Assembly Banking and Finance Committee

Innovation and Transformation in Payments Technology

March 16th, 2015
1:30pm,
California State Capitol, Room 444

BACKGROUND

Overview

The U.S. remains the last developed country reliant on magnetic stripe credit cards (mag stripe), a four-decade old technology. The U.S. is currently on pace to be a full decade behind Europe on the implementation of credit card chip & PIN technology (EMV-Europay, MasterCard, Visa standard). Currently, all face-to-face credit or debit card transactions use a magnetic stripe to read and record account data, and a signature for verification. Under this system, the customer hands their card to the clerk at the point of sale, who "swipes" the card through a magnetic reader. The merchant transmits to the acquiring bank the cardholder's account number and the amount of the transaction. The acquiring bank forwards this information to the card association network requesting authorization for the transaction and the card association forwards the authorization request to the issuing bank. The issuing bank responds with its authorization or denial through the network to the acquiring bank and then to the merchant. Once approved the issuing bank sends the acquiring bank the transaction amount less an interchange fee. This process occurs in a manner of seconds.

This system has proved reasonably effective, but has a number of security flaws, including the ability to get physical access to the card via the mail or via the use of black market card readers that can read and write the magnetic stripe on the cards, allowing cards to be easily cloned and used without the owner's knowledge. The inherit convenience of mag stripe cards is also their inherit weakness.

The terminology and process of a credit card transaction:

Acquirer- A bank that processes and settles a merchant's credit card transaction with the help of a card issuer.

Authorization- The first step in processing a credit card. After a merchant swipes the card, the data is submitted to merchant's bank, called an acquirer, to request authorization for the sale. The acquirer then routes the request to the card-issuing bank, where it is authorized or denied, and the merchant is allowed to process the sale.

Batching- The second step in processing a credit card. At the end of a day, the merchant reviews all the day's sales to ensure they were authorized and signed by the cardholder. It then transmits all the sales at once, called a batch, to the acquirer to receive payment.

Cardholder- The owner of a card that is used to make credit card purchases.

Card network- Visa, MasterCard or other networks that act as an intermediary between an acquirer and an issuer to authorize credit card transactions.

Clearing- The third step in processing a credit card. After the acquirer receives the batch, it sends it through the card network, where each sale is routed to the appropriate issuing

bank. The issuing bank then subtracts its interchange fees, which are shared with the card network, and transfers the remaining amount through the network back to the acquirer.

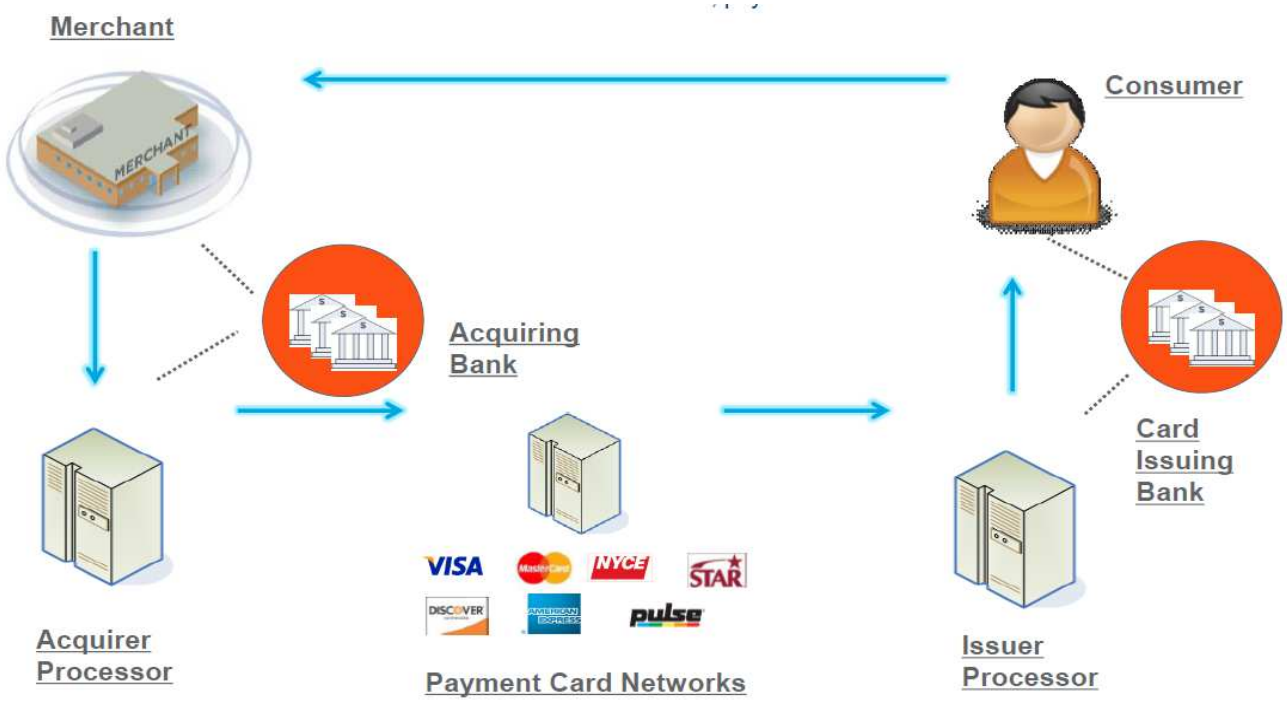
Discount fee- A processing fee paid by merchants to acquirers to cover the cost of processing credit cards.

Funding- The fourth and final step in processing a credit card. After receiving payment from the issuer, minus interchange fees, the acquirer subtracts its discount fee and sends the remainder to the merchant. The merchant is now paid for the transaction, and the cardholder is billed.

Interchange fee- A charge paid by merchants to a credit card issuer and a card network as a fee for accepting credit cards.

Issuer- A financial institution, bank, credit union or company that issues or helps issue cards to cardholders.

