change (Medich). Not upgrading to EMV machines could lead to a financial burden to the department super store because they would be responsible for all counterfeit fraud at their locations. With their quantity of business, that would be a significant amount of money. This is the same mindset that other merchants will take, shifting the liability back to the credit union. This now gives credit unions a reason to upgrade because EMV has a proven track record of reducing fraud in Europe.

IV. HOW DOES FRAUD TAKE PLACE NOW

History of Fraud

In order to understand how EMV helps stop fraud, it is important to understand the science behind fraud. Today fraud is a high-tech game of equipment with higher elevation of crime touching the lives off all members who have a debit or credit card.

The first credit card fraud were fake cards that had no real person assigned to them. The person would create a realistic card and pass it off to a vendor who would carbon copy the numbers and allow the person to walk out with the merchandise. There were no checks on the validity of the card until the merchant tried to collect money from the credit card company. This led to better technology to find out if the card was real or not.

Merchant machines for swiping magnetic strips replaced the carbon copy and soon there was instantaneous approval of whether the card was a real card or not. Fraud evolved into faking the information on the back of the card. Then balance checking was added to make sure the card had enough funds available for the purchase (The Fraud Practice). This lead to criminals making counterfeit cards of people who were using their cards regularly as it meant the card was valid and had available funds.

Like most things in America, fraud changed when internet commerce started. In the 1990's, the beginning of real internet business started taking place. This led to more elaborate fraud and more exposure to members. It was easy to shop online but it was easier for those willing to steal to find a place where many merchants housed information. It was no longer a 1-on-1 theft. Credit card thieves could find places where thousands of consumers' personal information was kept and could steal it all at once.

The first internet fraud was called a "Famous Name" fraud. Credit card fraudsters would use a third-party stolen credit card with a celebrity of the day's name on it (The Fraud Practice). This was due to fact that the name of the person purchasing was not checked. In the brick-and-mortal commerce, the name was checked easier because the person was standing there. Not verifying a name was a new human behavior, because the excitement about the new way to do business overshadowed the risk of fraud. It was not unusual during this time for orders to have names like "Mickey Mouse" or "Bill Clinton" (EMVCo). The only thing the fraudster had to do was make the name look like a real name to the system. The attacks were usually carried out over and over

at the same vendor until they were stopped and then the fraud would be moved to a different vendor.

In 1996, the internet was starting to be used to test if cards were real. Before this time the fake card would be taken to a gas station to check, but the internet gave them a place to check the cards in the comfort of their own home without having to mask their identity. As the world caught up to the fraud practice, the people perpetuating the crime expanded as well. Online fake names moved towards real names with fake numbers that mocked real numbers. Then the information boom moved them towards just stealing identities and using real cards and real names.

The counterfeit system has moved even further along. In today's environment, cards can be stolen by computers held in pockets, Magstrip mining of information and tried-and-true stealing of cards out of unlocked cars, mailboxes and store terminals.

Often the answer for most people is not to use the internet, but that doesn't always work. The card just has to be in close proximity to some of the various type of technologies and there are many times that cards are given freely to a criminal. A waiter taking a payment for dinner could swipe the numbers. A person working at the cashier line could be skimming information or a skimmer could be put on the front of an ATM or gas station terminal where the card can be read and PIN is recorded. Internet fraud only accounts for 12% of all fraud (Statistic Brain Research Institute). The remaining fraud comes from other points of contact with a fraudster. Even with the low number of internet fraud, it leads to some of the biggest frauds in history.

Some of the biggest scams in history

In the mid 2000's, a gang of fraudsters stole 32,000 credit cards. Masterminded by Russian and Eastern European criminals, the sophisticated system of money laundering and shifting money from the UK to Poland to Estonia helped clone and create credit cards that ended up scamming consumers over $17,000,000 through a period of several years (uSwitch).

At the same time, in a three-step scam, $200 million was stolen by 18 criminals in New York. This scam was more elaborate than the gang in Russia and Eastern Europe. They created all the information and documents needed to make false profiles in the credit agencies. They employed businesses to make fake credit card histories and creating perfect scores that were used to apply for large loans and high credit card limits. To further complicate the scam, all the money used to fund the operation was from laundered money that went through Pakistan, India, UAE and China.

It's not all doom and gloom

Today credit cards are more secure than ever, despite the fraud. Regulations are in place to help. Technology has caught up and surpassed some of the fraud technology and people in general are weary of 'phishing' and other scams for getting information. EMV is one of those technologies and it is fighting against the largest form of fraud, counterfeit cards. Below is a table that goes over the different types of fraud and what % each represents. It also explains which ones EMV

can stop. This is important because it helps give an understanding of what spending money on EMV can do for an institution.

Type of Credit Card Fraud	% of all credit card fraud	Can EMV protect against it.
Counterfeit Credit Cards	37%	Yes, it is the main target
Lost or Stolen	23%	No, but it can with PIN technology
No-Card Fraud	10%	No
Stolen During Mailing	7%	No
Identity-Theft Fraud	4%	No

Table 3

Here is a table on the different point of contacts used for creating counterfeit cards.

Initial Point of Contact	%
Physical card breach	48%
Internet Website	12%
Telephone	10%
Other	7%
Identity-Theft Fraud	4%

Table 4

Fraud isn't age restricted. A person who is internet savvy or has been around internet commerce their entire life is more likely to be part of fraud. Below is a table that shows the fraud age of complaints.

