The Technology of Consumer Financial Transactions

Assembly Committee on Banking & Finance

November 21, 2013

Assemblymember Roger Dickinson, Chair

Mark Farouk-Chief Consultant
Kathleen O'Malley-Senior Consultant
Tiffany Morrison-Committee Secretary

On March 11th, 2013 the Committee on Banking and Finance conducted a hearing titled, *Emerging Technology and the California Money Transmission Act.* That hearing focused on the growing use of alternative means to send and receive payments within the United States and around the globe. That hearing led to the introduction of AB 786 (Dickinson) which revised and updated various provisions of the Money Transmission Act (MTA) in order to address changes in technology that required revisions to the MTA. AB 786 was signed by Governor Brown on October 4, 2013. A substantial amount of consumer financial transactions are covered under the MTA. While working on AB 786 committee staff encountered a broad set of questions and issues concerning the growth of mobile payments and alternative payment networks. This growth has brought about numerous developments in regulatory policy making, as well as, potential legislative action. For the most part California and the United States have a financial regulatory system geared toward stagnant technology and business models. The existing structure largely covers insured depository institutions (banks) or non-bank entities that assist with international remittances. These historical models have focused on ensuring the safety and soundness of the institutions and preventing money laundering activity. In addition to these layers, existing legal frameworks establish the rights and responsibilities of each party to a transaction and the appropriate procedures if loss or fraud occurs. The emergence of new technologies has blurred these lines in some ways because new middle parties have been introduced into the payments space. Most developments in mobile applications that send or receive money, or pay for goods and services are still connected to a traditional payment method, such as credit card or checking account. In this environment the traditional payment offerings are still present, but the legality of the roles they play are still part of a larger discussion and debate within the payments industry and among federal and state regulators.

Traditional Methods of Payment:

Today, electronic payments made through payment card networks and the automated clearinghouse system (ACH) make up four out of five noncash payments in the United States according to a 2010 Federal Reserve study on payments. The use of plastic credit or debit cards has become ubiquitous for the majority of consumer payments. Consumers use their cards to pay for goods or services and within seconds a transaction is approved and the sale is complete. This interaction is so frequent that rarely would anyone ask about the behind the scenes aspect of this transaction. What happens in those few seconds? Who are the parties to the transaction? What legal frameworks govern these transactions?

The terminology and process of a credit card transaction:

Acquirer- A bank that processes and settles a merchant's credit card transactions 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.

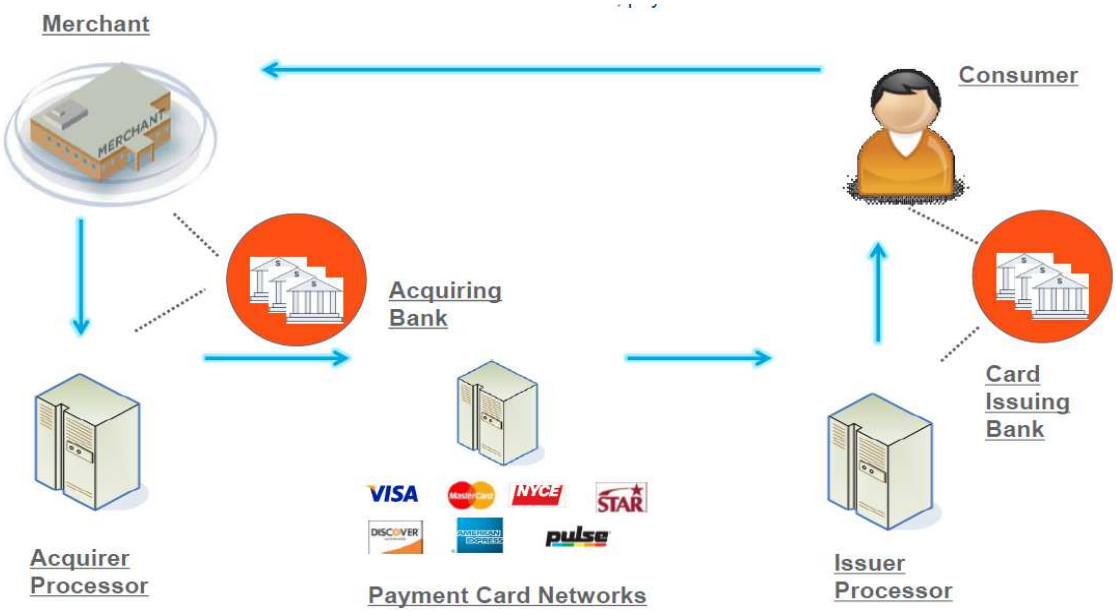
Clearing- The third step in processing a credit card. After the acquirer receives the batch, it sends it through the card network, where each sale is routed to the appropriate issuing bank. The issuing bank then subtracts its interchange fees, which are shared with the card network, and transfers the 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. They generally range from 1 to 3 percent of the transaction value.