Chart: Overview of Typical Credit Card Transaction[1]



Highlights from the *2013 Federal Reserve Payments Study Detailed Report*

[1] Provided by First Data.

- Credit cards are more prevalent than other general-purpose card types. Of the 776 million general purpose cards in force (issued, activated, and not expired) nationally in 2012, 334 million were credit cards, 283 million were debit cards, and 159 million were prepaid cards. Consumers held the majority of general-purpose credit cards - 10 times the number held by businesses (305 million and 28 million, respectively).

- Among general-purpose cards with purchase activity in 2012, consumers preferred debit cards, with an average use of 23 payments per month, compared with an average of 11 payments per month for general-purpose credit cards and 10 payments per month for general-purpose prepaid cards.

- Although the number of ATM cash withdrawals using debit cards and general-purpose prepaid cards dropped slightly, growth in the value of ATM withdrawals continued to exceed inflation over the years. New information on over-the-counter cash withdrawals shows that while the number of ATM withdrawals (5.8 billion) far exceeded the number of over-the-counter withdrawals (2.1 billion) in 2012, the average value of over-the-counter withdrawals, at $715, far exceeded the average value of withdrawals at ATMs ($118).

- In 2012, there were 1 billion ATM cash deposits with an average value of $374, compared with 1.6 billion over-the-counter cash deposits which averaged $1,000.

- Not surprisingly, businesses, not consumers, are the overwhelming users of wire transfers. There were 287.5 million wire transfers—including those sent over large-value funds transfer systems and those made on the books of depository institutions in 2012, with a value of $1,116.3 trillion. Consumers accounted for just 6 percent of all wire transfers by number and 0.14 percent by value. Business customers accounted for the significant majority of both the number and value of wire transfers.

- The number of online bill payments reported by major processors, which included those initiated through online banking websites and directly through billers and settled over ACH, exceeded 3 billion in 2012. Secure online payments, including methods that allow users to enter personal identification numbers (PINs) for debit cards into the computer or that redirect users to use an Internet payment account, totaled more than 1.8 billion in 2012.

- There were more than 250 million mobile payments made using a mobile wallet application, and at least 205 million person-to-person or money transfer payments.

- The number of private-label prepaid transportation payments exceeded all other prepaid card payments combined in 2012: Payments by prepaid transit cards and far-field radio frequency identification (RFID) transponders for auto tolls had reached a combined 9.9 billion payments.

- Checks continue to be written less frequently - more than 90 percent of the decline in total checks was due to reductions in checks for $500 or less, and 45 percent was from reductions in checks for $50 or less.

- As of 2012, there were 287 million consumer transaction accounts with an average value of $8,001, while 33 million business transaction accounts averaged almost $62,000. Meanwhile, there were almost 280 million consumer credit card accounts and almost 29 million business accounts. Credit card balances, which included both current spending and revolving credit, averaged $1,900 for both consumer and business accounts.

EMV: Chip Cards

The U.S. has over 10 million credit card terminals and 1.2 billion credit cards, with less than 2% of cards having chip technology according to the Smart Card Alliance. Annually, credit card fraud equals $11 billion globally, with the U.S. portion amounting to $4.73 billion.[2] The Nilson Report, a credit card industry newsletter, points out that the U.S. accounts for just over a quarter of the global volume of credit card transactions per year, yet accounts for almost 50% of the fraud worldwide.

Credit card chip technology was established in 1994 by Europay International SA. This chip technology is also called EMV, as it was named after its original developers, Europay, MasterCard® and Visa®.

EMV technology is used today in more than sixty countries outside of the U.S. with worldwide usage at 40% of the total credit cards and 70% of the total terminals based on the EMV standard.[3]

A cardholder's data is more secure on the chip-embedded card than on a mag stripe card. Chip-embedded cards support superior encryption and authentication as opposed to mag stripe card making the data on mag stripe cards easier to obtain via fraudulent means. Chip technology counters the static nature of mag stripe cards by implementing technology that creates dynamic values for each transaction in the form of a different verification code

[2] Saporito, Bill. "The Little Strip on Your Debit Card is a Massive Achilles's Heel," Time.com. Jan. 23, 2014

[3] First Data, EMV in the U.S.: Putting It into Perspective for Merchants and Financial Institutions. http://www.firstdata.com/downloads/thought-leadership/EMV_US.pdf

for each transaction. EMV cards can be used both online and in face-to-face transactions, both supporting signature and PIN verification with PIN being the dominant method used in Europe. However, while the EMV cards can complete online transactions, those transactions do not have the same level of security as provided by the chip in the face-to-face transaction. In the online scenario the consumer still enters their card data to complete payment with the addition of a PIN. Currently, several European payment technology companies are working to bring the Chip & PIN protection to online transactions.

EMV compatible cards come in three forms. A chip embedded card is inserted into the Point of Sale (POS) terminal and the consumer enters their PIN or uses a signature to complete the transaction. The other way to pay is via contactless cards in which the transaction occurs when the consumer swipes their card within the appropriate distance of the POS terminal that can read the radio frequency identification device (RFID) on the card. The third type of card is a hybrid chip card that allows for both contact and contactless transactions.

As previously mentioned, the U.S. has lagged behind in the implementation and acceptance of EMV technology. The first U.S. credit card utilizing EMV was issued by United Nations Federal Credit Union (UNFCU) in October of 2010. The primary reason UNFCU issued the card was that many of its members reside outside the U.S. and were in need of a globally accepted card. Outside of the U.S. mag stripe cards are becoming less accepted. Prior to last year's large scale data breaches, most large card issuers in the U.S. (Wells Fargo, JPM Chase, and U.S. Bancorp) have begun to migrate some of their portfolios over to EMV cards, but in limited quantities and targeted toward higher income card holders or those that frequently travel to European countries. Subsequent to last year's data breaches, several financial institutions replaced cardholder's magstripe cards with EMV cards if they were amongst the millions that had their payment data compromised.