Fraud Complaints by Age	%
20-29	19%
30-39	22%
40-49	25%
50-59	25%
60+	10%

Table 5[1]

[1] The three tables above were created by Credit Card Fraud Statistics at http://www.statisticbrain.com/credit-card-fraud-statistics/

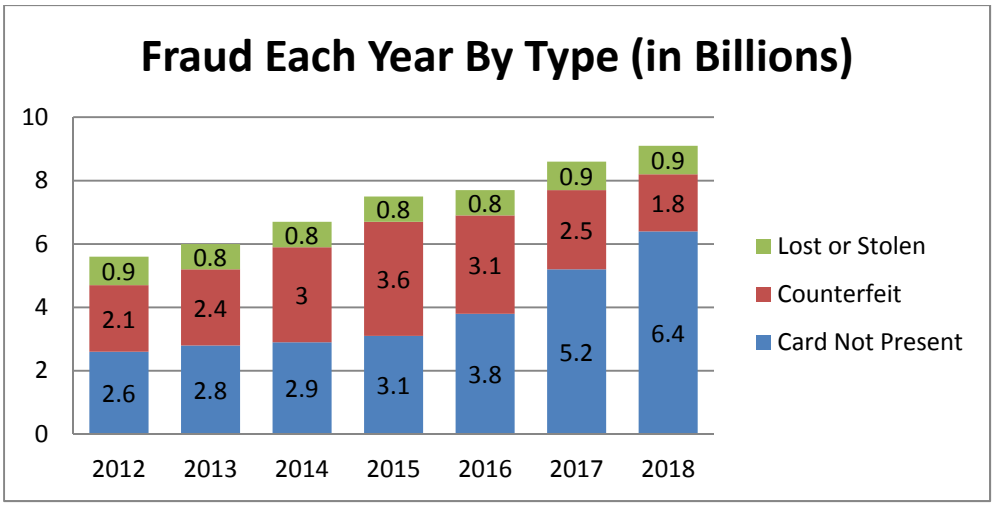

Table 6

This last chart shows the type of fraud per total fraud. It breaks out card not present fraud, counterfeit fraud and lost/stolen cards. It projects out until 2018 and shows a growing trend towards card not present fraud over counterfeit cards. This is the one chart that leads to many opponents of EMV. It shows that while counterfeit cards may be stopped there would still be a large number of fraud moving forward based on the card not present trend. Card not present fraud it mostly handled at the merchant and gives a great deal of responsibility on the merchant and online applications.

How technology helps create counterfeit cards

Before moving onto how EMV technology helps stop credit card fraud, the technology of counterfeit cards needs to be looked at. It is important to understand what the technology of EMV is doing to stop the counterfeit system.

The main way fake cards are created is through card skimming. A small device is mounted on top of an existing card reader, like at an ATM. The magnetic strip information is then stored through that machine when the card is swiped. There is usually a camera on the machine as well to see the PIN entered. The cameras aren't necessary anymore with new number overlays that scammers have been installing to store keystrokes on the machine's number pad. (uSwitch).

That information is then used by the individual or team to create real identical cards with working strips and accurate valid numbers, including the logos and Magstrip information. To a merchant the card looks the exact same as the card that would be presented any other time.

The Magstrip information is real, so the merchant machine reads the information and sends back the correct signals and protocols. If the card is not reported stolen, then the merchant takes it not knowing anything is wrong. This is the largest type of fraud and the type of fraud that EMV targets specifically through its technology.