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



Chip & Pin and Chip & Signature:

The U.S. remains the last development country reliant on the magnetic stripe credit cards (mag stripe). The U.S. is currently on pace to be a full decade behind Europe on the implementation of credit card chip & PIN technology. Until the introduction of Chip and PIN, all face-to-face credit or debit card transactions used a magnetic stripe or mechanical imprint 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 either "swipes" the card through a magnetic reader or makes an imprint from the raised text of the card. In the former case, the account details are verified and a slip for the customer to sign is printed. In the case of a mechanical imprint, the transaction details are filled in and the customer signs the imprinted slip. In either case, the clerk verifies that the signature matches that on the back of the card to authenticate the transaction.

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.

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®.

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. 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.

As previously mentioned the U.S. is lagging behind in implementation and acceptance of EMV technology. The first U.S. credit card utilizing EMB 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. Several 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 thus far in limited quantities and targeted toward higher income card holders. A factor that is contributing to the limited role out of EMV in the U.S. is that currently no merchant accepts EMV chip-embedded cards. Most EMV chip cards issued board and in the U.S. also contain a mag strip thus allowing acceptance at all U.S. merchants that accept credit cards.

Perhaps both the issuance and acceptance of EMV chip cards (and potentially other chip-enabled devices such as mobile phones) will increase with a recent announcement by Visa. This 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 percent of a merchant's transactions originate from chip-enabled terminals effective October 1, 2012. For the largest merchants, savings from an annual compliance validation would average approximately $225,000 a year. Further, Visa set October 1, 2015 as the date when a card-present counterfeit fraud liability shift from issuers to merchant acquirers will be implemented if fraud occurs in a transaction that could have been prevented with a chip-enabled payment terminal. 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.

Money Transmission & Mobile Money.

At the most basic level money transmission is the transfer of funds involving three parties, 1) Sender 2) Money transmitter and 3) Recipient. The transfer of funds may be intrastate, interstate, or international. Typically this service is conducted at a physical location where the sender of funds pays a fee to the remittance service and the money is then wired to the recipient.

Large money transmitters may have a home office, transaction clearing centers, service center (s), regional offices, and branches. They may also contract with agents. Agents may include established businesses such as grocery stores, truck stops, check cashers, pharmacists, travel agents and supermarket chains. The money transmission home office pays its agents using a fee schedule that provides predetermined charges for money transmission.

This is how the traditional model of money transmission works. A sender enters an agent location and wishes to send $500 to a recipient in another location. The sender provides the agent the funds and instructions for delivery to the recipient. The agent takes the funds and instructions and usually enters the transaction into a computer terminal owned by the money transmitter and that is linked to the money transmitter's processing system. Upon receiving the instructions, the money transmitter will contact its appropriate receiving agent for payout to the recipient. The sender and/or receiving agent will inform the recipient that the transmitted funds are available for pick-up. The availability of funds to the recipient may range from minutes to several days depending upon the location and availability of the receiving agent and money transmitter's delivery policy. While computers are the typical means for the transferring of money, telephone lines and fax machines are still widely used.

According to World Bank estimates, remittances totaled $414 billion in 2009, of which $316 billion went to developing countries that involved 192 million migrant workers. For some individual recipient countries, remittances can be as high as a third of their Gross Domestic Product (GDP). The top recipients in terms of the share of remittances in GDP included many smaller economies such as Tajikistan (45%), Moldova (38%), and Honduras (25%).

Historically, the money transmission involved face-to-face transaction between the consumer and transmitter agent that would accept the consumer's money and transmit those funds to another agent outside of the United States for delivery of those funds to the consumer's family or friends. These transactions were dominated primarily by a few large transmitters such as Western Union and MoneyGram. Subsequent to the issuance of the draft National Conference of Commissioners on Uniform State Laws money transmission act, states across the country amended their statutes to provide enhanced regulation to foreign and domestic transmission and non-bank issued stored value. Forty eight states and the District of Columbia have money transmission licensing statutes.

Money transmission activity is regulated via the California Money Transmission Act (Financial Code Sections 2000-2172). The United States Department of Treasury under the Financial Crimes Enforcement Network (FinCEN) requires registration of money services businesses (MSB). According to FinCEN an MSB includes any person doing business, whether or not on a regular basis or as an organized business concern, in one or more of the following capacities, and that meets a threshold of $1,000 per day or more transactions:

- Currency dealer or exchanger.
- Check casher.
- Issuer of traveler's checks, money orders or stored value.

- Seller or redeemer of traveler's checks, money orders or stored value;
- Money transmitter.