On August 9th, 2011 Visa announced an accelerated implementation to EMV technology and established October 1, 2015 as the date when card-present counterfeit fraud liability will shift from issuers to merchant acquirers if fraud occurs in a transaction that could have been prevented with a chip-enabled payment terminal.[4] While the announcement lays a path towards EMV chip card migration, it does not necessarily set a path to chip-and-PIN as Visa will continue to support both signature and PIN cardholder verification methods. The announcement specified incentives and deadlines to urge U.S. merchants to accept both contact and contactless chip-enabled cards. One merchant incentive includes the elimination of the requirement for annual card network compliance validation if 75% of a merchant's transactions originate from chip-enabled terminals. For the largest merchants, savings from an annual compliance validation would average approximately $225,000 a year. Some industry analysts conclude that only 60% of U.S. POS terminals will meet the target date.

[4] Press Release available at http://corporate.visa.com/newsroom/press-releases/press1142.jsp

The history of European adoption of EMV also took a different course and was instigated for varying reasons, many of those different than the current debate in the U.S. American payments model has been very efficient through the verification of transactions from POS over land line phone lines. In Europe, the inefficient telephone system used for verification, created pressure for card networks to create a secure and localized payment transaction system.

The impact of EMV in the United Kingdom was a large reduction in payment card fraud of 40% since 2000, however the U.K. Payments Administration claims that the failure of the U.S. market to adopt EMV has impacted the U.K. market as counterfeit fraud increased because criminals would copy data from stolen U.K. cards and would in turn use the stolen cards in countries with chip and PIN.[5]

Even in Europe where EMV is over a decade ahead of implementation in the U.S. EMV does not protect against all threats. EMV does not exist for card not present transactions such as online transactions or over the phone, and is unable to protect payment data downstream in the payment process once it has left the POS terminal. Statistics for the U.K. and other EMV countries demonstrate that criminals follow the path of least resistance as fraud migrated away from attacking the card present transaction to target transactions such as online banking, online shopping, mail, and phone orders.[6]

EMV is but one step of a multi-layered approach to payment security. Julie Conroy, a senior analysts and fraud expert with Aite Group has stated that the attacker's malware in the Target breach would have penetrated the payment system regardless of what cards were used by consumers.[7] EMV would have prevented the ability of fraudsters to make duplicate cards via stealing data at the POS terminal, but it is very unclear whether it would have prevented the Target and Neiman Marcus breaches specifically. However, EMV would make it difficult for criminals to use the information acquired from a breach to make fraudulent cards.

Obstacles for EMV Implementation:

A factor that contributed to the limited role out of EMV in the U.S. is was that few merchants accept EMV chip-embedded cards and the transition is both costly for issuers and merchants. Most EMV chip cards issued abroad and in the U.S. also contain a mag strip thus allowing acceptance at all U.S. merchants that accept credit cards. Also, up until the recent headline generating data security lapses, most American consumers were unaware of EMV technology or retailers that had EMV capable POS terminals.

[5] First Data, 7
[6] Ibid, 11
[7] *Why Target's CEO Changed His Mind About EMV*. American Banker. January 21, 2014

According to a First Data report on the implementation of EMV the estimated total costs could be around $8 billion.[8] The costs to financial institutions to issue mag-stripe cards costs as little as 10 cents each, whereas EMV cards can cost up to $1.30 each.[9] Estimates on the costs vary in terms of production and issuance to the customers, but some estimates find that EMV cards could cost, per card, as much as $10-$15 more than existing mag-stripe cards.[10] The Aite Group estimates that the implementation of EMV cards could cut fraud losses in half in the U.S. According to the Nilson Report, U.S. Merchants and banks had 2012 losses of $11.5 billion due to credit card fraud or about 5 cents on every $100 spent and will rise to over $12 billion by 2015.

As mentioned previously, some estimates find that only 60% of businesses will meet the October, 2015 EMV deadline. This means that even during initial phases the marketplace will still have a fair share of mag-stripe cards and EMV capable cards will also still include mag-stripes so that consumers are still able to use their cards at non-EMV compatible merchants. The story of the Netherlands adoption of EMV is telling as they began their transition to EMV in 2007 with a target completion date of 2010. This allowed magnetic stripe cards to stay in the market longer than most other European countries. During the transition, criminals targeted the remaining magnetic-stripe terminals and in 2011 there were 555 successful skimming attacks on payment terminals, up from 176 in 2010.[11] In a telling example of the potential issues that can occur with a transition to EMV, PayPal President David Marcus reported that on a recent trip to the U.K. his EMV enabled card was compromised.[12]

The European experience demonstrates that fraud shifts to the weakest links in the payment system during a transition to EMV. In what may be a controversial statement on EMV, a report from the Federal Reserve Bank of Kansas City finds:

> *Fraud for card-present transactions on lost or stolen cards may stay the same or even potentially increase. Many countries that use EMV payment cards do not allow cardholder authentication with signatures. Issuers in the United States, however, appear likely to continue to allow signature authorization on EMV debit and credit card transactions (Heun; Punch). As a result, fraud on lost or stolen cards may not decline in the United States. Fraud may even rise as fraudsters, unable to commit fraud on counterfeit cards, begin to target payments with relatively weak security, such as*

[8] First Data, 13
[9] *The Economics of Credit Card Security*. Washington Post. January 21, 2014.
[10] *Data Breaches Renew Fight Over Credit Card Chip Technology*. USA Today. January 30, 2014.
[11] Sullivan, Ricard. The U.S. Adoption of Computer-Chip Payment Cards: Implications for Payment Fraud.
[12] *PayPal President's Credit Card Hacked for Shopping Spree*. USA Today. February 10, 2014.

transactions that allow signature authorization. Fraudsters may put more effort into stealing computer- chip payment cards, knowing that they may be able to commit a few fraudulent transactions using a forged signature before issuers cut off use of the card...

