U.S. MOBILE PAYMENTS LANDSCAPE – TWO YEARS LATER

Marianne Crowe, Susan Pandy, and Elisa Tavilla, Federal Reserve Bank of Boston

Cynthia Jenkins, NACHA[1]

May 2, 2013

[1] At the time the white paper was written, Cynthia (Merritt) Jenkins was employed at the Federal Reserve Bank of Atlanta.

The authors would like to thank the members of the Mobile Payments Industry Workgroup for their valuable contributions to the work effort and insightful ideas and comments that are the foundation of this paper. The views expressed in this paper are solely those of the authors and do not reflect official positions of the Federal Reserve Banks of Atlanta or Boston, the Federal Reserve System or NACHA.

Table of Contents

I. Executive Summary

In 2010, the Federal Reserve Banks of Boston and Atlanta (FRB), through their Payment Strategies and Retail Payments Risk Forum groups, convened the first Mobile Payments Industry Workgroup (MPIW)[2] to discuss the benefits and obstacles to developing a successful U.S. retail mobile payments system. The MPIW meets with the FRB three to four times per year to discuss mobile industry developments and related issues. In response to expanded use of mobile payments and increasing interest among mobile stakeholders, the FRB expanded the MPIW's scope in 2012 to enable broader participation from groups with a specific interest in mobile payments adoption such as merchants, vendors, start-ups and regulators. The FRB will maintain this approach to ensure ongoing comprehensive discussion within the MPIW that encompasses prospective issues of collective concern.

After multiple meetings during 2010 and 2011, the group dialogues were captured in a white paper published in March 2011, *Mobile Payments in the United States: Mapping out the Road Ahead*.[3] Since the first paper was published, the mobile payments industry has undergone considerable changes. Notable changes include increasing convergence of channels that has blurred the lines between online and physical commerce. A broad range of technology developments are accelerating this convergence, including mobility, analytics, cloud, broadband and social networks.

The mobile device has become a pivotal driver in creating a dynamic marketplace that is bringing diverse companies and sectors together, both as competitors and collaborators and across traditional boundaries of industry and technology. Such changes have expanded the possibilities for new products, services and types of companies in this emergent commerce environment. The mobile device has introduced unique qualities such as the portability of the technology and additional factors inherent to the mobile device, including multimedia services, GPS, Internet access, mobile telephony, camera, and social media, which could all impact the payments environment.

In the retail payments space, these dynamic changes have created a market that offers digital and mobile wallets, near field communication (NFC) and cloud-based point-of-sale (POS) solutions, mobile apps, and Quick Response (QR) barcodes. The merging of these technologies with platforms (POS, online, other remote), uses (consumer-to-business (C2B), person-to-person (P2P)), new payment methods (virtual prepaid, direct carrier billing (DCB)), and many cross-industry players further changes the market for

[2] Use of the MPIW in this paper represents the existing workgroup or a modified version of the group in the future. The original MPIW included 22 members, representing various mobile payments industry sectors, and now has 42 members, including several merchants. MPIW member information can be found at http://www.bostonfed.org/bankinfo/payment-strategies/mpiw/index.htm.

[3] http://www.bostonfed.org/bankinfo/payment-strategies/publications/2011/mobile-payments-mapping.htm.

mobile payments. Large banks are collaborating through joint ventures, partnerships, consortiums, and bilateral relationships with mobile network operators (MNOs), card networks, retailers, mobile solution providers, and well-funded innovative start-ups to implement numerous mobile payment solutions. In some instances, stakeholders are experimenting with multiple approaches to see what consumers will use, and what merchants will accept.

These rapidly developing innovations in the mobile payments landscape created the need for the FRB and MPIW to update the original white paper to inform the payments industry concerning the evolution of a ubiquitous mobile payments system. The new report reflects what the FRB has learned from the MPIW, with the intent that it could inform policymakers and regulators, as well as the mobile payments industry.[4] The key findings note that while the mobile landscape remains characterized by fragmentation, various developments have gained importance. These include the convergence of channels, the role of nonbanks, the formation of new relationships, the unresolved security and privacy issues, and the increasing role of data monetization. As this ecosystem matures it will challenge new entrants in their ability to achieve scale and sustainability, while technology will continue to proliferate and drive improved efficiencies and innovation. The need for interoperability, industry guidance, and standards will become even more critical to ensure a secure and cost-efficient ecosystem. Creation of an open model could become a means to a secure an interoperable mobile payment system capable of building scale through consumer and merchant adoption. However, in this competitive and rapidly innovating market, new solutions have not waited for a uniform open model to become available.

Based on these findings, the MPIW updated the original strategic principles and introduced new themes. The paper expands on the benefits and challenges marking the landscape in light of recent developments and examines earlier considerations to determine if they are still relevant based on the many changes in the mobile payments marketplace. Finally, the paper revisits the long-term vision for POS mobile payments, including risk and regulatory concerns, along with implications for all stakeholders.

II. Changes in the U.S. Mobile Payments Ecosystem: 1Q2011 to 4Q2012

This section provides an overview of the accomplishments and challenges faced by primary mobile stakeholders over the last two years and outlines new infrastructures and capabilities offered in this span of time. The discussion includes the following stakeholders: MNOs, smartphone/terminal manufacturers,

[4] This paper provides the MPIW's assessment of the state of the U.S. mobile payments industry, but does not reflect any agreement among the MPIW members as to the manner in which mobile payments may be transacted.

mobile operating system providers, payment processors, alternative payment service providers, card and ACH networks, financial institutions (FIs), merchants, regulators and consumers.

MNOs

In the last two years, MNOs have partnered with banks, card networks and technology companies to pilot mobile payment solutions. New business models have emerged more quickly than some MPIW members had originally expected. For example, three of the largest MNOs formed an NFC mobile wallet joint venture (Isis) with several FIs and a card network. Sprint partnered with Google and Citi to launch Google Wallet.[5] Because MNOs typically subsidize and certify handsets on their networks, they have maintained control over which service providers can access the secure element[6] on mobile phones in their networks, although not without consequences to mobile service providers and ultimately to consumers by limiting their access in some cases.[7]

The mobile carrier's approach has some historical context. Before Apple and Google introduced their smartphone platforms and app stores, mobile subscribers were limited by their MNO in terms of applications that could be downloaded to their mobile phones and how the apps could be purchased (a.k.a. the "walled garden"). The introduction of app stores managed by Apple and Google, and the quick consumer acceptance of these app stores changed this mobile app dynamic. These factors reduced the MNOs' leverage and control of software on the handsets and gave customers options and capabilities that were unavailable through the MNO ecosystem.

Smaller mobile carriers have yet to engage in POS mobile payments, but some are exploring opportunities to address the needs of the unbanked and underbanked consumer markets with prepaid phones, mobile financial services, and other innovative use cases.

Smartphone/Terminal Manufacturers and Mobile Operating System Providers

The Google Android and Apple iOS mobile operating systems continue to have the largest share of smartphone subscribers, with 52.3 percent and 37.8 percent respectively.[8] While few mobile phones are currently enabled for use with either SIM or embedded NFC secure elements, more handset manufacturers are including these capabilities as a basic component. At the end of 2011, 45 global

---

[5] Google Wallet is a partnership between Sprint, Google, Citibank and MasterCard. Isis Wallet is a consortium comprising AT&T, Verizon, T-Mobile, Chase, Capital One, Discover, Barclaycard, Visa, MasterCard and American Express.

[6] A secure element is an encrypted smart card chip embedded in a mobile phone that safely stores and executes mobile payment applications and stores associated payment credentials and financial data.