FinCEN registration does not apply to a bank or a person regulated or registered with the Securities and Exchange Commission. Entities registered with FinCEN must make electronic filings under the Bank Secrecy Act (BSA). As of July 1, 2012, all such filings must be electronic and made through the BSA E-Filing System. Reports that must be filed through this system include, but are not limited to:

- Currency Transaction Report (FinCEN Form 104)
- Designation of Exempt Person (FinCEN Form 110)
- Suspicious Activity Report (Form TD F 90-22.47)
- Suspicious Activity Report by the Securities and Futures Industries (FinCEN Form 101)
- Suspicious Activity Report by Money Services Business (FinCEN Form 109, formerly 90-22.56)
- Suspicious Activity Report by Casinos and Card Clubs (FinCEN Form 102)
- Currency Transaction Report by Casinos (FinCEN Form 103, formerly 8362)
- Registration of Money Services Business (FinCEN Form 107)
- Report of Foreign Bank and Financial Accounts (Form TD F 90-22.1)

These activities are also subject to Federal Reserve Regulation E. On July 21, 2010, the Dodd Frank Wall Street Reform and Consumer Protection Act (Dodd Frank Act) was signed into law. Section 1073 of the Dodd Frank Act creates new protections for U.S consumers sending money abroad. Such transfers or remittances as the Act identifies them are now the subject of rulemaking by the Consumer Financial Protection Bureau (CFPB) the agency charged with implementing Section 1073. The CFPB issued a final rule regulating remittance transfers by amending Regulation E (Reg E) that governs electronic transfer of funds. CFPB issued new rules concerning remittance transfer that took effect October 28, 2013.

The new rules require companies to give certain disclosures on fees and other costs prior to payment for the remittance transfer. The rule also gives consumers 30 minutes to cancel a transfer and companies must investigate if a consumer reports a problem with a transfer. For more detail on these rules visit, http://www.consumerfinance.gov/remittances-transfer-rule-amendment-to-regulation-e/.

Mobile technology has opened up a range of possibilities for mobile payments and money transmission services yet other countries are far ahead of the U.S. in usage of these new payment applications.

Mobile money transfer typically refers to services whereby customers can use their mobile devices to send and receive money or to transfer money electronically from one person to another using a mobile phone. This transfer can be either a domestic transfer or international remittance transaction. The key characteristic of mobile money transfer services is the fact that they relate to private transactions only (i.e. transactions involving transfers of money from one person to another). Mobile money transfer addresses person-to-person (P2P) money transfers and is a subset of mobile payments.

Mobile money transfers using mobile phones require senders to give the money to a remittance center and pay a fee. The remittance center then transfers the money electronically through the phone service provider to the recipient's phone. In the case of international remittances, the person receiving the money gets a text message advising of the transfer. The recipient can go to any licensed outlet, including a retail store or restaurant, to get the money. The recipient may have to pay a fee to collect the money. In the case of domestic remittances, the transfer is handled automatically on the mobile money platform.

The mobile remittance industry is burgeoning due to the increased penetration of mobile phones in remote regions and the mushrooming of various remittance service providers, both national and international, for global money transfers. According to the Migration Development Brief of the World Bank, remittance flows to developing countries were estimated to have reached USD 372 billion in 2011, and are expected to reach USD 467 billion by 2014, and total worldwide remittance flows are expected to reach $615 billion by 2014. India and China rank highest as recipients of migrant remittances, to the tune of $64 billion and $62 billion respectively. Tajikistan and Lesotho receive remittances that are as high as 31 per cent and 29 per cent of GDP respectively. Various money transfers options (phone to phone, cash to phone, phone to cash, mobile-wallets etc.) can be made conveniently using mobile devices through platforms and applications provided by various banking institutions and money transfer operators worldwide. Various money transfer operators provide services either through a network of agents or partnering with banking institutions depending on the regulations of the central bank and other financial bodies of various nations.

In 2007, Safaricom and Vodafone launched a mobile money transfer service called M-PESA. Five years later M-PESA provides services to 15 million Kenyans (more than a third of the country's population) and serves as a conduit for a fifth of the country's GDP. M-PESA now processes more transactions domestically within Kenya than Western Union does globally and provides mobile banking facilities to more than 70% of the country's adult population. However, the service cannot function without the presence of the formal financial sector. Bank branches are a vital part of the cash management operation of an M-PESA agent. Moreover, the early adopters of the service in Kenya were more likely to be banked than non-users. M-PESA has also been implemented in Tanzania, South Africa and Afghanistan. The M-PESA application has also served as a

platform for innovations in other areas such as insurance, savings and banking in Kenya.