...The experience of countries that have adopted computer-chip payment cards shows that EMV payment cards offer capabilities for strengthening authentication and preventing fraud. The degree of payoff from adopting the cards only emerges over time, however, because authentication methods tend to evolve and improve during a transition period. Still, some fraud will migrate to payments with weak authentication capacities, and card issuers will need countermeasures to improve authentication.

Research and consulting firm Aite Group estimates that U.S. online card fraud will more than double to $6.6 billion from $3.3 billion between 2015 and 2018.

Another factor that will take some time is consumer education. Prior to the recent data breaches most U.S. consumers had not heard of EMV technology as these cards were available to a limited number of consumers that met certain guidelines, such as a frequent traveler. The implementation of EMV will require consumers to become comfortable with a new way to make purchases via inserting the card into the terminal and providing a PIN, or tapping the card against the contactless reader. One card network reported that only 5% of the contactless cards on the market today are ever used for contactless payments.[13] The experience of mobile payments implementation may also be telling for the transition to EMV. One of the often cited reasons for the initially slow adoption of mobile payments usage by consumers is a lack of viewing mobile payments as more convenient than simply swiping their card.

Finally, the form of EMV technology may offer additional points of concern and disagreement amongst industry participants. The form of EMV offered will be up to each issuer so that the credit card market in the U.S. will see a mix of Chip & PIN and chip & signature cards. Chip & signature cards offer less protection than those that require a PIN because should someone (other than the cardholder) get physical access to the card the signature is easily forged.

Estimates are that 70% of credit cards and 40% of debit cards will use EMV technology by the end of 2015, though the rollout of upgraded POS terminals may take until the end of the decade.[14] Whatever the timeline may be urgency is necessary as security experts predict

[13] First Data, 16
[14] Preparing for Chip-and-PIN Cards in the United States. The New York Times. December 2, 2014

increased data breaches as hackers close in to exploit the current payment system before the door closes.[15]

Additional Payments Security:

EMV technology is a vital piece of a larger puzzle in protecting payment information as it does not alleviate the "need for secure passwords, patching systems, monitoring for intrusions, using firewalls, managing access, developing secure software, educating employees and having clear processes for handling of sensitive payment card data."[16]

Point-to-point encryption (P2PE) technology helps merchants and acquirers protect payment card data within their systems by encrypting sensitive cardholder information. Because the card data can only be accessed, or unscrambled, with decryption keys held securely by the acquirer, gateway or card network, cardholder information is protected within the payment processing environment.

P2PE ensures sensitive credit and debit card data is protected from first card swipe, while in transit, all the way to the payment processor. This technology is also referred to as end to end encryption, or E2EE.

State of the art encrypting devices scan and encrypt cardholder information prior to performing an electronic payment transaction. These sophisticated devices use Triple DES Encryption and DUKPT key management technology to encrypt and transmit cardholder data securely over any network. The encrypted cardholder data being transmitted is NOT equivalent to the original cardholder data in any way. Even if the data were to be intercepted, it would be useless to data thieves.

Tokenization

Tokenization has advantages for both merchant and service providers. Tokenization is software-based and replaces the cardholder's primary account number (PAN) with a randomly-generated proxy alphanumeric number ("token") that cannot be mathematically reversed and is used for long-term storage or for use as a transaction identifier. From a service provider's perspective, being a software-only technology, it is fairly easy to institute.

For recurring payments from a merchant's standpoint, tokenization is ideal. For these type of payments, the card number is only on the merchant's network "in flight" during the

[15] Experian 2015 Data Breach Industry Forecast.
[16] Statement of Troy Leach, Chief Technology Officer, Payment Industry Security Standards Council. *Before the Committee on Banking, Housing, and Urban Affairs, Subcommittee on National Security and International Trade and Finance United States Senate*. February 3, 2014.

initial transaction which can now be encrypted and protected using P2PE but beyond that, the merchant uses the token that represents the original card for subsequent payments or to track customer transactions for marketing purposes. A myriad of targeted marketing programs can be developed by the merchant using cardholder purchase history data in a tokenized fashion in the merchant's database to, for instance, project what new products may complement those the consumer previously purchased.

One of the major benefits of the tokenization implementation planning process is that it offers the opportunity for merchants to potentially get a head start in compliance with PCI version 3.0, which requires an annual assessment of the locations and flows of cardholder data. Locating all the cardholder data within a merchant's location and identifying who should have access to it could help merchants get ahead of future PCI compliance by re-engineering the logical controls and restrictions to tokenized data.

Tokenization is also a major part of mobile payments security. In the case of mobile payment applications like Square, the consumer's face is the token because it is shown to the merchant but the actual payment information is secure and never shared. Apple Pay uses tokenization where the actual credit card number is removed and replaced with a randomly generated number. The number, or token, can expire after one purchase or a after a specific number of transactions. This process prevents the storage of payment information by retailers as their systems never actually see the customer's credit card information.

Mobile Payments & Mobile Banking

The Aite group forecasts that U.S. mobile payments will reach $214 billion in gross dollar volume in 2015, a monumental rise from $16 billion in transactions in 2010. Consumer behavior has drastically changed with the smartphone becoming a crucial part of everyday activities. Four out of every five shoppers use smartphones to shop and 85% of all merchants say that mobile commerce is a focus up from 68% in 2012.[17] In the U.S. over $4.6 billion worth of transactions are made using mobile money every month accounting for 224 million monthly transactions with 30 million active users, 520,000 agents, and 150 mobile money services.[18] In spite of these numbers the Yankee Group, an information technology research and advisory company, only 16% of mobile users used a mobile wallet to make an in store purchase.