[7] At this time, only selected Android phones work with the two wallets. The Apple iPhone is not NFC-enabled.

[8] As of the date of this publication. See http://gigaom.com/2013/03/06/comscore-android-still-top-us-smartphone-os-but-iphone-top-smartphone-and-ios-gaining/.

handset manufacturers announced plans to add NFC/SIM cards to their mobile phones,[9] and Isis planned to have up to 20 NFC-enabled mobile phones available by the end of 2012.[10] Assuming that MNOs activate NFC in the handsets, these efforts could begin to alleviate some barriers to adoption of NFC mobile payments.

Early industry expectations assumed that the majority of POS terminals would have been upgraded to accept contactless NFC payments by 2013. For several reasons this has not been the case. The three big terminal manufacturers, Verifone, Ingenico, and Equinox, have incorporated NFC functionality into their new POS terminals, but merchant implementation has been slow.[11] Rolling out new hardware to enable NFC on every POS terminal, changing POS software, and upgrading POS terminals to support NFC is not only costly, but also an operational challenge. While implementation of the Google and Isis NFC mobile wallets may have helped gain traction with some merchants, many others still must decide if and when to invest in upgrading their POS terminals to NFC.

Payment Processors and Alternative Payment Service Providers

Payment processors, online payment service providers, mobile software solution vendors, and application and hardware developers are exploring new market opportunities and innovations in the mobile payments space, ranging from digital wallets to dongle plug-in smartphone card readers. They continue to provide the enabling technology for mobile payments or to serve as intermediaries in the payments supply chain.

Google's first mobile wallet stored payment credentials issued by Citi MasterCard in a secure element embedded in the mobile phone. Google adapted its business model in response to limited transaction volume and introduced a hybrid mobile/digital wallet that stored a virtual MasterCard number associated with the mobile phone in the secure element. The virtual card does not correspond to any specific payment card account, but is a proxy for the real account credentials stored in the cloud and is used for NFC transactions at the POS. This change enabled Google Wallet customers to store and pay with credit and debit card credentials issued by any FI. It also demonstrated Google's flexibility and capacity to adapt quickly to overcome barriers in the market. In contrast, FIs cannot adapt as quickly to market changes because of competing needs for resources and funding within their organizations, impacts to legacy systems, financial impacts to their interchange revenue, and regulatory requirements.

---

[9] GSMA announced at its Mobile Asia Congress that it has commitments from 45 MNOs worldwide to implement SIM-based NFC. See http://www.nfcworld.com/2011/11/16/311363/45-mobile-operators-commit-to-nfc/.

[10] See http://www.wired.com/gadgetlab/2012/10/isis-sets-oct-22-launch-date/. The Isis Wallet uses a SIM-based secure element; Google Wallet uses an embedded secure element.

[11] See http://gigaom.com/2011/03/04/verifone-all-new-point-of-sale-terminals-will-get-nfc/ and http://www.finextra.com/news/fullstory.aspx?newsitemid=23494.

Apple took a different approach and chose not to deploy NFC for the iPhone. Instead, Apple created a non-payment app-based mobile wallet called Passbook that serves as a repository for boarding passes, movie tickets, retail coupons, and loyalty cards. Passbook provides a platform that supports third-party integrations, including digital wallet providers, for a closed-loop network of merchants. It enables customers to select, download and store QR codes from registered merchants' apps and access them as needed to pay at the POS or at a barcode scanner. By storing non-payment accounts on their mobile phones consumers can reduce the need to carry paper or plastic.

The convergence of online, mobile, and physical POS channels has provided alternative payment providers with the opportunity to develop solutions and applications that leverage a range of technologies, such as cloud, QR codes, and geo-fencing.[12] Unlike NFC, cloud-based and QR code technologies are less dependent on mobile carriers because they rely on software that does not store payment information on the mobile device, and therefore does not require access to the mobile network. However, Internet access is typically necessary to complete a transaction.

Payment Cards and ACH Networks

Credit: The major U.S. credit card networks face growing competition from other mobile stakeholders. They continue to actively pursue multiple mobile payment efforts to gain market share. In recent years, the card networks have introduced a variety of strategic initiatives and acquisitions that demonstrate the importance they place on mobile in both developed and developing countries. They have leveraged their ability to connect services through their standardized global networks. They have formed strategic partnerships with MNOs, issuers, merchants and mobile payment technology vendors, as well as investing in mobile start-ups. They have been complementing plastic cards with mobile payments at the POS, with prepaid, transit, and P2P. A notable change over the past two years is their new focus on cloud-based digital wallets and merchant loyalty programs. And, while following different strategic paths to implementation of mobile payments, the card networks continue to promote and support NFC, approving more NFC mobile phones for their services globally, participating in the Google and Isis mobile wallet programs in the U.S., and engaging in NFC initiatives in Europe and Asia.[13]

---

[12] In the cloud model, payment credentials are stored in a remote file server (cloud), not in the secure element in the mobile phone. In one use case, a consumer registers and then pays for purchases by entering his mobile phone number and PIN at the merchant POS terminal. Some cloud-based digital wallets use location-based technology in the mobile phone. Geo-fencing leverages location-based services (such as GPS and RFID) to create a virtual perimeter in which a mobile device can be recognized and a notification generated. For example, Square uses geo-fencing to notify a merchant when a customer has entered the store.

[13] According to one mobile payments stakeholder, "NFC is still the fastest, quickest and best user experience. It is the least clunky and works in different environments with no connectivity. NFC is fit for the purpose, which is NFC payments." James Anderson, SVP Mobile, MasterCard, *NFC Times*, November 7, 2012.

Debit/Prepaid: Debit card networks are experiencing growth in mobile payment transactions processed through virtual prepaid access accounts, prepaid card systems and online payment providers. Online and mobile prepaid options offer the unbanked and underbanked access to financial services without requiring a traditional bank account. Two recent major prepaid initiatives include Green Dot, which in 2012 purchased a bank and introduced its GoBank account,[14] and Bluebird, a digital/mobile prepaid account offered by American Express and distributed through Walmart.[15] As prepaid products grow, the Consumer Financial Protection Bureau (CFPB) and other regulators will continue to monitor their progress because of concerns about excessive fees and lack of transparency for consumers regarding such fees and other card usage terms and conditions. Any potential regulatory actions should be evaluated to determine their impact to the growth of prepaid debit accounts and the prepaid debit model for mobile payments.

ACH: ACH is a major payment network that competes with card networks in the United States. Only recently have mobile ecosystem stakeholders begun to actively consider ACH as a viable alternative in the mobile/digital wallet evolution. Use of the ACH network for mobile payments continues to grow as a segment of online ACH payments. Currently, the majority of these transactions are comprised of bill payments. FIs and non-bank payment providers are developing Internet and mobile applications to implement P2P payment products that are processed via the ACH network, creating opportunity for future growth as more consumers use their smartphone apps and browsers for mobile P2P and Internet purchases. Several companies in the mobile payments ecosystem are pursuing solutions that leverage the ACH network to clear and settle mobile payments and offer ACH to consumers as an alternative payment method for retail purchases. This use of the ACH at the POS also responds to merchant demands for less costly alternatives to credit and debit. Ultimately, the ACH will be another component for expanding consumer choice in the future, particularly for recipients of electronic benefits and transfers (EBT) and other government benefit payments.

Financial Institutions

FIs face many competitive pressures from other banks and nonbanks, particularly as the banking industry tries to determine its role in the fast-paced mobile payments environment. FIs' current moderate

[14] GoBank is an FDIC-insured mobile-only bank that is accessible using a mobile app. It includes a Visa debit card linked to a traditional checking account, but it does not issue checks. GoBank has been available in limited launch since January 2013. See www.gobank.com.