In Pakistan, 89% of the adult population does not have a bank account. Easypaisa was established in 2009 in Pakistan through a partnership between Telenor Pakistan and Tameer Microfinance Bank. The regulation mandated a bank led model and hence the license for branchless banking rests with Tameer Microfinance Bank, while Telenor Pakistan also acquired 51% ownership in Tameer for better governance of the new business. The partnership has developed a network of over 20,000 agents. The main differentiating factor in Easypaisa is that customers do not require a mobile phone or account with Telenor to pay their bills or to send/receive money. These transactions are done at any of the 20,000 Easypaisa shops around the country by the merchant on his mobile phone. In 2010, Easypaisa mobile accounts (m-wallets) were launched for Telenor SIM subscribers only. Mobile Account subscribers use their own phones for all transactions and only need to go to Easypaisa shops in Pakistan to deposit or withdraw cash from their Easypaisa mobile account. Services offered include bill payments, money transfers, airtime purchase, savings and insurance, retail purchase, corporate solutions, viewing account balances and recent transactions, managing PIN codes, and so on. In 2012, Easypaisa conducted on average over 5 million transactions every month.

GCASH is a mobile money transfer service from Globe Telecom in the Philippines, which transforms a mobile phone into a virtual wallet for secure, fast, and convenient money transfers at the speed and cost of a text message. The recipient in the Philippines can easily receive a sender's remittance direct to his mobile phone. Globe Telecom issues an account which is the GCASH account in which the money is sent by the sender to be withdrawn by the recipient. The recipient is sent an SMS alert indicating the amount sent to his or her GCASH account.

Airtel Mobile Money is a core offering of Airtel which offers more than money transfer services. By July 2012, Airtel Mobile Money had been launched in 14 countries where Airtel operates. This follows successful improvements to the previous product called Zap. Airtel Mobile Money enables customers to send money, pay bills, buy airtime, pay online and also receive batch payments. With over 11 million registered customers representing about 20% of Airtel Customers, Airtel Money is intended to service the unbanked population. Airtel Mobile Money is set up as a separate operation within the Airtel business. It uses an internally developed application which enables both STK and USSD access. It is aiming to introduce new relevant financial products, mainly savings and insurance.

Payment Innovation: Rise of Mobile Payments and Alternative Payment Networks.

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 noncommercial payments from one person to another, or commercial payments to a small scale merchant. Second, is for goods or services purchased over the internet on a mobile device. The third option is at point of sale (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 app to generate barcodes, or a QR Code that allows the user to pay for something from funding source associated with the mobile wallet. Other options connect a virtual wallet with an email address or username and password.

Mobile payment systems are designed to create a system of disintermediation where the traditional payment networks and financial institutions are removed from the payment system. In *Overview of Mobile Payments in the United States* (Banking & Financial Services Policy Report, Volume 32, #8, August 2013), Erin F. Fonté writes:

> The most famous and successful company to achieve disintermediation from the established credit/debit card networks and processors is Square, a mobile POS startup co-founded by Twitter founder Jack Dorseyand launched in 2009. The initial goal of Square was to use a plug-in device for an iPhone or iPod (called a "dongle," and, not surprisingly, square in shape) that turns the mobile device into a mobile POS terminal. Square has been one of the most successful non-FI entrants into the payments space since PayPal, and as of June 2012, was processing $6 billion in payments annually. After seeing the success of Square, the companies that manufacture POS hardware and software created their own mobile POS devices. Verifone created its mobile POS device called Sail. Intuit, the company that created QuickBooks, launched GoPayment, a mobile POS device and virtual signature service that integrates with QuickBooks. PayPal launched PayPalHere.
>
> Disintermediation at the wallet refers to the current race by several companies to create a virtual wallet in which all of the payment cards in the average person's wallet—debit cards, credit cards, store gift cards, stored value cards—are housed in a virtual wallet app on the purchaser's smart phone. The smart phone is then used as the payment device that will interact with the POS for a proximity payment or to conduct a remote payment.
>
> There is currently a lot of time and money being invested by major credit card networks, mobile network operators (such as AT&T, Verizon, T-Mobile, and Sprint), major banks, major alternative payments providers (such as PayPal), and major technology companies (such as Google) to create and corner the market

on the mobile wallet. Although there are several other mobile wallet startups, the activities of mobile wallet providers Isis, Google Wallet, and PayPal are currently garnering a lot of attention. Isis is a joint venture between AT&T, T-Mobile, and Verizon, but is also partnered with Visa, MasterCard, and American Express. JPMorgan Chase, Capital One, and Barclaycard have agreed to issue cards for the wallet. Google Wallet involves MasterCard and payment processor First Data Corporation, and Sprint Nextel is the designated mobile network operator (but Google Wallet only works on Sprint mobile devices). Google Wallet is also going to include some form of coupon or offer redemption, and may be expanded to include loyalty and rewards components as well. The PayPal wallet just gained major publicity by announcing a partnership with Discover to bring PayPal's digital wallet and payment services to millions of merchants in the Discover network, with services currently scheduled to roll out in 2013. Mobile payments industry pundits are waiting to see what Apple does on the mobile payments/mobile wallet front. Apple's recent announcement of Passbook, along with confirmed rumors that Apple will include NFC technology in the iPhone 5, lead industry observers to speculate as to whether Apple has its own mobile wallet offering in mind given that it manufactures the iPhone. And the recently announced Merchant Customer Exchange (discussed earlier in this article) is a merchant-created mobile wallet initiative.