Consumers currently can make three types of payments using a smartphone or tablet computer. The first is a person-to-person transfer initiated by a mobile device that could include non-commercial payments from one person to another, or commercial payments to

[17] *Simplicity is the Ultimate Sophistication: The Future of Mobile Payments*. Oracle. October 2014.
[18] Ibid. 4

a small scale merchant. Second, is for goods or services purchased over the internet on a mobile device. The third option is at POS device initiated from a mobile device at a physical location. These payments can be made using a variety of technologies such as a wallet system that may utilize a smart phone based application to generate barcodes, or a QR Code that allows the user to pay for something from a funding source associated with the mobile wallet. Other options connect a virtual wallet with an email address or username and password. The potential security benefit to a consumer using a mobile payment application is that the consumer's underlying payment data can be shielded from the retailer's payment system.

The aforementioned systems can further be divided into two main categories of mobile payment, Proximity Payments and Remote Payments. Proximity payments are those that occur when the technology is embedded in, attached to, or displayed on the purchaser's mobile device and interfaces with the merchants POS. Examples of this are Apple Pay, Google Wallet and the Starbucks payment application. A remote payment occurs when the purchaser uses a mobile device to initiate a payment to a merchant or other payee without regard to the proximity of the POS or the payee.

Mobile payments by the numbers:

- 55% of US millennial smartphone owners who use mobile payments prefer to have a unified app that can be used in multiple stores while integrating individual store coupons and loyalty programs (Customer Engagement Via Mobile Wallets: There's No Way It Won't Become a Norm LOYALTY360 Published: 12/08/2014)
- "Pre-Apple Pay, nearly a quarter of smartphone users had already used a mobile payment app at some point. And we know that if anyone can drive new technology adoption, it's Apple" - Robyn Hannah, VP, PR and Communications, PunchTab
- 29% of US smartphone owners who have used mobile payment apps to make a purchase have used the Starbucks app, compared to 25% for Google Wallet, 10% for Visa Checkout, and 9% for PayPal Wallet (Customer Engagement Via Mobile Wallets: There's No Way It Won't Become a Norm LOYALTY360 Published: 12/08/2014)
- 13% of North American millennials use their smartphones to make payments at merchant locations at least once per week, and 26% expect to do so by 2020 (Digital Payment Technologies Convenient for Customers LOYALTY360 Published: 10/30/2014)

- 18% of North American consumers expect to use digital currencies to complete a mobile payment transaction at least weekly by 2020. (Digital Payment Technologies Convenient for Customers)

- 8% of North American consumers use digital currencies to complete a mobile payment transaction at least weekly. (Digital Payment Technologies Convenient for Customers)

- "Millennials are most likely of any age group to use a smartphone to make a mobile payment, and are in fact driving the adoption of new payments technologies" - Matthew Friend, Accenture Payment Services

- There will be 516 million mobile users of near field communication contactless payment services by the end of 2019, up from 101M in 2014. (*Apple Pay and HCE To Push NFC Payment Users to More Than 500 Million* by 2019, Juniper Research Published: 10/28/2014)

- 36% of Americans who use mobile payments have done so to pay household bills. (The Modern Wallet: Mobile Payments are Making Life Easier, NIELSEN Published: 07/04/2014)

Ironically, with the pace of technological development, specifically in California, the United States lags behind the developing world on mobile payment use. Several developing markets are bypassing traditional banking all together and jumping straight to mobile banking options. Merchants, acting agents for traditional banks, in small villages use mobile phones and card readers for customer deposits, withdrawals and money transfers. Keyna is a leader in using this technology for mobile banking as 12 million people send and save money using M-Pesa a completely telephone based banking system.

Mobile payment platforms continue to be an area of fierce competition and development as various industries have created their own mobile wallet applications. These developments change monthly as industries pivot into new directions and philosophies in the payments space. Just recently, Softcard, a joint venture between T-Mobile, AT&T and Verizon sold its technology to Google. The mobile carriers had an edge in pushing Softcard, formally the poorly named ISIS wallet, as it was often preloaded on mobile phones and would actually block the NFC chip of such phones to prevent the user from using another wallet service such as Google Wallet. With Google purchasing the technology of Softcard they are on a mission to offer a competing wallet on par with Apple Pay.

Not to be left out of this mobile payment arms race, Samsung is rolling out a new payments platform with the release of its newest Galaxy phone model called Samsung Pay. Samsung

purchased a company called LoopPay to make its new platform possible. The company uses a patented technology called Magnetic Secure Transmission (MST) to turn payment terminals into contactless readers. Samsung Pay could be accepted at millions of terminals and merchants may not even notice. This technology allows users to pay using almost any magnetic stripe payment gateway, which as you know sits on the countertop of just about every retail establishment in the US. MST broadcasts data magnetically, making it so you can send your payment credentials just by tapping your phone to the side of the terminal you would normally swipe your card in, and no additional tech is required from the vendor. As far as the register behind the counter is concerned, you just swiped your card.

Retailers have jumped into the mobile payments mix with a project called CurrentC, backed by Merchant Customer Exchange (MCX). CurrentC is estimated to roll out over the next year and in a preempted strike several retailers (Rite Aid and CVS) who are members of MCX have disabled the NFC readers in their stores to block the use of Apple Pay. The motivation behind CurrentC is to remove credit card infrastructure from the transaction in order to remove the fees paid by merchants for credit card transactions. While Apple Pay and other NFC based aps provide convenience and potentially layers of encryption for a transaction, NFC based wallets still rely on the existing payments network. With Apple Pay users take a photo of their credit cards, storing this information on their phone. When checking out the consumer holds their iPhone to the NFC POS terminal and then authenticate the transaction via the Touch ID sensor on the phone. The means to the transaction has changed but the behind the scene processing still operates the same as if the consumer used their plastic credit card. CurrentC changes this by eliminating the credit card from the equation and instead links it to the consumer's checking account. In order to pay, the customer scans a QR code or the cashier scans a QR code generated on the customer's phone. If the account information were to be stolen a consumer would have less protection because the funding mechanism was an Automated Clearing Housing (ACH) payment. Under certain conditions, a credit card holder has certain protections in the case of a dispute with the merchant. Additional protection is provided for credit card holders from their card issuers if the ordered merchandise is never delivered or different merchandise is delivered than what is ordered. No comparable protection is provided for ACH transactions or debit card users. While a consumer’s liability for unauthorized transactions is generally limited, the liability can increase for debit card and ACH users if they do not provide timely notice of unauthorized transactions and there continue to be unauthorized transactions on the account.