[15] Bluebird is an FDIC-insured alternative to debit and checking accounts that can be linked to a mobile app which allows consumers to make mobile deposits to their prepaid account, make mobile bill payments, or send P2P payments. See www.bluebird.com.

approach to implementing mobile payment solutions stems from the economic consequences, uncertainty, and risk aversion created by the recent financial crisis and in response to broad financial regulatory reform. The largest FIs have taken different, but overlapping, strategic directions and approaches to building their business models. A few have participated in NFC wallet initiatives through collaboration with card networks and MNOs. Beyond NFC, FIs have also formed relationships with start-ups to test other mobile payment solutions such as cloud-based digital wallets, QR codes and mobile device card acceptance applications for small businesses. Financial institutions are simultaneously expanding their mobile banking platforms to include mobile remote deposit capture (mRDC), P2P payments, and corporate mobile banking services. P2P payments have helped FIs expand their role as a facilitator of mobile commerce by enabling money transfers between FIs or through retail payment networks.[16]

Financial institutions have the chance to leverage their reputation as trusted payment providers and effective risk managers to strengthen their role in the mobile payments ecosystem. Various studies have shown that consumers have more trust in mobile payment solutions driven by FIs and/or credit card companies than alternative providers.[17] Financial institutions have broad experience that puts them at an advantage to drive and shape consumer acceptance – from due diligence, know your customer, authentication and authorization, corporate security, fraud monitoring and prevention tools, risk management policies and systems, to anti-money laundering tools. Partnering with viable nonbank mobile ventures can complement the FIs' strengths and generate innovation, technology and a better understanding of the market dynamics. Strong customer marketing and communication efforts can also help FIs succeed in the mobile space. However, if FIs cannot leverage their unique advantage as the trusted entity for consumer mobile payments, they risk being viewed by other participants simply as a utility that provides the transactions.

Merchants

Since the inception of the MPIW, merchants have expressed concerns related to the overall business case for mobile payments. Their concerns stem from the expanse of costs in comparison to the benefits of rolling out mobile contactless payments. These costs include, but are not limited to, processing, investment in terminal upgrades, chargebacks from card payments, security (including PCI compliance),

[16] Examples include clearXchange, a network between Bank of America, Wells Fargo and Citi that allows customers to send and receive P2P payments electronically, and Fiserv's PopMoney.

[17] Javelin Strategy & Research (March 2012). *Gang of Four (and Possibly Five) Apple, Google, Facebook, Amazon – and PayPal: Positioning for Payments in the New Mobile-Social Technology Era* and 2011 Fiserv Consumer Trends Survey. *Beyond Mobile Banking: It's Time to Stake the Claim for Mobile Payments*. Retrieved from http://www.flickr.com/photos/fiserv/6153751056/in/photostream.

and EMV implementation. [18] [19] In addition to cost considerations, merchants are concerned about rules and liability shifts that vary depending on how a payment is handled, for example, whether a transaction will be processed as card-present (CP) or card-not-present (CNP). As such, merchants of all sizes (e.g., big box retailer, quick-service restaurants (QSRs), small and micro-businesses), and across various segments, are experimenting with different mobile payment technologies to build cost-efficient POS solutions that enhance customer experience and lower costs.

Several retailers are offering closed-loop prepaid account solutions using QR code applications to make mobile payments. QR codes are non-proprietary and relatively quick and easy to implement. However, a customer still needs a custom app and QR code for each merchant or group of merchants, who must agree to a common set of technology standards and/or a common app. Recently, over 30 of the leading U.S. merchants formed the Merchant Customer Exchange (MCX)[20] to create a secure mobile platform with a common set of standards to reduce costs in the payments system, keep merchants' customer data securely with merchants, and provide their customers with a better shopping experience. According to public statements, the MCX solution will utilize barcode technology (i.e. QR codes) for mobile proximity payments.

Many QSRs are heavily franchised making it difficult for them to implement uniform payment solutions. However, several chain QSRs and drug stores that initially deployed NFC terminals to accept contactless cards are now leveraging those terminals to accept NFC mobile payments.

Merchants are generally positive about the business case for mobile, but regard it as a more holistic development of which payments is a small piece. Merchants see mobile as an opportunity to introduce competition and innovation in the payments market.

---

[18] EMV is a global specification for credit and debit payment cards based on chip card technology that defines requirements to ensure interoperability between chip-based payment cards and terminals. EMV chip cards contain embedded microprocessors that provide strong transaction security features and other application capabilities. The EMV specification encompasses credit, debit and contactless (card and mobile) payment transactions. The primary use for these chip-based cards is to perform payment transactions that store encryption data for authentication. As part of the transaction authorization, the card uses the data to prove it is authentic, thus preventing the use of stolen or cloned cards. For more information on EMVCo see http://www.emvco.com.

[19] U.S. EMV migration plans accelerated between mid-2011 and early 2012 when all four major card networks announced plans to migrate U.S. merchants and issuers to a more secure EMV chip payment environment – merchant acquirers must be ready by April 2013, liability shift for POS as of April 2015 and for automated fuel dispensers as of October 2017

[20] At the time of publication, MCX included the following merchants: 7-Eleven, Alon Brands, Bed Bath & Beyond, Best Buy, CVS/pharmacy, Darden Restaurants, DICK's Sporting Goods, Dillard', Dunkin' Brands, Gap, HMSHost, Hobby Lobby Stores, Hy-Vee, Lowe's, Meijer, Michaels Store., Publix Super Markets, QuikTrip, Sears, Sheetz, Shell Oil US, Sunoco, Target, Wakefern Food, Wal-Mart and Wawa.

Consumers

Growing smartphone ownership will influence stronger adoption of mobile banking and payments.[21] As consumers become increasingly adept at using smartphones (e.g., through downloading and using applications), this will likely lead to an increase in consumer mobile commerce activities, (e.g., using mobile phones to search the Internet for product reviews and comparing prices) and mobile banking. Use of mobile banking and related mobile financial services products builds trust and awareness, and contributes to the willingness of consumers to try emerging mobile payment offerings.[22]

Mobile payment services can also help unbanked and underbanked consumers who have access to mobile phones. Fifty-nine percent of individuals who are unbanked have access to mobile phones, and 50 percent of these phones are smartphones. Notably, 90 percent of the underbanked have mobile phones, 56 percent of which are smartphones. Both of these groups have a higher percentage of smartphone ownership than the general population.[23] For many of these users, their smartphones represent their primary connection to the Internet. They can use their smartphones to reload their mobile accounts, make purchases, deposit checks, and pay bills, alleviating expensive check cashing services and ATM fees.

The growing ubiquity of mobile commerce, coupled with the expanded functionality and greater convenience of smartphones, provide the framework for driving consumer mobile payment behavior. However, the primary barriers to adoption remain the limited availability of some technologies (e.g., NFC) and concerns with security and privacy. Substantial educational outreach and awareness by the industry is required because consumers will play a critical role in driving mass adoption of mobile payments and will likely dictate the sustainability of mobile solutions in the long-term.[24]

Regulators

Mobile payment instruments use the existing payments infrastructure in different ways. Some mobile payment solutions clearly fall under the scope of existing regulations, while other alternatives using new

---

[21] Pew Research reports that smartphone ownership in the United States is at approximately 46% and growing, while feature phone ownership is at about 41 percent.

[22] Javelin Strategy & Research (2012, September). *Battle for Control of Mobile Wallet* estimates that over 60% of consumers using mobile banking are likely to adopt a mobile wallet in the next 12 months. Forrester (2012). *State of Mobile Banking 2012*, forecasts that the number of mobile bankers in the U.S. is expected to double by 2017.