According to the Payments Strategies Group at the Federal Reserve Bank of Boston Starbucks is viewed by analyst and industry trade reports as a very successful model of a closed loop mobile payment model. Starbucks enables customers to utilize a mobile app that generates a QR code that can be scanned by the in store POS reader. Mobile phones account for 10% of Starbucks' U.S. transactions. Starbucks couples this mobile app with their customer loyalty rewards system creating additional incentives so consumers will use the app. Based on this success other merchants are also rolling out closed loop mobile payment apps. Other retailers offer customers who use mobile payment apps the opportunity to order in advance of arriving at the physical location of the store so that the consumer does not have to wait in line for their purchase.

Between December 2011 and January 2012, the Federal Reserve Board conducted a survey of consumers concerning the use of mobile financial services (http://www.federalreserve.gov/econresdata/mobile-devices/files/mobile-device-report-201203.pdf). The following are brief findings from their report:

1) Mobile phones and mobile Internet access are in widespread use.

   a) 87 percent of the U.S. population has a mobile phone.

   b) 44 percent of mobile phones are smartphones (Internet-enabled).

   c) 84 percent of smartphone users have accessed the Internet on their phone in the past week.

2) The ubiquity of mobile phones is changing the way consumers access financial services.

    a) 21 percent of mobile phone owners have used mobile banking in the past 12 months.

    b) 11 percent of those not currently using mobile banking think that they will probably use it within the next 12 months.

    c) The most common use of mobile banking is to check account balances or recent transactions (90 percent of mobile banking users).

    d) Transferring money between accounts is the second most common use of mobile banking (42 percent of mobile banking users).

3) Mobile phones are also changing the way consumers make payments.

    a) 12 percent of mobile phone owners have made a mobile payment in the past 12 months.

    b) The most common use of mobile payments was to make an online bill payment (47 percent of mobile payment users).

    c) 21 percent of mobile payment users transferred money directly to another person's bank, credit card, or PayPal account.

4) Perceptions of limited usefulness and concerns about security are holding back the adoption of mobile financial services.

    a) The primary reason why mobile phone users had not yet adopted mobile banking was that they felt their banking needs were being met without the use of mobile banking (58 percent).

    b) Concerns about the security of the technology were the primary reason given for not using mobile payments (42 percent) and the second most common reason given for not using mobile banking (48 percent).

    c) More than a third of mobile phone users who do not use mobile payments either don't see any benefit from using mobile payments or find it easier to pay with another method.

5) The "underbanked" make significant use of mobile financial services.

   a) The underbanked make comparatively heavy use of both mobile banking and mobile payments, with 29 percent having used mobile banking and 17 percent having used mobile payments in the past 12 months.

   b) 62 percent of the underbanked who use mobile payments have used it to pay bills.

   c) 10 percent of the completely unbanked reports using mobile banking in the past 12 months, and 12 percent have made a mobile payment.

An April 2013 report from Business Insider found the following:

- In-store mobile payments nearly quadrupled last year: eMarketer has estimated in-store mobile payments as adding up to $640 million in transaction volume in the U.S., up from $170 million in 2011. However, this figure does not include swipes on mobile credit card readers like Square and PayPal Here, only consumer-side mobile payments.

- Card readers are building up real scale: Square's mobile payments volume rose to $10 billion in 2012, up from $2 billion in 2011. Starbucks is switching its credit and debit card processing to Square, and as of January 2013 accepts the "Square Wallet" app at 7,000 locations.

- Mobile payments as part of mobile commerce are also exploding**:** PayPal processed some $14 billion in mobile payments last year, evidence of mobile catching on as a transactional platform. PayPal hopes to build a merchant-powered network based on the ubiquity of PayPal as a payment and money transfer platform. PayPal users are already able to pay at thousands of traditional stores by keying in their mobile number and a PayPal PIN selected online (or in their PayPal app).

- Credit card companies are getting in on the action: Credit card companies have responded by making aggressive moves to enter the space. Visa (V.me), and American Express (Serve) have each introduced digital wallet-like products, MasterCard's PayPass is an NFC-enabled system that is also integrated with the "Google Wallet" app, and Discover has opted to partner with two of the bigger names in the digital payments space ("Google Wallet, and PayPal).

- In the early stages**:** As of year-end 2012, only 7.9 million U.S. consumers (less than 90 percent of the total) had adopted a consumer-facing NFC-compatible system like "Google Wallet," or apps that use QR codes or other methods to generate a payment.

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*

Legal & Regulatory Issues.

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 institutions, but certain provisions apply to "any person."	**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 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	**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

nonbanks engaged in financial activities.		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.		