V. TECHNOLOGY OF EMV

How EMV Works

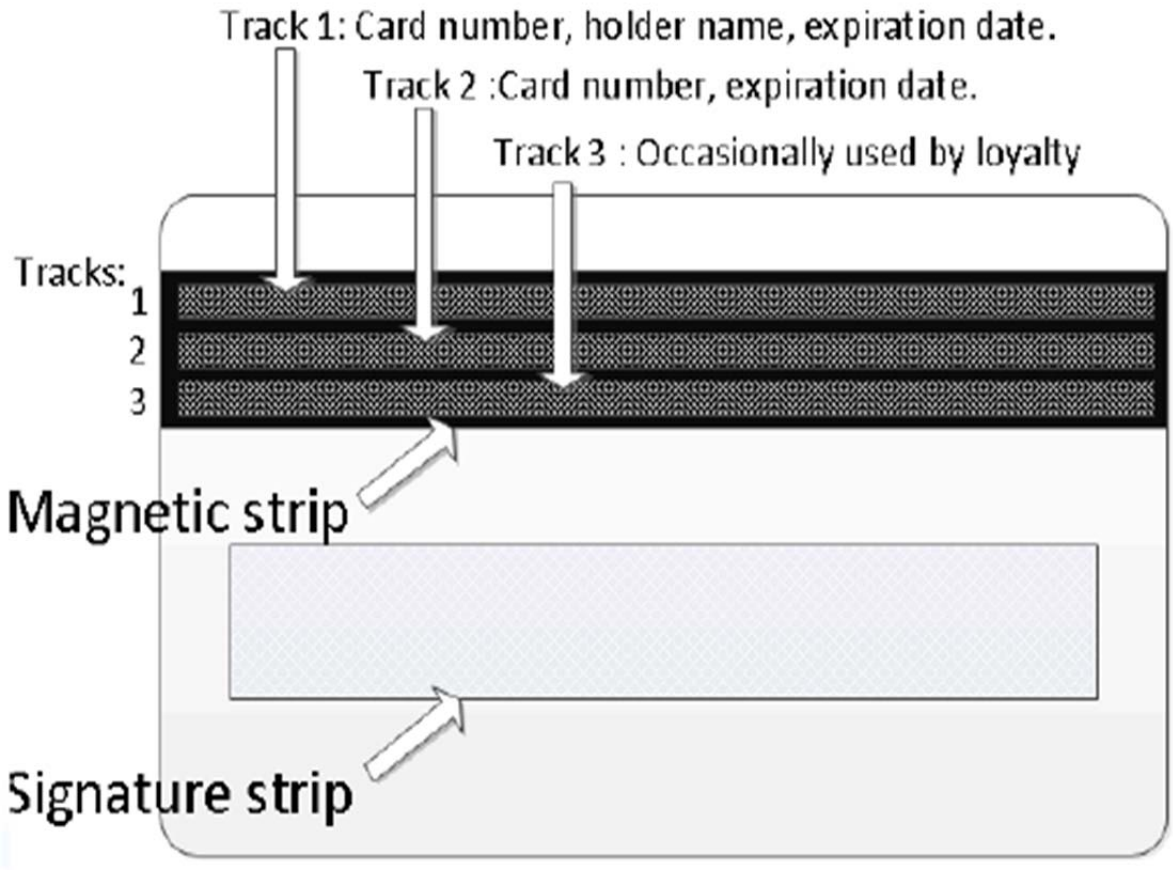

Figure 1[2]

The above picture is of a Magstrip which contains three tracks providing information as to the identity of the card holder. The first track has the card number, holder name and expiration date. The second track has the number and expiration date and the third track is used for loyalty programs.

That information is usually verified over the connection to the financial institution to make sure the member has enough in balance to pay for the purchase or the card has not been marked as stolen. The information in the strip is static, it doesn't change. The codes, the name and loyalty information are not dynamic and is the reason cards can be made using just the encoded information.

[2] Figure provided by LSC

Below is a figure for how EMV card differs.

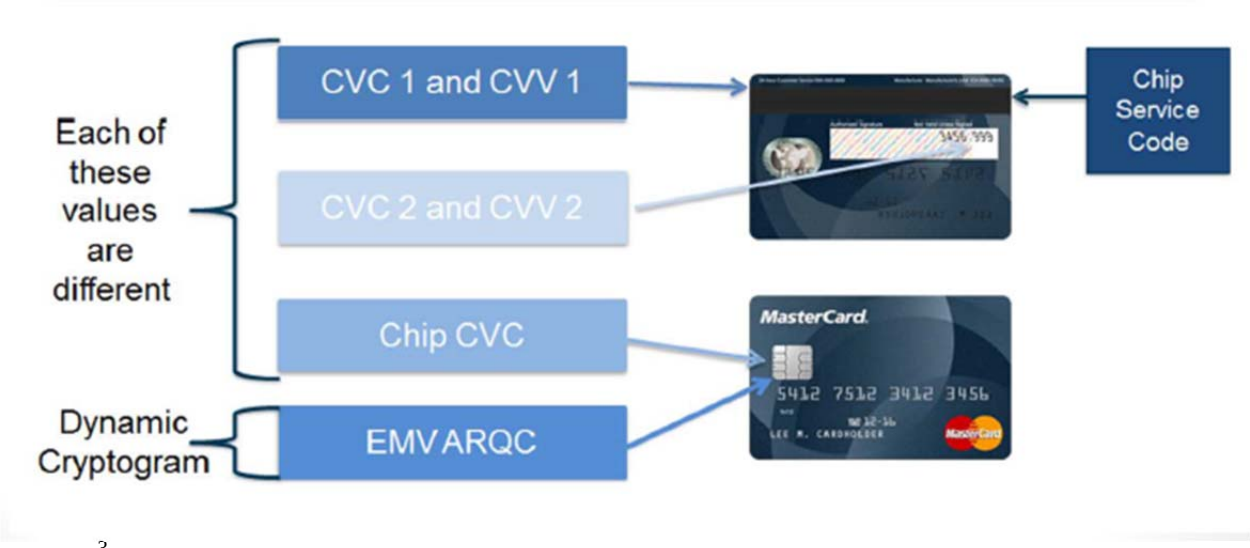

Figure 2[3]

On an EMV card, the same Magstrip information is included but there are added features. On the front is a Chip Card Verification Code that is encrypted. It transforms data to produce a digital signature that is used to verify the integrity of the data. It is capable of sending and receiving the information from the chip itself.

The card sends an Authorization Request Cryptogram (ARQC) online to the Issuer Host to confirm the chip is not counterfeit. The code is encrypted with a different key each time the card is used, which makes it impossible to duplicate because the counterfeiter would not know the encryption logarithm (Gray and Ladig, The Implementation of EMV Chip Card Technology to Improve Cyber Security Accelerates in the U.S. Following Target Corporation's Data Breach).

Once the card is inserted into a machine it is left in the terminal to perform all security functions, as opposed to how cards are handled now with the swipe and read method. With the card in the machine the technology takes over.

The card sends the ARQC through the terminal using a Dynamic Authentication Code. The terminal sends the EMV Transaction data over the network to the acquirer system. The acquirer system reads the data and decides the validity of it and passes it through the pipeline to the payment brand center, whether it be Visa, Mastercard, Discover or American Express. The brand will forward the information to the Issuer Authentication System where the card is decrypted and the information about the member is verified. It checks if the member has enough available funds for the purchase, if the card is legitimate and if the member's card has expired.