[23] Gross, M. B., Rock, A.M., and Schmeiser, M.D. (2013, March). *Consumers and Mobile Financial Services 2013*. Board of Governors of the Federal Reserve System. According to the FDIC's *2011 National Survey of Unbanked and Underbanked Households*, 8.2 percent (almost 10 million) of U.S. households are unbanked and 20.1 percent (24 million) are underbanked.

[24] For more information on consumer adoption of mobile payments, see Elisa Tavilla. (July 2012). *Opportunities and Challenges to Broad Acceptance of Mobile Payments in the United States*. Available at http://www.bostonfed.org/bankinfo/payment-strategies/publications/2012/opportunities-and-challanges-to-broad-acceptance-of-mobile-payments.htm.

technologies (e.g., NFC, QR code) may not have an obvious fit and require a better understanding before regulations might be prescribed. Mobile payment stakeholders perceive that regulators have not kept pace with mobile payment innovation and that the industry would benefit from more specific guidance and a legal framework for mobile payment providers. While industry participants acknowledge the applicability of current regulations and laws to underlying payment methods (credit, debit, prepaid, and ACH) that govern mobile payments today, they are concerned over the uncertainty related to coverage and liability responsibilities and a need for enhanced coordination among regulatory bodies. Financial institutions and related organizations also express concern for participation by nonbanks, including MNOs and alternative payment providers which may be less familiar with payment banking laws (e.g., BSA/AML, KYC, state money transmission licensing, risk compliance, and consumer protection).

The MPIW and representatives from several regulatory agencies[25] met in April 2012 to discuss issues, concerns, and potential gaps in regulatory coverage. The primary concerns they raised were focused on consumer protection, privacy, and data security; however, neither the regulatory agencies nor industry stakeholders concluded that there was an immediate need for additional regulation. Rather, they expressed support for clarification of existing regulations and their applicability to mobile payment service providers in order to increase understanding at the policy level, dispel misperceptions, and focus collective energies on potential risk vulnerabilities in the mobile channel. It was suggested that stakeholders focus on education and communication between the industry and the agencies, while regulators ensure that industry stakeholders are informed if and when the need for mobile regulation arises.

Given Congress's high level of interest in mobile payments and attention to the MPIW's initial white paper and ongoing work, several Federal Reserve, MPIW, and other mobile payment industry experts testified at House and Senate hearings in 2012. The House Financial Services Subcommittee on Consumer Credit examined the growing trend of mobile payments at a hearing held on March 22, 2012.[26] On March 29, 2012, the U.S. Senate Committee on Banking, Housing, and Urban Affairs held a hearing,

[25] Regulators included the Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC), Consumer Financial Protection Bureau (CFPB), National Credit Union Association (NCUA), Federal Reserve Board (FRB), Conference of State Bank Supervisors (CSBS), Washington State Department of Financial Institutions, Massachusetts Division of Banking, Federal Trade Commission (FTC) and Federal Communications Commission (FCC).

[26] Panelists included Rich Oliver, formerly Executive Vice President and director of the Retail Payments Risk Forum, Federal Reserve Bank of Atlanta, and representatives from PCI Data Security Standards Council, MasterCard, Smart Card Alliance and the Consumers Union. See http://www.c-span.org/Events/C-SPAN-Event/10737429273/.

"Developing the Framework for Safe and Efficient Mobile Payments,"[27] and held part two in July 2012.[28] Stephanie Martin, Associate General Counsel, Board of Governors of the Federal Reserve System, testified on regulation of mobile payments before the Subcommittee on Financial Institutions and Consumer Credit, House Committee on Financial Services on June 29, 2012. She commented that current payments laws "may not be well-tailored to address the full range of mobile payment services in the marketplace."[29]

Summary

Each primary stakeholder in the mobile payments ecosystem has an innovative approach to how mobile payment capabilities can be rapidly and reliably developed and implemented. While their efforts have provided consumers with multiple options, they have complicated the development of interoperable standards for mobile payments and the widespread adoption of any one mobile payment solution. Given the fragmented and dynamic market, it is important for the FRB to regularly convene the mobile stakeholders and other parties, including regulators, to discuss the mobile ecosystem, especially as the newer solutions evolve.

III. Progress towards Achieving Benefits

At the end of 2010, the MPIW identified a number of clear benefits of a future U.S. mobile payments infrastructure that was built on an NFC contactless technology platform. This section evaluates progress towards achieving benefits such as improved security and fraud reduction, merchant cost efficiency, competitive technologies, value-added services, revenue and monetization opportunities, and data privacy, in light of environmental developments in the ecosystem.

Improved Security and Fraud Reduction

The planned migration from today's mag-stripe environment to more advanced technology introduces the potential for a more secure payments environment. In the first Mobile Payments Landscape paper, the MPIW acknowledged the potential for NFC/secure element technology, along with the intelligence and data storage capabilities of the contactless chip embedded in the mobile phone, to improve authentication

---

[27] See http://banking.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=eab14748-aea3-48f1-a4f8-88f49613f0e1

[28] Witnesses included professors and industry experts from the University of California, Berkeley, University of Indiana, and University of California, Berkeley School of Law.

[29] Witnesses included Sandra F. Braunstein, Director, Division of Consumer and Community Affairs, Board of Governors of the Federal Reserve System and Kenneth C. Montgomery, First Vice President and Chief Operating Officer, Federal Reserve Bank of Boston. See http://www.federalreserve.gov/newsevents/testimony/martin20120628a.htm.

and reduce the risk of fraudulent transactions.[30] However, it is too soon to attribute any actual fraud reduction or enhanced security to NFC chip technology or the applications and tools built into the mobile phone hardware in light of the slow growth of POS mobile payments. To further complicate the measurement of mobile-based fraud reduction, alternative mobile technology solutions which are simpler and less costly for merchants and FIs to deploy have emerged. Examples include QR codes and cloud-based solutions that can store and manage payment credentials remotely, possibly addressing some of the complexities associated with managing data in the secure element embedded in the mobile device.

The implementation of EMV chip technology in other countries has resulted in decreased card fraud and is predicted to reduce mobile payments fraud in the future. Most developed countries have already converted to EMV industry specifications, while the U.S. migration is in the early stages. EMV is important to the security of NFC card-based mobile payments because NFC uses the underlying EMV technology infrastructure, and relies on the same dynamic data authentication (DDA)[31] for mobile payment security. Despite the leadership role of the credit card networks in driving U.S. migration to EMV card payments, they do not agree on the cardholder verification method, generating a debate about the level of risk of chip-and-PIN vs. chip-and-signature.[32]

While consumer behavior surveys report that privacy and security are consumers' most important concerns, in actuality they use their mobile phones to interact quickly with websites, businesses, and other people, valuing their ability to access social media. Problems stem from consumer failure to adopt available safeguards such as PINs, passwords, device lock features or anti-virus software. They also continue to engage in risky behaviors such as opening spam emails and jail-breaking phones, behaviors that will require change if a wallet containing payment credentials is added to the mobile phone.

Mobile applications downloaded to the handset can expose payment platforms and networks to fraud and other security risks. The vulnerability posed by mobile applications is largely attributable to a lack of industry standards. This situation is somewhat mitigated by moderating oversight from Apple and

[30] Despite anecdotes claiming that NFC data can be intercepted as the device communicates with a terminal, momentarily exposing data in transmission or by other sophisticated hacking schemes, the only reported breaches have occurred in lab settings, with none reported in the real world.