In California, most mobile payment systems that rely on the transfer of money from one party to another fall under the regulatory supervision provided in the MTA. Most other states also have statutes regulating domestic and international money transfer. Like California, most, if not all, states require that an operator wishing to do business in that state must also be licensed in that state. This creates a requirement for licensing in all 50 states if a mobile payments provider wants to have full market access across the U.S. California's MTA, like most states is broad in its interpretation of what factors constitute money transmission for sake of licensing. The broadness of the statute has raised a number of questions, some of which were addressed by AB 786, referenced earlier in this document. However, other questions have yet to be resolved. For example, what effect, if any occurs when the mobile payment app is used to pay for a retail goods or services. Traditionally, money transmission activity involved sending money from A to C via B, not sending money in exchange for goods or services. If a consumer shops via an online marketplace that fulfills orders via third parties does acceptance of money from the consumer make the online marketplace a money transmitter under the law?

Another issue and one that may hold back some consumers from the use of mobile payments is how does the use of a mobile payment app or system change how disputes are resolved in the case of fraudulent payments or unauthorized charges. Mobile payment services typically function by linking to one or more payment sources. Many mobile payment platforms allow consumers to choose among several different funding sources for payment, such as a credit card, debit card, bank account, or mobile phone account. For instance, a particular payment application on a smartphone may be linked to a credit card so that the credit card is charged when the consumer pays using that application. Depending on the payment source used to fund the mobile payment (e.g. credit card versus prepaid card versus mobile carrier billing), consumers may or may not have statutory protections regarding unauthorized charges. The Federal Trade Commission convened a mobile payments workshop to look at these issues and found the following:

> Mobile payment users may not recognize that their protections against fraudulent or unauthorized transactions can vary greatly depending on the underlying funding source. Generally, credit cards provide the strongest level of statutory protection, capping liability for unauthorized use at $50. If a mobile payment is linked to a bank debit card, a consumer's liability for unauthorized transfers is limited to $50 if reported within two business days, and up to $500 for charges reported after two business days. However, if consumers do not report unauthorized debit transactions on their bank account within 60 days after their periodic statement is mailed to them, they can face unlimited liability, whether or not the charges result from a lost or stolen card or another electronic transfer. Other types of funding mechanisms, however, do not have the same statutory protections as credit cards and debit cards. For example, there are no federal statutes besides the FTC Act that protect consumers from unauthorized charges if their mobile payment mechanism is linked to a pre-funded account or stored-value card such as a gift card or general purpose reloadable card, also known as a pre-paid debit card. At the workshop, one consumer group advocated for the extension of the additional federal protections afforded to credit and debit cards to these financial products, specifically pointing out the inequitable situation caused when these cards are used as payment vehicles for mobile payments. Certainly, the inconsistency in protections complicates the landscape for consumers who may not understand the differences between these funding sources.

Additionally, the FTC looked at data security and mobile payments and found:

> Another key concern for consumers when making mobile payments is whether or not their sensitive financial information can be stolen or intercepted. As noted above, a Federal Reserve study reported that 42% of consumers were concerned about data security, and this concern was the most cited reason why consumers have not used mobile payments. Specifically, consumers were concerned about

hackers gaining access to their phone remotely, or someone intercepting payment information or other data. Given that a major impediment to consumers' adoption of mobile payment technologies is the perceived lack of security, the incentives for industry to get security right should be strong. Nevertheless, although the technology to provide enhanced security in the mobile payments market is available, it is not clear that all companies in this market are employing it.

Technological advances in the mobile payment marketplace offer the potential for increased data security for financial information. A number of workshop panelists described how, under the traditional payment system, financial data is often transmitted or stored in an unencrypted form at some point during the payment process. By contrast, mobile payment technology allows for encryption throughout the entire payment chain, which is often referred to as "end-to-end encryption." Additionally, under the traditional payment system, financial information on a card's magnetic stripe that is transmitted from a merchant to a bank consists of the same information sent each time a consumer makes a payment. Thus, if this information is intercepted, it can be used repeatedly for subsequent, unauthorized transactions. Mobile payments, however, can utilize dynamic data authentication, whereby a unique set of payment information is generated for each transaction. Accordingly, even if the data is intercepted, it cannot be used for a subsequent transaction. In the mobile context, payment information also can be stored on a secure element that is separate from the rest of a phone's memory, preventing hackers who access a phone operating system from compromising sensitive financial information.

Mobile payment providers should increase data security as sensitive financial information moves through the payment channel, and encourage adoption of strong security measures by all companies in the mobile payments chain. Consumers may be harmed when less responsible companies use insecure methods to collect and store payment information.

Further, the reputation of the industry as a whole may suffer if consumers believe lax security practices are the norm. Many federal and state laws also impose data security requirements on businesses that collect and use financial information and other sensitive data.