The Issuer's System sends an Authorization Response Cryptogram (ARPC) back to the Payment Brand either approving or declining the transaction. At this point, the decline can come from the credit union (for low balance) or from the Issuer (for stolen card or offline balances). When it reaches the Payment Brand, the transaction has either been approved or declined. The Payment

[3] Figure provided by Carolinas Credit Union League

Brand forwards the ARPC to the Acquirer system and then back to the terminal where it uses the card chip to decrypt the ARPC (Verhagen).

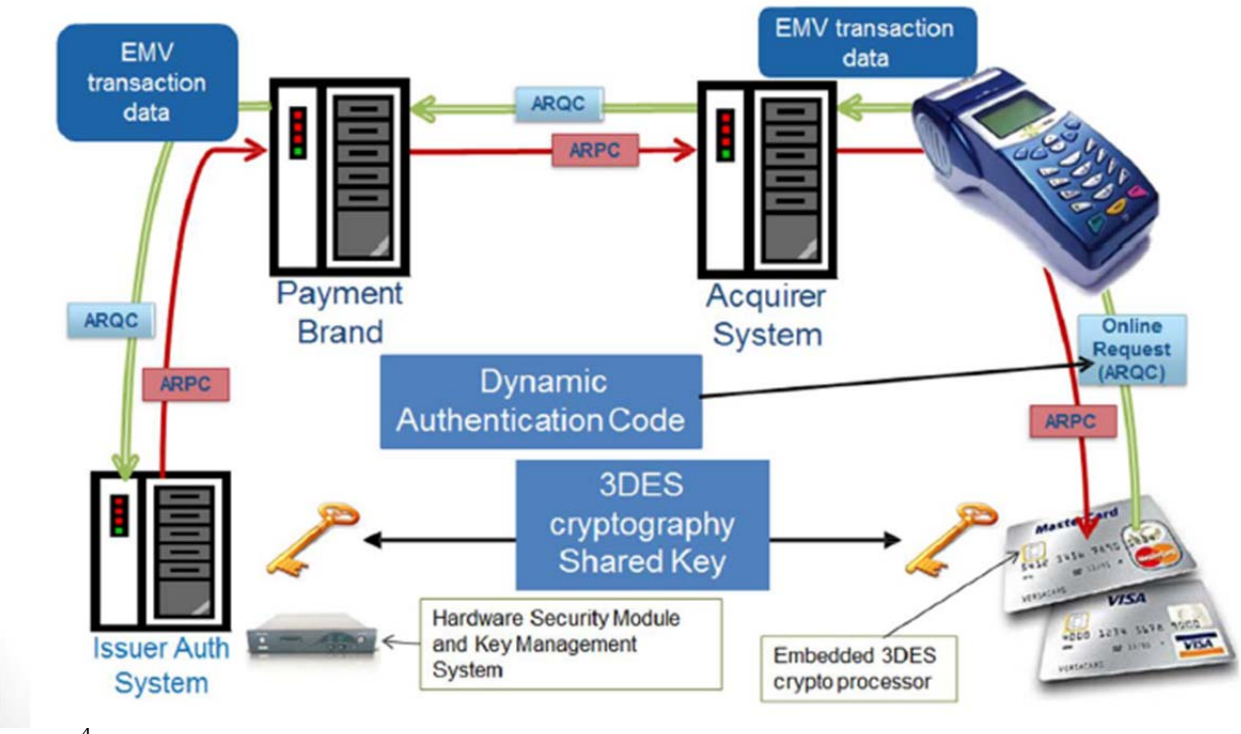

Figure 3[4]

The figure above illustrates the path that the EMV takes to approve debit/credit card transactions using EMV. The encryption is the key to the security; it provides information to the card and is controlled by the chip and it tells the terminal what type of card is being used. The dynamic code changes each use and if both the terminal and card are EMV it provides a way to combat counterfeit cards which is 37% of all fraud.

Difference between EMV and Magstrip

The technology in both the EMV and Magstrip is different, yet still the same in many ways. The Magstrip uses the name, card number and expiration date to send information from the terminal to the Issuer Authentication System. It reads from the first and second tracks, while EMV uses the chip to encrypt information that is stored on the chip and sends it over the same network. The end result is the same. Both return the decision based on many different factors. Does the member have enough money, has the member reached the daily limit, is the card marked stolen, does the transaction fall under any fraud rules, is the member authorized to use the card in the location. The difference in the two comes only in how the information is read.

The chip and terminal and the Magstrip and terminal work together to produce the information needed to approve or decline transactions. The card has security features such as expiration date and card numbers while the terminal uses the network to talk to the Issuer Authentication

[4] Figure provided by Carolina Credit Union League

System. The terminal is given Application IDs to use and the IDs are stored in the system. Each Payment Brand has its own AID. Logic and configuration is added to the terminal. This does not change in either EMV or Chip technology. Again the only difference is the encryption key that EMV uses. While the EMV Chip is dynamic, the Magstrip is static. This makes counterfeiting a card with Magstrip much easier because there are no changing parts. The Magstrip will have the same information every time and that information is stored in the terminal. In an EMV transaction the chip stores the information behind a dynamic code and it is not stored in the terminal.