[31] DDA uses an encryption key to generate unique, dynamic data values to authenticate the transaction when it is authorized by the card network. These values are only valid for one authentication. If a thief tries to re-use the payment account data, it will be out of sync with the number stored by the card issuer and rejected, making it harder to skim usable data and clone for counterfeiting

[32] MasterCard supports Chip and PIN as the most secure payment technique to provide the greatest protection against fraud liability to retailers and acquirers. Visa supports a range of cardholder verification methods (CVMs) with EMV chip, including signature, online PIN and no-signature for low-value, low-risk transactions. American Express also supports a range of CVMs with EMV contact chip, including signature, online pin and no-signature for low-value, low-risk transactions.

Google of their app stores. However, many smaller app stores operate independently in the mobile ecosystem, with little to no oversight. The major operating systems approach security very differently, with Android and its open platform characterized as the "Wild West" and Apple as the "Frontier Fort."

As mobile payment transaction volume increases, the mobile payments channel is expected to become a more attractive target for criminals. Security providers need to anticipate risks and incorporate automated mitigation tools where feasible, such as preloading mobile antivirus software on phones, and leveraging the ability of mobile phones to share real-time data (e.g., location and customer-entered authentication). The mobile device has a number of security attributes that have the potential to make the mobile channel more secure than the online channel against fraud and to repel fraud attacks.[33]

Many parties are involved in supporting the multi-faceted mobile payments ecosystem. All share in the responsibility for mitigating mobile payment security and fraud problems. The industry must collaborate to identify potential threats and vulnerabilities in the mobile payments ecosystem, to share applicable data, to assess the security gaps in the mobile process, and to assign responsibility for remedying these gaps. They must also develop interoperable standards, guidelines and rules for newer technologies. The MPIW is vested in recognizing and/or developing industry-wide solutions to the security challenges presented by mobile commerce and can leverage its expertise to: (1) identify evolving threats and vulnerabilities that exist for mobile; (2) address the need for stronger authentication; and (3) advance security awareness among consumers and industry stakeholders in the mobile payments ecosystem. Mobile has the potential to provide a safer payments option if leveraged appropriately.

Merchant Cost Efficiency

While merchants would like to use mobile payments as an opportunity to achieve efficiencies, impediments exist. For example, the traditional card model treats mobile contactless payments as card-not-present, but a shift to treating such transactions as card-present instead would reduce merchant costs. Applying mobile wallet fees is another example that may inhibit innovation and add incremental costs. A number of large and small merchants are still participating in NFC-wallet pilots, but without a strong

[33] These attributes include context, tactile interface, sensors, cloud and social media. Geo-location can be used to enhance authentication and detect fraudulent charges. Technology is emerging that will leverage the sensory features of swiping or sliding across mobile device screens or to authenticate signatures via their touch screens. The tactile interface also opens up the possibility of fingerprint verification for financial transactions or account logins. Other features include the camera functionality which can authenticate users through facial recognition. All of these attributes can be layered to enhance security and authentication. Camhi, Jonathan (2012, October 26). Why mobile will be more secure than online banking. *Bank Systems & Technology*. Retrieved from http://www.banktech.com/channels/why-mobile-will-be-more-secure-than-onli/240009653?pgno=1.

business model, and ability to reduce the cost of deployment, merchants continue to investigate lower-cost alternatives that are not card-based and not supported by NFC.

Migration to EMV is also impacting merchant cost efficiencies because it requires investments to upgrade terminals. Merchants must weigh the investments against the risk of liability responsibility for counterfeit fraud associated with mag-stripe data breaches and the benefit of reduced fraud. The MCX model could help to reduce merchant deployment costs by clearing and settling over a lower cost network such as ACH, rather than over the more expensive card networks.

Cloud-based payment services may offer merchants cost-effective and rapidly deployable capabilities. Often cloud-based technology leverages barcode technology and card tokenization to further reduce the likelihood and costs of dealing with fraud. Tokenization is a technology that enables the payment service provider to exchange a one-time payment token at the merchant's e-commerce or POS system to redeem for payment. On the other hand, barcode technology is a more feasible solution to other mobile payment technologies from a customer integration perspective. Several mature and start-up companies offer cloud-based payment solutions – which initially serviced small merchants, but are expanding to larger retailers. Some of these companies are incenting mobile payments with lower fees and loyalty programs.

As merchants develop their strategies for mobile payments, they must consider multiple options related to hardware, software, choice of technology platform, and how they implement external factors (e.g., EMV). Some industry stakeholders hope that the inclusion of NFC capability in POS terminals upgraded for EMV may encourage merchants to adopt mobile contactless payments at the POS. However, merchants still incur incremental costs to enable NFC and view implementation of EMV and use of NFC for mobile payments as two distinct investment decisions. For EMV, merchants want assurances that their investments are in sync with issuers and mobile operators.[34] For mobile payments, merchants must do a cost-benefit analysis on whether to buy an NFC-enabled terminal, whether to enable NFC functionality, and what payment brands to accept.

Competitive Technologies

The current mobile payments ecosystem depicts a fragmented market, rather than a cohesive interoperable mobile payments approach. The various emerging technologies have the potential to benefit the payments systems by improving overall efficiency and security in the long-term, and the end result will

[34] Randy Vanderhoof, interview with Payments Source, September 2012. The *EMV Migration Forum* was created in September 2012, under the leadership of Randy Vanderhoof, president of the Smart Card Alliance. The primary role of the Forum is to prepare merchants, acquirers, issuers and processors for the pending conversion to EMV smart card technology in the U.S.

likely include several competing models that could be categorized broadly as cloud-based or NFC-like. These systems will eventually co-exist and may be selected for payments based on their venue and risk profile. For example, QR codes may work well for micropayments in a closed-loop proprietary payment system. NFC solutions may be best applied in cases that require enhanced security features such as transit, where speed and convenience of processing a high volume of transactions is necessary.

Value-Added Services

Retail: The mobile payment and commerce landscape is opening doors for innovative value-added services that enhance mobile payments. Such services can be provided before and after the actual payment transaction. These services are instrumental to offering relevant and timely information to customers, increasing the likelihood of generating additional sales, strengthening brand loyalty, and offering additional points of interaction with the customer. Both NFC mobile and cloud-based digital wallets can allow for the generation of customized coupons, timely discounts, and loyalty and reward program tracking and redemption directly from the mobile device. Value-added services are becoming more important than the actual payment transaction for driving mobile payment adoption. For sustainability, the value proposition of mobile commerce will need to include concrete value-added services beyond payments.

The ability to collect and analyze information on consumer preferences and buying habits tied to mobile payment transactions may enable customized promotions and rewards, but may also present risk to the customer's transaction information if not managed properly. A driving force behind collection of the data is the desire for enhanced data monetization by the data owners (e.g., FI, card network, merchant, MNO, payment service provider), who want to leverage their data to increase profit and efficiency, improve customer experience, and build customer loyalty. Competition over data ownership and its subsequent use exists, and stakeholders will need to agree on how to protect, share and present the data, subject to customer preferences.

The concept of a mobile or digital wallet can create a convenient and efficient tool for the consumer in the long-term. Initially consumers may be frustrated by limited payment choices included in the wallet, and by providers flooding the market with wallet offerings to attempt to gain market share. Research by TSYS and Mercator Advisory Group shows that consumers wish to consolidate their store loyalty and rewards cards in the mobile phone, and want to pay for purchases with their preferred payment method in a mobile wallet.[35]

[35] TSYS and Mercator (2012). *2012 Consumer Debit Payment Choice Research Study*.