Table 1: Mobile Payments Technologies	
Near Field Communications	Wireless protocol that allows for encrypted exchange of payment credentials and other data at close range.
Cloud Based	Leverages mobile connection to the Internet to obtain credentials not stored on the mobile device.
Image Based	Coded images similar to barcodes used to initiate payments. Credentials may be encrypted within image or stored in cloud.
Carrier Based	Payments billed directly to mobile phone account. Merchants paid directly by mobile carrier, bypassing traditional payment networks.
Proximity Based	Geolocation used to initiate payments. Merchant will identify active users within range and verify identity. Credential exchange is cloud-based.
Mobile P2P	Payment initiated on mobile device using recipient's email address, mobile phone number, or other identifier. Payment is via ACH, card networks, or intra-account transfer.

FIDC, Supervisory Insights - Winter 2012, *Mobile Payments: An Evolving Landscape*

Table 3: Laws and Regulations That Apply to Mobile Payments Transactions		
Law or Regulation / Description: Electronic Fund Transfer Act (EFTA) / Regulation E *Establishes rules for electronic fund transfers (EFTs) involving consumers.*		
Coverage: Generally includes any "transaction initiated through an electronic terminal, telephone, computer, or magnetic tape that instructs a financial institution either to credit or debit a consumer's account." This includes transactions such as debit card transactions, direct deposits and withdrawals, and automated teller machine (ATM) transactions. The regulation generally applies to financial	**Applicability to Mobile Payments**: Applies when the underlying payment is made from a consumer's account via an EFT.	**Key Obligations / Other Information**: The rule establishes consumer rights to a number of disclosures and error resolution procedures for unauthorized or otherwise erroneous transactions. The disclosures include upfront disclosures regarding, among other things, the terms and conditions of the EFT service and how error resolution procedures will

institutions, but certain provisions apply to "any person."		work.
Law or Regulation / Description: Truth in Lending Act (TILA) / Regulation Z *Establishes rules regarding consumer credit; intended to help consumers understand the cost of credit and compare credit options.*		
Coverage: Generally applies to "creditors" that offer or extend credit to consumers and includes both open-end and closed-end credit products, including credit cards.	**Applicability to Mobile Payments:** Applies when the underlying source of payment is a credit card (or other credit account covered by TILA and Regulation Z).	**Key Obligations / Other Information**: Creditors are required to provide disclosures to consumers describing costs; including interest rate, billing rights, and dispute procedures.
Law or Regulation / Description: Truth-in-Billing *Requires wireless carriers to provide certain billing information to customers.*		
Coverage: Applies to wireless carriers.	**Applicability to Mobile Payments**: Applies when mobile payment results in charges to mobile phone bill.	**Key Obligations / Other Information**: Wireless carriers must provide clear, correct, and detailed billing information to customers. This includes a description of services provided and charges made.
Law or Regulation / Description: Unfair, Deceptive, or Abusive Acts or Practices (UDAP) under the Federal Trade Commission (FTC) Act /Unfair, Deceptive or Abusive Acts or Practices (UDAAP) under the Consumer Financial Protection Act of 2010 *Prohibits "unfair or deceptive acts or practices in or affecting commerce."*		
Coverage: Applicable to any person or entity engaged in commerce. Made applicable to banks pursuant to Section 8 of the Federal Deposit Insurance Act.[16]	**Applicability to Mobile Payments**: Applies to all mobile payments regardless of underlying payment source.	**Key Obligations / Other Information**: Prohibits "unfair or deceptive acts or practices in or affecting commerce." The Dodd-Frank Act also added the concept of "abusive" practices to "unfair" or "deceptive" ones, and gave the Consumer Financial Protection Bureau (CFPB) authority to further define abusiveness.
Law or Regulation / Description: Gramm-Leach-Bliley Act (GLBA) Privacy and Data Security Provisions *Establishes rules regarding consumer privacy and customer data security.*		

Coverage: The privacy rules and data security guidelines issued under GLBA apply to "financial institutions," which include depository institutions as well as nonbanks engaged in financial activities.	**Applicability to Mobile Payments**: Applies when a financial institution handles information of a "consumer" or "customer."	**Key Obligations / Other Information**: Financial institutions are required to provide consumers with certain notices regarding the privacy of nonpublic personal information and allow them to opt out of certain types of information sharing. The GLBA data security provisions give guidance on the appropriate safeguarding of customer information.
Law or Regulation / Description: Federal Deposit Insurance or NCUA Share Insurance *Protects funds of depositors in insured depository institutions and of members of insured credit unions in the event of failure of the institution.*		
Coverage: Applies to "deposits" and "accounts" as defined in laws and regulations of the FDIC and National Credit Union Administration. These include savings accounts and checking accounts at banks and share accounts and share draft accounts at credit unions.	**Applicability to Mobile Payments**: If the funds underlying a mobile payment are deposited in an account covered by deposit insurance or share insurance, the owner of the funds will receive deposit or share insurance coverage for those funds up to the applicable limit.	**Key Obligations / Other Information**: Deposit insurance or share insurance does not guarantee that a consumer's funds will be protected in the event of a bankruptcy or insolvency of a nonbank entity in the mobile payment chain.
Note: This table is not exhaustive, and other laws, regulations, and policies may apply.		