How the Issuer Authentication System knows the difference

Each transaction is accompanied by CVC information, whether it is an EMV transaction or a Magstrip transaction. The Magstrip transaction has a three digit code that tells the system what type of transaction is taking place. It lets the terminal, acquirer system, payment brand and issuer system know that the information following is coming from a Magstrip track and will be decrypted.

The EMV has a different code that precedes the information and tells the network that an EMV transaction is coming. The code lets the terminal, acquirer system, payment branch and issuer system know the information will be coming from the chip and will be encrypted.

The code returns immediate input to the terminal for the person using the card to follow. If a person were to swipe a card that is EMV the terminal let's that person know right away that the card needs to be dipped or inserted and left alone. In this case, it is part of the CVC that is providing that information.

How the Credit Union and Members knows the difference

Other than the credit union already knowing that EMV cards are out and looking for certain CVC information, there isn't much for the credit union to see when a transaction happens. The transactions are handled by the issuer payment system, and unless the credit union handles the payment infrastructure without help of a third party there isn't much for the credit union to see any different. The connection to the issuer allows balance and other validating information to be sent.

There is a slight difference in the way the traffic flows through the network, but is usually handled by routers placed on the network of the credit union and may require a certain port to be opened on the firewall. Usually that is handled early on the in the conversion process and isn't something that needs to be done more than once.

The member on the other hand notices the difference because it is no longer just a swipe and go. They are required by the CVC to insert the card and leave it in place. This is a change to many members and can lead to some confusion.

Why this Technology Matters

The difference between Magstrip and EMV is the chip and the way the network handles transactions. The path that EMV takes can slow transactions for members, but it also provides a higher form of encryption.

Encryption is a way of making information private. There are laws set to handle credit/debit card privacy but criminals do not follow the law which means the only way to protect members and the credit union is to keep fraudsters from getting the information.

Encryption on the chip takes the data that is usually found on the Magstrip and makes it unrecognizable. The only way to decrypt the information is to know the key. Knowing the key makes decrypting information a breeze, but criminals will not be able to get the key because it changes with each use. A 256-bit key provides the possibility for 2^{256} possible keys. That's so many combinations of keys that today's modern computers could never crack the key. It is estimated that 256-bit encryption could be cracked by a computer in the next 192 years (Verhagen). Then add to the equation that key is dynamic and changes every use and it is an impossible task to crack.

The technology of EMV is complex, but needs to be because criminals have become complex as well. The Magstrip no longer provides an uncrackable way to protect member's data. Like all technology there are tradeoffs that need to be taken into consideration.

VI. RECOMMENDATIONS

As credit unions consider whether or not EMV is worth the cost, there are many pros and cons that are worth considering.

Pros

The card targets counterfeit cards which is the largest portion of crime against members' debit/credit cards. The technology provides an easy way to stop criminals from profiting from the member. Criminals are high-tech but they do not have the capability to break 256-bit encryption.

It also protects from human negligence on the merchant side. In an article released in April 2015 Jose Pagliery of CNN Money reported that 90% of credit card readers use the same password for accessing supervisor mode. He reported that the code was the same since the 1990's and was 166816 or Z66816 depending on the machine (Pagliery). The machines go through so many channels to be sold that nobody stops to change the master code, so thieves can use the machine type and an internet search to find the default master code. They can then infect machines with malware to steal information. EMV would protect against that type of attack. They would have an old code but the code would be changed by the time of use.

Credit unions would then save on the fraud. Currently, the fraud is at an all-time high (Wilson). Ten percent of Americans have been victims of credit card fraud in the last year ((Statistic

Brain). The median report of fraud is $399. For a small credit union with 10,000 members that could mean almost $400,000 in fraud losses.

EMV technology will bring the United States financial institutions into the worldwide standard as well as stop fraud. The technology has been around for over 20 years and has been a success in the other countries that have used it. It is the reason that America has seen an increase in fraud and why it has seen a 21% increase in fraud in the last 8 years (Statistic Brain).

Another pro can be traced back to member marketing. With new cards, there are new ways to advertise. The card will last longer which is a desired feature to members. It opens a dialogue with membership and gives a reason to send a letter or insert and allows for advertising without looking like an attempt to advertise.

Cons

With all the pros and the threats of fraud, there is one question that needs to be asked. Why would it take a liability shift and other mandates by the payment brands for EMV to finally take root in the United States?

The number one deterrent was the price of changing for both the merchant and the financial institution. In **Appendix A,** there is a sample expense estimate for Georgetown Kraft Credit Union. On the estimate it lists the different functions that have to happen during each process of the EMV conversion.

The one-time fees such as BIN Redefinition, EMV Bin Set-up, Reissue Project, Reissue Files, Database Change, and other functions were $8,000. The price of the plastic stock itself was $15,859.81. Add on shipping, embossing and PIN mailing the cost rose to $16,359.81. After the other project related expenses were added, the total cost to convert came in at $53,811. That was on a card base of just 11,000 cards which is roughly $5.40 per card.

Some credit unions had larger bases and had higher expenses, but even a smaller base around 5,000 cards would be paying $27,000 to upgrade a program that was working. Even with fraud factored in, credit unions don't pay that much in recovery each year. Georgetown Kraft Credit Union had a total of $25,000 in fraud in the year 2014, not even half of what the cards cost to convert.