Transit: The benefits of mobile contactless payments for mass transit are starting to emerge. Some U.S. transit systems are exploring opportunities to leverage open-loop card networks for transit payments. Contactless chip payments, particularly in the mobile channel, provide a use case for interoperability, lower operating costs through reduced transit fare card issuance expense, and increased acceptance to address the myriad of different payment acceptance systems for transit authorities across the U.S. Today, most of the largest U.S. transit systems are already invested in smart card systems for more flexible and efficient revenue collections. A transition from proprietary transit-only systems to open-loop NFC contactless payments represents an opportunity for even greater efficiency, reduced operational costs, and enhanced consumer convenience. The 2012 Isis mobile wallet launch in Salt Lake City with the Utah Transit Authority is an example of one of the first commercially available mobile payment transit programs in the U.S. In October 2011, Google Wallet conducted a NFC mobile payments trial with the New Jersey Transit Authority for NFC.

Revenue and Monetization Opportunities

New nonbank players and the conjoining of industries unaccustomed to partnership are disrupting payment models, as mobile emerges as a new payment vehicle. The new models are evolving without one standard approach dominating the playing field, making it difficult to achieve revenue goals. Mobile advertising with customized, promotions-based consumer shopping behaviors represents a new source of revenue. The Google Wallet business model is built primarily on gathering of user data and subsequent advertising, in contrast to the Isis wallet model, which provides a neutral, fee-based platform on which bank issuers load their credit, debit, and prepaid cards. Three of the top U.S. mobile carriers (AT&T, Verizon and T-Mobile) invested in the Isis joint venture receive a share of revenue from card issuers for wallet payment transactions, together with rent paid by the issuers to add their customers' cards to the secure element. The revenue potential and cost implications associated with the rent model are unforeseen, particularly given that participation in the Isis wallet is currently limited to three financial institutions (Barclaycard, Capital One, and Chase).

New solutions will be developed in response to the need for business models that meet the expectations of all stakeholders in the ecosystem. The variety of payment solutions may advance new schemes for revenue and cost-sharing that benefit customers and merchants.

Data Privacy

The MPIW focused considerable attention on the need for data privacy in the mobile channel, recognizing that the success of the mobile payment ecosystem hinges on trust and transparency. Similar to other channels, mobile can expose payments data to new parties and create the opportunity for data to be compromised. While the rewards resulting from data monetization may benefit the consumer, misuse of

the data may create serious privacy considerations if the consumer's payment or personally identifiable information (PII) is used without the consumer's explicit consent (e.g., opt-in) and lead to potential harm and unintended consequences.

Privacy risks are heightened with data monetization in the mobile payments space. The use of location-based services (LBS) by merchants and payment service providers to drive active and passive mobile marketing efforts has also heightened the concerns around privacy. While it is expected that consumers must register and/or opt-in to the application to allow it to use their location information, they may unknowingly allow companies to compile detailed profiles of their lives. Some popular LBS-enabled tools lack clear and concise disclosures about personal information collection, how that data is used, and the process for consumer consent.

In response to concerns over privacy risks in the mobile commerce environment, the FTC issued its Final Privacy Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*,[36] in March 2012, and the Obama Administration released its Consumer Privacy Bill of Rights.[37] While these reports are guidelines, any well-publicized incidents of privacy intrusions could result in legislative or regulatory action.

IV. Update of Original Strategic Principles

The purpose of the initial paper was to inform the FRB and other interested parties of the MPIW's assessment of the foundational principles intended to guide the development of an integrated end-to-end mobile payments process that could promote successful adoption. At the time, MPIW members supported rapid achievement of these principles to advance the realization of the benefits of mobile payments. However, the last two years have witnessed considerable change in the market and the business models, while NFC mobile payments have not evolved as quickly as originally predicted. Cloud-based and other innovative technologies, coupled with new market entrants and creative partnerships, have changed the dynamics of the mobile payments ecosystem, calling for a re-evaluation and modification of the MPIW's original strategic principles.[38]

---

[36] Available at http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

[37] In the report, the White House proposed legislation based on the privacy principles it contained and called on the U.S. Commerce Department's National Telecommunications and Information Administration (NTIA) to convene stakeholders to develop enforceable codes of conduct implementing these principles for specific industries. The NTIA has since held a series of multi-stakeholder workshops to develop voluntary codes of conduct to protect users' privacy in specific business contexts.

[38] The following commentary presents policy propositions for the FRB's consideration and does not seek to influence competing technological or commercial models currently being developed in the industry.

Open Wallet concept has evolved to include both mobile and digital wallets

The successful model for an open mobile wallet has not changed; however the initial concept of a mobile wallet has expanded into a digital wallet. Two years ago, the MPIW's definition of a mobile wallet was focused on NFC contactless technology which would store payment credentials, coupons, rewards, and other value-added features in the secure element in the physical mobile phone. In contrast, a digital wallet leverages cloud computing (i.e. remote servers) and wireless networks to enable proximity and remote mobile purchases and bill payments, without requiring secure financial data to be embedded in the mobile device. In a digital wallet, a payment may also be transacted without the physical presence of the mobile device by using a mobile phone number and a PIN/password at the POS. Although the NFC/secure element solution remains a viable option, cloud-based mobile services also provide secure storage and access to payment credentials, without the limitations inherent in a hardware model. The open wallet will likely evolve to include some components of NFC with the secure element and cloud, depending on consumer chosen functionality in terms of the type of payment and payment-related apps pre-loaded onto the mobile device, or via download through various app stores.

A true digital wallet is expected to be open and ubiquitous, accepted at most merchant locations, and across a multiplicity of different payment terminals. It should allow complete access by all consumers for various services, including transit, vending and ATMs. None of the current mobile or digital wallets truly meet this open standard, based on the original vision. Rather, current business models offered by major stakeholders are largely based on card platforms, with loyalty features. As long as wallet participation is bilateral, requiring exclusivity agreements that motivate other businesses to work independently to develop their own versions of the wallet, progress towards a true open wallet will remain slow.

Convergence of multiple technology platforms for mobile payments

Although NFC contactless mobile payments remain a key component of this principle, NFC is no longer viewed by industry stakeholders as the exclusive technology that will drive mobile payment adoption. It may gain ground when NFC-enabled phones and merchant terminals become widely available, but the slow pace and cost of NFC implementation has led to the pursuit of alternative solutions and technologies among industry stakeholders.

Currently, support for and opposition to NFC varies widely across stakeholders in the mobile payments ecosystem. Some stakeholders are hedging their bets by finding opportunities to implement complementary and/or competing mobile payment schemes where the alternative mobile payment method may be more cost-effective and more suitable to a certain venue or service, until consumer demand for NFC reaches critical mass. Other stakeholders remain unconvinced about the viability of NFC as a business or technical platform for payments and are actively pursuing non-NFC solutions. Despite

reservations by some stakeholders and other market participants, NFC offers benefits that other mobile technologies may not. Unlike cloud and QR code technologies, NFC is standards-based for chips and the secure element. NFC is well-suited as a cash replacement for small dollar purchases. It can enhance opportunities for loyalty programs with two-way communication. Coupled with the secure element in the mobile device, NFC can process prepaid debit, electronic benefits and transfer (EBT), and transit payments, enhancing efforts for financial inclusion of the underbanked.

Establish a ubiquitous platform for existing and new clearing and settlement rails[39]

Existing clearing and settlement rails provide a sound foundation for mobile payments platforms and for mass adoption and consumer choice, without precluding the opportunity for new rails to emerge. Current mobile/digital wallet solutions are either leveraging existing rails or developing innovative ways to use them (e.g., ACH). One exception to the use of traditional payments rails is direct carrier billing (DCB), which charges mobile payments directly to the customer's wireless phone bill. This service is only being used for very small value digital content in the U.S.