Virtual Currency

Recent headlines concerning virtual currency have been dominated by Bitcoin with some of this attention resulting from negative publicity. The high profile *Silk Road* case in which federal law enforcement officials arrested the operator of an online illegal drug market place that facilitated the sale of drugs and other illegal goods through acceptance of Bitcoins. Bitcoins were used because it is a decentralized currency allowing users to be pseudonymous to some extent, even though every Bitcoin transaction is logged. Bitcoin is not the first, nor the only virtual currency. Numerous models of virtual currency have sprouted up over the last decade, and this growth has inspired additional questions by government officials and policy makers.

Bitcoin has received its share of negative attention from its wild price fluctuations, awareness against Bitcoin "Wallets" (as the individual software applications that manage bitcoin holdings) to being credited with being the currency of choice for criminal activity. As to the latter attribution, cash money is still the dominant and preferred source of anonymous payment for illegal activities. Some of the attention, specifically in relation to the risk associated with storing virtual currency has raised the attention of state regulators across the country.

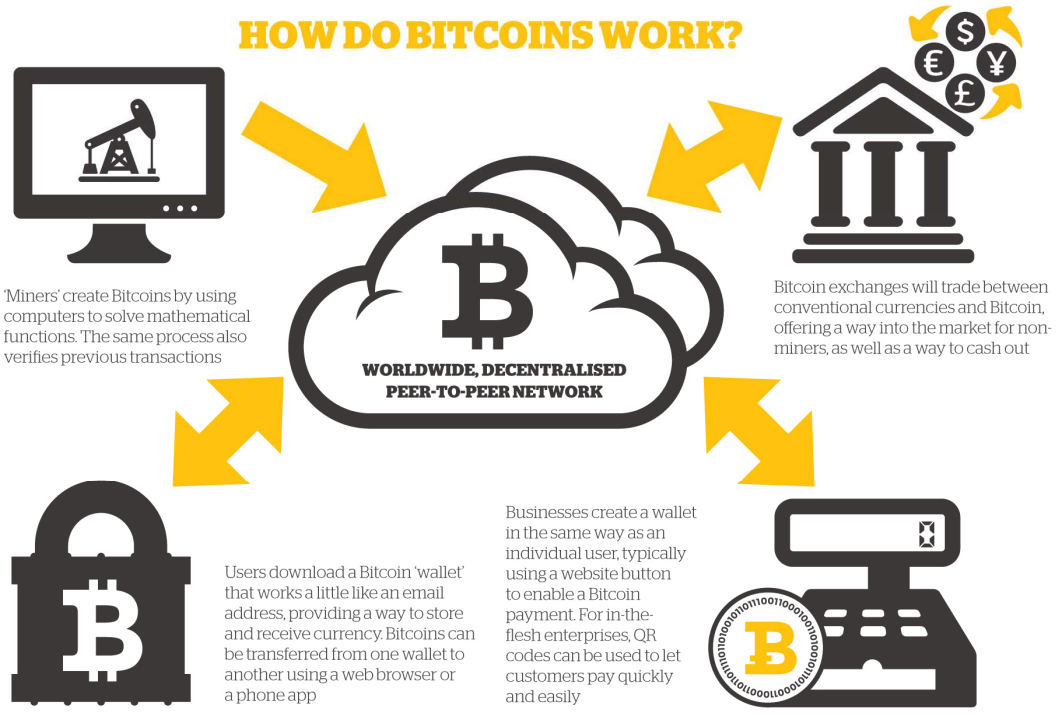
Even though the core program that runs bitcoin has resisted six years of hacking attempts, the successful attacks on associated businesses have created the impression that bitcoin isn't a safe way to store money. Bitcoins exist purely as entries in an accounting system—a transparent public ledger known as the "blockchain" that records balances and transfers among special bitcoin "addresses." With bitcoin, the balances held by every user of the monetary system are instead recorded on a widely distributed, publicly displayed ledger that is kept up-to-date by thousands of independently owned, competing computers known as "miners."

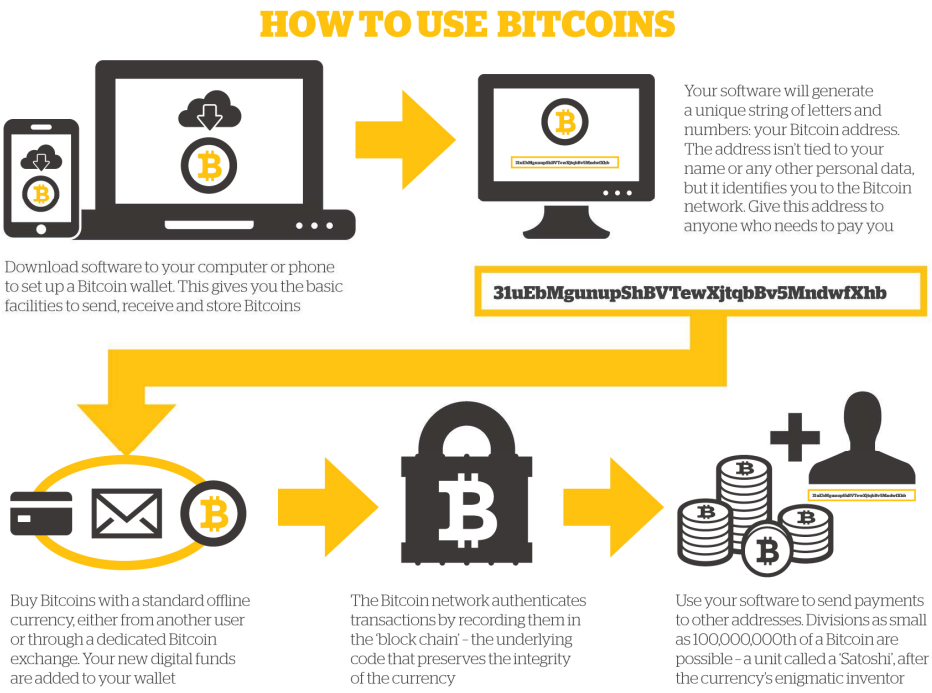
What does a real world transaction look like such as buying a cup of coffee at your local coffee shop? If you pay with a credit card, the transaction seems simple enough: You swipe your card, you grab your cup, and you leave. The financial system is just getting started with you and the coffee shop. Before the store actually gets paid and your bank balance falls, more than a half-dozen institutions—such as a billing processor, the card association your bank, the coffee shop's bank, a payment processor, the clearinghouse network managed by the regional Federal Reserve Banks—will have shared part of your account information or otherwise intervened in the flow of money. If all goes well, your bank will confirm your identity and good credit and send payment to the coffee shop's bank two or three days later. For this privilege, the coffee shop pays a fee of between 2% and 3%.