Table 6 (on page 9) shows that fraud from counterfeit cards, which is what EMV technology is targeting, is declining while card not present (CNP) fraud is rising. While card fraud is going up, the one thing EMV hopes to eliminate is going down. This could be attributed to EMV or to the ease of CNP fraud.

Converting also adds to employee frustration as the project has to be run by a project manager at the credit union and some processes have to be changed and upgraded along the way. It is a time consuming project, most taking 6 to 8 months to complete. Plus, with more credit unions doing it at once, there is a back-log order for plastics with chips to complete the process. This adds time to an already long process.

Add to it member frustration and the ease of use. Magstrips are easy to use as they just swipe and go, but EMV cards are put into the machine and left. Many members aren't aware of the new process and pull the card out the minute it is stuck into the machine. Members don't realize that leaving the card in the machine is the only way the chip can decrypt the message coming back from the issuer. This can sometimes make them feel like the card isn't working and the transaction is taking much longer than normal.

The transactions do take longer. There is no longer information just stored on the card. It is encrypted and has to be decrypted through the process discussed in Figure 3 on page 13. This slows the transaction down and while it is reported as around 15 seconds, overtime that adds up.

In addition, there is a change in the technology infrastructure. Most of that is handled by the credit card/debit card vendor. Still there are a small number of changes in the credit union firewall (ports being opened up) and sometimes even the computers the employees use to order cards (new styles are added and other website functions) will need some configuration changes.

If the credit union gets overcomes these frustrations there is still the possibility that the area the credit union services are not compliant. While the card is backwards compatible (meaning the Magstrip on it can be used), it hardly is worth the price if all the merchants are not using the technology. This was handled some with the liability shift but it could still mean some members could be declined because of the merchant machine returning a wrong code.

There is also the uncertainty of the new technology to produce the results it promises. Some credit unions believe it doesn't work and that there will still be counterfeit fraud and the liability shift only handles one type of specific fraud. This leads to them not upgrading out of concern that they would be using the money for no reason. These are some of the concerns that are raised at each credit union board meeting whenever EMV is brought up.

Do the Pros Outweigh the Cons

EMV is here to stay and has been around for decades. It has a proven track record and the technology is unbreakable. But the cost and ease of use raise serious issues for those who are going to upgrade and gives a good starting point for those who oppose. With such a proven track record the pros do outweigh the cons.

EMV is costly but it is effective. Along with tokenization, fraud could be eliminated down to lost/stolen and some card not present fraud. Lost/stolen fraud could even be eliminated by mandating chip & PIN technology instead of chip/signature. The pros have been proven numerous times in Europe for many years and even through projections in the United States in the next 2 years.

VII. CONCLUSION

If we, as a group, were running a credit union would the cost of EMV be worth the benefit?. After researching and seeing the track record, we agree that it would be worth it.

Criminals are not going away. The fraudsters are ever changing and the price of doing business in a financial setting is spending money to protect our members from every risk possible. EMV does just that. It is costly, and it adds a workload on back office employees but credit unions have always had to adjust for security reasons. This is just one more weapon credit unions have in combating fraud and protecting members. Which is something everyone can agree is needed.

Final Word

Each team member learned something new from doing the research and weighing out what their credit union would do. The group also came up with a collective agreement that is discussed below each individual's thoughts on the project. Here is each of their thoughts:

Allison Beckham-

While researching this topic the history of fraud stood out to me. Fraud has evolved throughout the years due to the efforts of financial institutions trying to stop it. Each time a new procedure or technology was put in to place to stop fraud, criminals were able to change their practices to continue their schemes. This proves that EMV is needed to limit card-present fraud in the US, as it has in other countries.

Robyn Blaylock

Prior to researching this topic, I had no sufficient knowledge as to what EMV really was or the benefits it could bring to credit unions. After examining crucial facts and its proven history, I believe the pros far outweigh the cons. There's no denying that EMV is costly. However, in my opinion, it will be more costly for credit unions not to implement it. As with any change, some people do not embrace it as well as others. Given time and education, my hope is that members will accept that it is an added benefit to them that will provide safety and additional security. Protection against fraud is a top priority and upgrading to EMV is a necessity I believe every credit union should provide to their members.

Tina Farris

This project has truly enlightened me on the differences between the magstrip cards and EMV chip cards. The new technology with EMV has the potential of creating a new safer way for consumers to carry out their day to day transactions without fear of fraud.

Scammers are constantly trying to find new ways to steal money. As the financial industry continues to progress into the 21st century, the EMV card is a huge step into the right direction for consumers. The initial implementation cost to the industry is huge; but overall, the impact will minimize fraud losses for consumers and financial institutions.

As technology continues to grow, it will be important for the financial industry to continue investing and developing new ways to stay ahead of the criminals. The EMV chip card is a step in the right direction.

Kevin Langford

I came into the project having gone through the converstion already and saw a lot of the trouble first hand. I was at the point where I thought it wasn't going to be worth all the hassle until I started the research and found all the ways it could help. Seeing the technology in action was very enlightening to me and I felt that as the technology grows so should our credit union. This project helped me see that and I'm glad to have been part of it.

Group Thoughts

In this paper, there was a lot of research done into what EMV means and how it works. It led to many discussions as to what a fictional credit union would do to protect its members. There were arguments on both sides of the fence but in the end thinking of breaches and other ways fraudsters hurt our members led us to the conclusion that upgrading was worth the cost. The liability shift helped and was one of the biggest deciding factors when it came to upgrading. If not for the shift, the cost of the conversion would have been too much for the benefit of the program. In the end the shift was the reason most credit unions have decided upgrading was beneficial. Maybe it will end up helping our members move towards less worry when using the cards. We know that EMV is helping our troubled minds.