Dynamic data authentication provides long-term integrity and security for transactions across all channels

Dynamic data authentication (DDA) provides a secure method for protecting user data such as cardholder and other sensitive data for card-based mobile contactless payment transactions. From a security perspective, EMV is important because it uses DDA to secure Chip and PIN payments and can further secure mobile contactless payments. NFC is an extension of EMV chip technology that adds a radio interface. POS terminals that are upgraded to comply with EMV specifications are capable of supporting the payment card brands contactless (NFC) payment applications and processing both contact (smartcard) transactions and contactless (mobile NFC) transactions, should merchants decide to enable that capability. At a minimum, U.S. merchants must upgrade their POS terminals to support EMV in order to avoid the liability shift for fraudulent card transactions.

Given the credit card networks' directive for EMV in the U.S., this principle has been updated to include migration to the EMV specifications and encouragement by the card networks of early adoption of this payment scheme to assist in strengthening the security of card and mobile payments, and to ensure stronger security of the payment system and enhanced protection of the payment transaction data.

[39] Existing rails include: credit, debit, ACH, prepaid and mobile carrier billing.

Develop and adopt a global interoperable platform in the U.S. for mobile payment standards and certification of payment methods, leveraging existing standards where possible

To accelerate the adoption of mobile payments in the U.S., mobile devices must work safely and securely, and be capable of performing payment functions consistently, regardless of the technology platform, application, wallet, or underlying payment method. Standards should be applied across mobile payment solutions through a platform that can ensure domestic and global interoperability of technology, process and security.

Certain components in the current mobile payments ecosystem are already standards-based. The most developed are global technical standards for NFC-based mobile payments and the associated secure element. Any mobile contactless payment form factor used via NFC at the POS should follow established contactless standards endorsed by the International Standards Organization (ISO) and NFC industry groups, such as Smart Card Alliance, NFC Forum, GSMA, and Mobey Forum.[40] In the U.S., mobile contactless payments employing computer chip security and NFC technology must be based on ISO standard 14443.[41] Minimum compliance requirements for adoption of NFC contactless payments should include dynamic data authentication, digital/mobile wallet contactless functionality, and inclusion of the secure element in the mobile device. Furthermore, the industry would benefit from further analysis of ISO 18092[42] as a potential extension of contactless payments to enable peer-to-peer communication in addition to card emulation achieved with ISO 14443.

NFC mobile payments must also be capable of supporting all payment methods and networks, comply with business rules and standards, and reside in a secure container in the mobile device to interface with mobile payment applications. Mobile stakeholders are working with solution providers to build NFC mobile payment platforms based on all three secure element options: SIM card, embedded NFC chip, and micro SD chip. While no one secure element option is dominant in the U.S. marketplace, the SIM card approach is more prominent in the global market.

---

[40] The NFC Forum develops NFC specifications for device architecture and protocols to ensure interoperability between conforming devices, while GlobalPlatform handles secure element specifications to support the development of internationally interoperable, multi-application NFC solutions. The GlobalPlatform scope includes setting specifications for securely loading confidential content (e.g. customer data) onto the card by external entities such as the Trusted Service Manager (TSM).

[41] ISO 14443 is an international standard that defines proximity cards used for identification, and the transmission protocols for communicating with it.

[42] ISO 18092 defines communication modes for Near Field Communication Interface and Protocol (NFCIP-1) using inductive coupled devices operating at the center frequency of 13,56 MHz for interconnection of computer peripherals. It also defines both the Active and the Passive communication modes of NFCIP-1 to realize a communication network using NFC devices for networked products and also for consumer equipment.

For other components in the mobile payments ecosystem, standards do not exist. Mobile payments that leverage the cloud and QR codes do not have a standards framework. There are no defined end-to-end standards to support the efficient use and security of the mobile device, the actual mobile payment during the transaction process, and the provisioning of the mobile/digital wallet. Privacy and security standards related to downloadable mobile apps are needed. While control of the application marketplace by the operating system providers has been helpful, there is room for improvement in the development of consistent rules and security measures. With the exception of PCI, no consistent standards exist to guide the use of encryption and tokenization as tools to enhance mobile payment security.

Whether implementing NFC/hardware-based or cloud/software solutions, all U.S. mobile payments stakeholders support the principle of a safe and secure mobile payment transaction. While it may be premature to establish cohesive standards for mobile payments, it may be appropriate for a broad, organized effort in the U.S., led by the appropriate organizations and/or regulatory bodies, to engage mobile payment stakeholders in beginning to develop a high level set of principles and a common roadmap or taxonomy to sort out the different components for mobile payments. These principles should include an agreed upon set of interoperable standards that encompass mobile devices (smartphones), NFC chips, secure elements, cloud, QR codes and mobile applications. The standards (accredited or otherwise) must also support the provisioning and maintenance of credentialing, open interoperability, and related security and privacy concerns. The process should leverage the best of existing standards and rules, without diminishing future innovation for the benefit of consumers. The MPIW may be well-positioned to leverage collective industry expertise to identify the potential gaps in the current standards framework that could be addressed by best practices, guidelines and principles.

Neutral Trusted Service Managers (TSMs) should oversee the provision of shared security elements used in the mobile phone for an NFC solution

This principle was written to be deliberately broad, leaving the individual mobile payment providers to determine what TSM(s) to choose and how to utilize the TSMs to manage functions. For example, Google's TSM handles all the related services, while two TSMs (managed by the same company) support Isis, one for FIs and one for MNOs.

A TSM typically coordinates the technical and business relationships between multiple stakeholders, including MNOs and service providers such as banks, ticketing agencies and other public and private sector issuing authorities, to deliver and maintain end-user services on mobile devices. These functions include: providing end-to-end application security by authorizing access to the secure element as required by each of the stakeholders; and application lifecycle management, including over-the-air provisioning, personalization, activation, and deactivation of services and privileges.

Going forward, the MPIW may want to consider how interoperability, standards, and management of the digital wallet could be factored into the role of TSMs. The group should also discuss whether the time is right to broaden the TSM role for wallets in the U.S. to include other responsibilities such as customer service, certification of mobile payment applications and vendors, and how the TSM fits into the larger structure of the trusted intermediary.

Regulatory Clarity

Regulatory clarity continues to be a critical core principle. Some progress has been made towards industry understanding of the regulatory responsibilities and concerns related to mobile payments. The MPIW has primarily focused on enhancing communication between regulators and industry stakeholders and on monitoring current developments and education through conferences and other media. The MPIW and Federal Reserve will continue dialogue with regulators to clarify oversight responsibilities, help create regulatory guidelines for security and privacy, and develop business standards and best practices.

Understanding the Role of Nonbanks in the Mobile Payments Ecosystem

One of the unique qualities of the mobile payments ecosystem is the expanse and diversity of industry stakeholders. The mobile environment has created opportunities for many nonbanks to introduce innovation and creative partnerships to the evolution of the mobile payments ecosystem, contributing to the success of mobile payments adoption. Start-ups and mature nonbank businesses are developing apps and providing lower cost solutions (compared to traditional card rails) for making and accepting mobile payments, and for clearing and settling payments that leverage existing payment rails. Merchants and alternative service providers are also demonstrating increased interest and influence over the direction of the mobile payments ecosystem.

Participation by mobile app developers illustrates a potential risk/benefit paradigm that is introduced to the payments environment. Many mobile app developers are small and independent, and not as familiar with the regulations and risk management practices that characterize the financial services industry. Without some guidance and direction, mobile payment app developers could potentially create serious consumer payment vulnerabilities. Partnering with industry incumbents could help to educate them and mitigate risks.