While numerous laws overlap and exist that already govern portions of the mobile payments process, many of these laws still operate and respond the same as if the technology behind the business activity has not changed.

How will the source of the funds used to make the mobile payment (e.g., bank account, credit card, prepaid credits, etc.) affect the answers to the questions above?

Mobile Payments Security & Consumer Privacy

While implementation and adoption by merchants remain significant challenges to broader use of mobile payments, consumer concerns regarding security also hold back greater use. In a Federal Reserve study concerning the use of mobile payments by consumers, 42% of consumers cited concerns with security as the primary reason for not using mobile payments. The Federal Trade Commission (FTC) concluded in a staff report, *Paper, Plastic…or Mobile*, that

> Given that a major impediment to consumers' adoption of mobile payment technologies is the perceived lack of security, the incentives for industry to get security right should be strong. Nevertheless, although the technology to provide enhanced security in the mobile payments market is available, it is not clear that all companies in this market are employing it.

Additionally, the FTC Workshop of Mobile Payments gathered stakeholders together to discuss the emerging policy issues relating to mobile payments. Their discussion revealed that in the traditional payments system consumer financial information is at some point in the payments process stored or transmitted unencrypted, but that the rise of mobile payments has the ability to ensure that consumer data is encrypted throughout the process. Further, the information on mag strip cards is static so that once it is captured it could be used repeatedly. On the other hand, as mentioned earlier mobile payments can utilize dynamic authentication where each transaction generates unique data.

In the traditional payments space banks, merchants, and payment card networks have access, or potential access to information about the consumer. In the mobile payments space, in addition to the traditional actors, payments include operating system and software manufactures, hardware manufacturers, mobile phone carriers, application developers and loyalty program administrators. Furthermore, the FTC found:

> For example, when a consumer pays using a credit or debit card during a traditional point of sale purchase, the merchant typically has detailed data about the products the consumer purchased, but does not have the consumer's contact information. Conversely, the financial institution that issued the card has a consumer's contact information and the name of the merchant where the consumer shopped, but generally does not have information about specific purchases. Mobile payments can allow multiple players within the mobile payments ecosystem to gather and consolidate personal and purchase data in a way that was not possible under the traditional payments regime. Such consolidation may provide benefits to consumers, such as helping merchants

> offer products or services that a consumer is more likely to want. This collection of data may also help reduce the incidence of fraud. However, these data practices also raise significant privacy issues.

In a current transaction via the use of a credit card a merchant would get very little information about the consumer as they are restricted in how they collect data through state law, credit card acceptance agreements, and customer loyalty considerations. Mobile payment systems could provide avenues for merchants to discover shopping habits of the consumer that could be used for marketing or analytical purposes. California is very clear on prohibiting the collection of personal information by merchants from consumers when using credit cards, but this is potentially clouded when a mobile payment system is used. Given that traditional payments are still a near universal option, consumers still have the ability to avoid mobile payments completely without hindering their ability to purchase goods and services.

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.

On November 18, 2013 the United States Senate Committee on Homeland Security and Governmental Affairs conducted a hearing "Beyond Silk Road: Potential Risks, Threats and Promises of Virtual Currencies." Some excerpts from testimony at that hearing are reprinted below:

Mythili Raman, Acting Assistant Attorney General, Criminal Division:

> Early centralized models, where the currency is controlled by a single private entity, have expanded and now encompass a wide range of business concepts. Some centralized virtual currencies take the form of digital precious metals, such as e-Gold and Pecunix, where users exchange digital currency units ostensibly backed by gold bullion or other precious metals. Others exist within popular online games or virtual worlds, such as Farmville, Second Life, or World of Warcraft. Still others are online payment systems such as WebMoney and Liberty Reserve, which are available generally outside of specific online communities and denominate users' accounts in virtual currency rather than U.S. Dollars, Euros, or some other national currency. Decentralized systems such as Bitcoin, which have

no centralized administrating authority and instead operate as peer-to-peer transaction networks, entered the scene relatively recently but are growing rapidly. A network of sites and services, including exchangers who buy and sell virtual currencies in exchange for national currencies or other mediums of value, have developed around virtual currency systems, as well.

Criminals are nearly always early adopters of new technologies and financial systems, and virtual currency is no exception. As virtual currency has grown, it has attracted illicit users along with legitimate ones. Our experience has shown that some criminals have exploited virtual currency systems because of the ability of those systems to conduct transfers quickly, securely, and often with a perceived higher level of anonymity than that afforded by traditional financial services. The irreversibility of many virtual currency transactions additionally appeals to a variety of individuals seeking to engage in illicit activity, as does their ability to send funds cross-border.

Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury:

Indeed, the idea that illicit actors might exploit the vulnerabilities of virtual currency to launder money is not merely theoretical. We have seen both centralized and decentralized virtual currencies exploited by illicit actors. Liberty Reserve used its centralized virtual currency as part of an alleged $6 billion money laundering operation purportedly used by criminal organizations engaged in credit card fraud, identity theft, investment fraud, computer hacking, narcotics trafficking, and child pornography. One Liberty Reserve co-founder has already pleaded guilty to money laundering in the scheme. And just recently, the Department of Justice has alleged that customers of Silk Road, the largest narcotic and contraband marketplace on the Internet to date, were required to pay in bitcoins to enable both the operator of Silk Road and its sellers to evade detection and launder hundreds of millions of dollars. With money laundering activity already valued in the billions of dollars, virtual currency is certainly worthy of FinCEN's attention.

That being said, it is also important to put virtual currency in perspective as a payment system. The U.S. government indictment and proposed special measures against Liberty Reserve allege it was involved in laundering more than $6 billion. Administrators of other major centralized virtual currencies report processing similar transaction volumes to what Liberty Reserve did. In the case of Bitcoin, it has been publicly reported that its users processed transactions worth approximately $8 billion over the twelve-month period preceding October 2013; however, this measure may be artificially high due to the extensive use of automated layering in many Bitcoin transactions. By way of comparison, according to information reported publicly, in 2012 Bank of America processed

> $244.4 trillion in wire transfers, PayPal processed approximately $145 billion in online payments, Western Union made remittances totaling approximately $81 billion, the Automated Clearing House (ACH) Network processed more than 21 billion transactions with a total dollar value of $36.9 trillion, and Fedwire, which handles large-scale wholesale transfers, processed 132 million transactions for a total of $599 trillion. This relative volume of transactions becomes important when you consider that, according to the United Nations Office on Drugs and Crime (UNODC), the best estimate for the amount of all global criminal proceeds available for laundering through the financial system in 2009 was $1.6 trillion. While of growing concern, to date, virtual currencies have yet to overtake more traditional methods to move funds internationally, whether for legitimate or criminal purposes.

Jeremy Allaire, Chairman and CEO, Circle Internet Financial

> All of these risks and opportunities require that governments around the world take a proactive stance with regards to guidance around digital currency. It should be noted that digital currency has expanded globally due to different regulatory standards and attitudes overseas, particularly in the European Union and China. Several foreign firms have also refused to accept U.S. customers due to the lack of clear regulatory guidance. We do not think that it is in anyone's best interest for digital currency to become an offshore industry, or an industry dominated by China. No other country in the world has a startup entrepreneurial culture like the United States. We should protect and embolden this spirit that creates economic growth and provides us with a considerable global advantage. In terms of U.S. regulation, it appears to me that Federal and State regulators generally appear to have ample statutory authority to adopt regulations and take enforcement actions as necessary to protect consumers and ensure responsible conduct in the world of Bitcoin commerce, that their actions to date have been constructive, and that we stand ready to assist them in their ongoing efforts to adapt their regulatory tools to new digital currency.

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.

For a more detailed overview of digital currency and Bitcoin see testimony of Jerry Brito, Senior Research Fellow, Mercatus Center at George Mason University which can be found at:

http://www.hsgac.senate.gov/download/?id=0dcd748d-035a-4c0f-b695-7680adc2425d.

Policy Questions for Consideration:

As policy makers continue to examine the evolving nature of mobile payments the following questions should be considered:

1. Are the mobile payment services appropriately regulated as mere communication services or as money transfer services (or as a hybrid, or even as some other type of service)?

2. Who is responsible for providing consumer disclosures for products and services requiring such disclosures, and what protocols will apply to proving that these disclosures were given?

3. What privacy rules apply to, and who is responsible for, security of customer data? Should consumers be allowed to select higher or lower levels of identity protection as a matter of their own convenience?

4. To what extent should consumers be responsible for unauthorized or fraudulent mobile payments if they handle their mobile devices carelessly or share their identification information with others?

5. How will theft of mobile devices or hacking of customer authentication data affect responsibility for unauthorized payments?

6. What protocols are essential to ensure accuracy of payment data in transmission?

7. What consequences should follow if the data are compromised in transmission?

8. Should consumer disclosures be focused on the liabilities and risks associated with different funding options (Credit card vs Debit, vs ACH) for mobile payments?

9. Should the MTA be amended to address payments that go for retail transactions vs straight money transmission from A to B?

10. Should those accepting or facilitating mobile payments be allowed to use customer data for marketing or other purposes? Should consumers have a right to opt-in or opt-out of such data sharing?

11. To what extent must mobile payment services be accessible to the disabled, and how might this be achieved?

12. Who will keep records of mobile payment transactions, and how? How may consumers obtain these records?

13. What obligations and liabilities result when mobile payment systems "go down"? Is unavailability of a mobile payment system the equivalent of denying consumers the right to their funds?

14. Given that all new mobile payment options operate using existing payment infrastructure are new rules needed at all?