VIII. APPENDIX A (SAMPLE COST ESTIMATOR)

Georgetown Kraft CU

March, 2015

Debit - Mass Reissue EMV Expense Estimate

	Quantity	Rate	Billing Amt.	Notes
ONE-TIME AND RE-ISSUE PROJECT EXPENSES				
Project Expense - BIN Redefinition	1	$2,000.00	$2,000.00	Includes Debit EMV BIN Re-definition project
EMV Per BIN Setup	1	$1,500.00	$1,500.00	$1,500 per BIN - Program.
Reissue Project	1	$2,500.00	$2,500.00	Bundled project cost for Network paperwork processing, Msg. format changes, 2 Database Entry files - and up to 15 hours of certification per project.
Reissue Files	1	$2,000.00	$2,000.00	Pricing per wave of re-issued plastics.
Database Change	0	$300.00	$0.00	Per BIN, per database change beyond the first 2 included in the Reissue Project above.
Card Associations Fees and Licensing	1	Varies	Quote	Based on business requirements and specific to Brand issued.
Visa Custom Profile (Offline)	0	$25,000.00	$0.00	Assume a single profile applied to VISA BIN(s). Charged directly by Visa. Per BIN.
MasterCard Key Exchange Fee	0	$1,700.00	$0.00	Charged directly by MasterCard.
FIME Testing	0	$1,500.00	$0.00	If applicable.
Additional Online Certification with Data Processor	0	$125.00	TBD	Only applicable after 15 hours of certification.
EFT Network - Files, Personalization	1	Varies	Quote	If applicable.
SUBTOTAL ONE-TIME AND RE-ISSUE PROJECT EXPENSES			*$8,000.00*	
MASS REISSUE EMV PLASTICS				
VISA Debit Plastics*	11,000	$1.4418	$15,859.81	Per unit based on purchase of 11k custom plastics.
Select Program Plastics*	0	Quote	Quote	
Select Program Plastics*	0	Quote	Quote	
Select Program Plastics*	0	Quote	Quote	
Select Program Plastics*	0	Quote	Quote	
Select Program Plastics*	0	Quote	Quote	
Select Program Plastics*	0	Quote	Quote	
Select Program Plastics*	0	Quote	Quote	
Select Program Plastics*	0	Quote	Quote	
Plastics shipping/freight to warehouse	1	$500.0000	$500.00	Shipping to warehouse facility. Assumes orders will be shipped together.
Digital Plastics Base Setup Fee	0	$350.0000	$0.00	Charge per plastic type setup for digital plastics.
RFID Chip	0	$1.90000	$0.00	Optional. For clients electing contactless/Dual Interface.
Chip Encoding	0	$0.65000	$0.00	Optional. For clients electing contactless/Dual Interface.
SUBTOTAL MASS REISSUE EMV PLASTICS			*$16,359.81*	
CARD REISSUE RELATED EXPENSE				
EMV Cards Embossed	9,027	$1.750	$15,797.25	Estimated volumes. Embossing charge.
PEP Card Carrier	9,027	$0.12500	$1,128.38	Estimated mailers based on number of accounts.
EMV Machine Setup	1	$3.000	$3.00	Charge for each time embossing machine is set-up.
Card Mailer Postage	9,027	$0.490	$4,423.23	Pass-through of USPS postage fees.
PIN Mailer Postage	0	$0.490	$0.00	Pass-through of USPS postage fees.
Mail Integration	9,027	$0.04718	$425.89	
Inserting Setup	0	$2.116	$0.00	Optional, for inserts with plastics. Frequency - per day.
Card Activation - IVR	7,222	$0.750	$5,416.20	Estimated volume based on average activation rates.
PIN Now	2,257	$1.000	$2,256.75	Per PIN change. Assumes 25% will change PINs at reissue.
SUBTOTAL CARD REISSUE RELATED EXPENSE			*$29,450.70*	
TOTAL ESTIMATED EXPENSE**			**$53,811**	
EMV AVERAGE PER CARD EXPENSE***			**$5.40**	
ESTIMATED FIRST YEAR NATURAL REISSUE EXPENSE******			**$30,905**	
OTHER RECURRING EXPENSE				
EMV Chip Verification Transaction (Annualized)	508,809	$0.0050	$2,544.05	Authorization charge for each completed EMV authorization. Assumes 25% of transactions to process EMV based on gradual merchant adoption.

Application Transaction Counter Validation (Annualized)	508,809	$0.0050	$2,544.05	Recommended transaction counter, maintained by the chip card application (incremented by the chip), that provides a sequential reference to each transaction. Assumes 25% of transactions to process EMV based on gradual merchant adoption.
EMV Chip Scripting	TBD	$0.0020	TBD	Future enhancement for Debit. Any instance that scripted data is passed back to the chip during a transaction. Will only apply to a fraction of EMV processed transactions.
MasterCard Per Transaction	TBD	$0.010	TBD	Based on each CU's individual volume.
ESTIMATED DIFFERENCE IN ANNUAL EMV PROCESSING EXPENSE			**$5,088**	
*Plastics costs are based on design specifications and quantity ordered. The example above assumes a basic 8 color plastic; unit cost may be higher or lower depending on design specifications.				
**Assumes mass-reissue expense excludes "Other Recurring Expense" section.				
***Excludes "Other Recurring Expenses".				