Now let's pay in Bitcoin. If you don't already have bitcoins, you will need to buy some from one of a host of online exchanges and brokerages, using a simple transfer from your regular bank account. You will then assign the bitcoins to a wallet, which functions like an online account. Once inside the coffee shop, you will open your wallet's smartphone app and hold its QR code reader up to the coffee shop's device. This allows your embedded secret password to unlock a bitcoin address and publicly informs the bitcoin computer network that you are transferring $1.75 worth of bitcoin (currently about 0.005884 bitcoin[19]) to the coffee shop's address. This takes just seconds, and then you walk off with your coffee. Next, in contrast to the pay with credit/debit system, your transaction is immediately broadcast to the world (in alphanumeric data that can't be traced to you personally). Your

[19] As of March 12, 2015

information is then gathered up by bitcoin "miners," the computers that maintain the system and are compensated, roughly every 10 minutes, for their work confirming transactions. The computer that competes successfully to package the data from your coffee purchase adds that information to the blockchain ledger, which prompts all the other miners to investigate the underlying transaction. Once your bona fides are verified, the updated blockchain is considered legitimate, and the miners update their records accordingly. It takes from 10 minutes to an hour for this software-driven network of computers to formally confirm a transfer from your blockchain address to that of the coffee shop—compared with a two- to three-day wait for the settlement of a credit-card transaction. Some new digital currencies are able to finalize transactions within seconds. There are almost zero fees, and the personal information of users isn't divulged. This bitcoin feature especially appeals to privacy advocates: Nobody learns where you buy coffee. The advantages of digital currency are far more visible in emerging markets. It allows migrant workers, for example, to bypass fees that often run to 10% or more for the international payment services that they use to send money home to their families. Although many companies now accept bitcoin (the latest and biggest being Microsoft Corp.), global usage of the digital currency averaged just $50 million a day in 2014. Over that same period, Visa and MasterCard processed some $32 billion a day. The market capitalization for BitCoin is almost at $4 billion with virtual currency Ripple the next largest at over $340 million.





FinCEN Issues Guidance on Virtual Currencies

FinCEN issued interpretive guidance earlier this year to clarify how the Bank Secrecy Act (BSA) and FinCEN regulations apply to users, administrators and exchangers of virtual currencies. Under the regulatory framework, virtual currency is defined as having some but not all of the attributes of "real currency" and therefore, virtual currency does not have legal tender status in any jurisdiction. Specifically, the FinCEN guidance addresses convertible virtual currency which either has a real currency equivalent value or serves as a substitute for real currency.

The roles of persons (including legal entities) involved in virtual currency transactions are defined by FinCEN as follows:

- User: A person who obtains virtual currency to purchase goods or services
- Exchanger: A person engaged as a business in the exchange of virtual currency for real currency, funds or other virtual currency
- Administrator: A person engaged as a business in issuing into circulation a virtual currency and who has the authority to redeem and withdraw from circulation such virtual currency

A person, or legal entity, may act in more than one of these capacities. Further, it is important to note that "obtaining" virtual currency covers much more than the scenario of a "user" who merely purchases virtual currency. Depending on the model of the particular

currency, a party could "obtain" virtual currency through various acts including earning, harvesting, mining, creating, auto-generating, manufacturing or purchasing.

The threshold issue is whether actions will subject a person or legal entity to BSA's registration, reporting and recordkeeping regulations that apply to money services businesses (MSBs). A user who obtains convertible virtual currency and uses it to purchase real or virtual goods or services is not subject to MSB compliance because such activity does not meet the definition of "money transmission services" and the user would not be a "money transmitter."

However, an administrator or exchanger engages in money transmission services and, as a result, is a "money transmitter" under FinCEN definitions by (1) accepting and transmitting convertible virtual currency or (2) buying or selling convertible virtual currency. As a money transmitter, the administrator or exchanger would generally be subject to MSB reporting and recordkeeping.

Further, the FinCEN guidance expressly addresses the category of de-centralized virtual currency – the Bitcoin model – and states that "a person is an exchanger and a money transmitter if the person accepts such de-centralized convertible virtual currency from one person and transmits it to another person as part of the acceptance and transfer of currency, funds, or other value that substitutes for currency."

In the area of foreign exchange, accepting real currency in exchange for virtual currency is not subject to FinCEN regulations applicable to "dealers in foreign exchange" since a forex transaction involves exchanging the currency of two countries and virtual currency does not constitute legal tender as a currency of a country.

Last year, the Legislature passed and the Governor signed AB 129 (Dickinson) which clarified California law to ensure that alternative currency, including virtual currency would not be potentially deemed illegal tender. California continues to lead the way on these issues as this year Assembly Banking and Finance Committee Chair Matt Dababneh has introduced AB 1326 which would require licensing and capitalization requirements for some entities that offer virtual currency exchange services. The goal behind this legislation is to provide protections for users of virtual currency when they store that currency with a service that offers a digital wallet function. With greater oversight and protections virtual currency may gain even greater mainstream participation.

For a detailed review of Bitcoin and virtual currency see Bitcoin: A Primer for Policy Makers either attached to this background or available at http://mercatus.org/sites/default/files/Brito_BitcoinPrimer_v1.3.pdf