IX. APPENDIX B (AUTHORS)

Allison Beckham

After growing up in a credit union home where “banks are bad” was imprinted in her head, Allison Beckham began working at ArrowPointe Federal Credit Union in 2009. She started, like most, as a teller while she completed her Associates in Accounting. She quickly moved to the position of Senior Teller and then Member Service Representative while completing her Associates in Management. It was as a MSR that Allison realized that everyone did not have the same financial education as she did growing up. She grasped how easy it could be for unknowing individuals to fall in to the cycle of payday lenders or big bank fees. It was then that she became an advocate for the Credit Union movement. In 2013, Allison was promoted to Loan Officer and then in 2015 to Branch Manager. She began training her branch staff to promote the Credit Union movement alongside her and has seen substantial growth in her small branch. She hopes to continue the growth of her branch, as well as the entire credit union, to educate their underserved community.

Robyn Blaylock

Robyn Blaylock is employed at Monroe Telco Federal Credit Union, located in West Monroe, La. She started with the credit union in 1997 as a part-time receptionist while she attended school at Northeast Louisiana University. Shortly after, she moved to the Teller Department full time. It was there that she discovered a passion for the credit union philosophy of "People Helping People." As time has passed, she has experienced working in the Collections Department, Loan Department and was the Marketing Manager for several years. These positions have led her to where she has been working as a Branch Manager for the past three years. As she embarks on her seventeenth year with the credit union she calls home, she hopes her leadership skills will allow her to help evolve Monroe Telco into her community's primary financial institution.

Tina Farris

Tina Farris is 43 years old and lives in Clover, SC with her husband Frank and son Bradley. She loves the small town atmosphere and the sense of security in knowing many of the residents there.

During the ten years she has been employed with Family Trust, she began as a part-time teller, moved to audit and compliance, then changed positions to be back in the branch. She has been in every position within the branch; teller, member service, lender, and assistant manager. She voiced her career goals to her manager which allowed her the opportunity to receive the training and experience to continue her career progression. She is now the Branch Manager at Clover.

As a branch manager, she is excited to be continuing her mission to encourage, support, train, mentor, and empower her employees. She wants each of them to feel the sense of success that she feels every day in knowing that they are important and valued as a person and employee.

Kevin Langford

Kevin Langford is the IT Director at Georgetown Kraft Credit Union. He has been with the credit union for 6 years. He started in the United States Navy and moved into a Law Firm. In the Navy is where he was trained in Networking and Computers. He has a Bachelor of Business Management from University of Phoenix and 4-year technical certification from the Navy.

He is married with 3 kids. He plans on staying with credit unions because he loves their mission of helping members. He leads all project management as his credit union including the EMV conversion.

X. WORKS CITED

EMVCo. n.d. 08 August 2015 <http://www.emvco.com/about_emv.aspx>.

Foundation, Wikimedia. Wikipedia. n.d. 7 August 2015 <https://en.wikipedia.org/wiki/EMV#History>.

Gray, Dahli and Jessica Ladig. "The Implementation of EMV Chip Card Technology to Improve Cyber Security Accelerates in the U.S. Following Target Corporation's Data Breach." IJBA International Journal of Business Administration (2015): 6-12.

—. "The Implementation of EMV Chip Card Technology to Improve Cyber Security Accelerates in the US Following Target Corporations Data Breach." International Journal of Business Administration (2015): ALL.

Javanovic, Vladimir. CUInsight. 24 July 2015. 24 August 2015 <https://www.cuinsight.com/emv-101-understanding-the-new-landscape.html>.

Medich, Cathy. "Understanding the 2015 U.S. Fraud Liability Shifts." 01 May 2015. EMV Connection. 1 August 2015 <http://www.emv-connection.com/downloads/2015/05/EMF-Liability-Shift-Document-FINAL5-052715.pdf>.

Miller, Phillip, et al. "EMV for US Acquirers: Seven Guiding Principles for EMV Readines." US Insights (2012): 1-12.

Pagliery, Jose. CNN Money. 29 April 2015. 1 August 2015 <http://money.cnn.com/2015/04/29/technology/credit-card-machine-hack/index.html>.

PSCU. EMV Whitepaper. October 2014. 01 August 2015 <http%3A%2F%2Fwww.pscu.com%2Fcontent%2Femv-whitepaper.html>.

Statistic Brain. n.d. 28 February 2016 <http://www.statisticbrain.com/credit-card-fraud-statistics/>.

Statistic Brain Research Institute. 12 July 2014. 27 February 2016 <http://www.statisticbrain.com/credit-card-fraud-statistics/>.

The Fraud Practice. n.d. 1 August 2015 <http://www.fraudpractice.com/fl-fraudhist.html>.

uSwitch. uSwitch. n.d. 07 August 2015 <http://www.uswitch.com/credit-cards/guides/credit-card-fraud-the-biggest-card-frauds-in-history/>.

Verhagen, Vincent. "The Making of Europe by Payment Cards." PhD Thesis. 2015.

Wilson, Michelle. Cam Blong. n.d. 1 January 2016 <http://camblog.topssoft.com/bid/324260/With-Fraud-at-an-All-Time-High-Secure-Checks-Help-Deter-Fraud-Detect-Tampering>.