While innovation is encouraged in the mobile payments marketplace, participation by new entrants, large and small, generates new risk to the ecosystem, along with new opportunities. It also raises questions about the need for third-party (nonbank) enhanced risk management considerations. Therefore, the need

to keep abreast of and understand nonbank activity in the payment space has been added to the MPIW strategic principles.

Summary of Principles

Overall, the original principles established by the MPIW hold true, albeit with some modifications, particularly the shift to an expanded mobile technology platform that includes both NFC and cloud-based mobile and digital wallets. Some change is not surprising with almost two years of experience testing different mobile models: the introduction of new participants, technologies, and services; learning what works and what does not; the influence of merchants on the cost structure of mobile payments; and all stakeholders gaining a better understanding of the consumer demands and security requirements. As the MPIW has grown in size and diversity of representation, it has broadened its perspective on the evolution of mobile payments in the United States.

This broader perspective lends itself to an expansion of the original strategic principles to emphasize two additional points: (1) understanding risks associated with nonbanks; and (2) recognizing that incorporating transparent value-added services –such as incentives and offers into mobile payment platforms –have the potential to motivate consumers to adopt mobile payments.

V. Long-term Vision

The MPIW's support for a secure and open mobile payments system remains unchanged. Despite the variety of technology platforms, the ultimate solution must be safe, open, interoperable, and available ubiquitously on any mobile device, with any bank or merchant, and ideally over any network. Security in mobile payments will continue to be top of mind for all stakeholders, particularly consumers and merchants, who must have confidence in the safety and reliability of the mobile payments system for it to succeed. Ongoing technology advancements and disruption will continue to alter the landscape; mobile and digital wallets will co-exist; technology platform and channel convergence will increase; and big data monetization will need to be included in the risk management process.

Ongoing Technology Advancements will Alter the Mobile Payments Landscape

The MPIW's ultimate long-term vision is for a safe, secure, and technically interoperable mobile ecosystem built on multiple technology platforms. However, in the absence of any limits or standards restricting entry, the mobile payments landscape will continue to introduce more alternative payment solutions in the near term.

Mobile and Digital Wallets will Co-Exist

Future wallet business models may leverage emerging standards such as the FIDO[43] Alliance that combine the strong device-level security (a characteristic of NFC) with cloud-based technologies, driving improved efficiencies and innovation for user experiences, while standardizing the back-end protocols for interoperability, ubiquity, and optimum security.

Increasing Channel Convergence using Existing Rails

The increasing ubiquity of mobile phone usage globally is driving commerce to the Internet and mobile channels. Subsequently, payment service providers are introducing solutions that leverage both channels, blurring the lines of demarcation among payment delivery methods.

Interestingly, there is little evidence of industry support for the creation of new clearing and settlement rails, suggesting that new payment systems will continue to build on existing infrastructure or create new models using components of the existing rails. It is very costly and complicated to build brand new payment rails and achieve scale, particularly in the United States where the existing payment rails are mature, trusted, secure and regulated.

Big Data Monetization with Risk Management Oversight

The MPIW initially predicted that customer data analytics and marketing efforts might need a combination of private and public oversight to avoid privacy violations. As a result, mobile industry participants will need to find ways to share customer information to establish sufficient audit trails to manage payments fraud. New mobile business models will need to strike a reasonable balance for information sharing between who needs to know and what information should be shared.

While alternative payment providers have demonstrated sufficient self-governance with respect to mobile marketing, future growth and competition in the mobile landscape may potentially compromise consumer privacy, creating opportunities for data mismanagement. This could be particularly true with nonbank technology start-ups that are unfamiliar with regulatory schemes and consumer protection laws associated with traditional financial services. Data owners may jeopardize consumer protections by leveraging data to maximize revenue. Increasing use of LBS to track consumers and offer real-time, customized promotions may also raise questions about access to customer data for marketing purposes. The CFPB will monitor consumer protections, including disclosures governing privacy. The FTC is also increasingly focused on developments in the mobile channel with respect to consumer protections and privacy, which may serve to strengthen industry self-governance.

[43] Fast Identity Online (FIDO) is an organization formed to enable interoperable strong authentication and authorization between mobile phones and cloud services. The FIDO Alliance was co-founded by Validity, PayPal, Infineon, Lenovo, and NokNok Labs and launched in February 2013.

VI. Conclusion

Much has happened in the two-plus years since the first MPIW report on the U.S. mobile payments landscape was published, and not entirely in the direction many industry stakeholders had anticipated. There have been some unexpected obstacles to mobile payment adoption, some surprises in the mix of players in the market, and some new solutions developed to compete with NFC. As a result, the U.S. mobile payments market and consumer adoption did not grow as quickly as expected. It is clear that mobile payments will continue to expand and become a permanent fixture in the payments system. However, without continued collaboration and movement toward open access, the likelihood of achieving mass adoption and the associated benefits to stakeholders, consumers, and the payment system is uncertain.

Next Steps for the MPIW

The MPIW will continue to convene and work collaboratively to inform the FRB, regulators, policymakers, and Congress on developments in the mobile payments industry and the adoption of open and interoperable mobile payment solutions, both for the retail POS as well as other venues. Much work remains to be done to achieve a viable mobile payment system, including development of a risk management program, implementation of necessary technology standards, identifying and closing regulatory gaps, strengthening stakeholder business cases, and achieving broad consumer adoption.

Gaining a better understanding of the risks and security requirements for mobile payments will be a top priority. This is a broad topic because of the many components and parties involved in provisioning and processing a mobile payment across different platforms. As such, the MPIW will first need to define the scope of the effort.

The MPIW will also provide input and recommendations for mobile and digital wallet standards and best practices in order to address compatibility, interoperability, privacy, and security (including accommodating multiple payment options and applications securely, accessing multiple payments networks).

Finally, the group will continue to educate members and engage outside groups in discussions on the long-term benefits of mobile payments in the retail space, and keep abreast of regulatory developments, particularly related to consumer protection and data privacy, and how the U.S. migration to EMV may impact the progress of mobile payments.

Appendix: MPIW Activity 2011-2012

January 2011	• Met to discuss current mobile activity and review draft of white paper
March 2011	• Published first white paper, *Mobile Payments in the United States: Mapping Out the Road Ahead*
July 2011	• Met to discuss mobile wallet, merchant business case, and security of NFC mobile payments • First meeting to feature inclusion of several merchants (previously represented by MAG) • Merchants expressed concerns related to business case for mobile payments, future role of NFC, processing costs, investment in terminal upgrades, and cost of PCI compliance • Attendees expressed need for broad education to allay consumer security and privacy concerns for mobile payments, and supported a roadmap that would allow for industry self-regulation
December 2011	• Met to discuss current trends related to mobile wallet initiatives (e.g., Google Wallet, Isis, Visa, PayPal), security requirements and end-to-end risk management, TSM roles and responsibilities, and interoperability and management of secure elements and multiple wallets • Prior to meeting, several MPIW members participated in series of calls to examine different NFC secure element approaches – embedded, SIM, microSD, and mobile payments in the cloud
April 2012	• Met with representatives from Federal and State banking agencies, FTC and FCC to discuss issues, concerns, and potential gaps in regulatory coverage of mobile payments in the United States
July 2012	• Published white paper, *The U.S. Regulatory Landscape for Mobile Payments*, summarizing the April 2012 meeting
September 2012	• Met with retailers and start-ups to understand their perspective on mobile payment opportunities and challenges
November 2012	Findings from security information presented at December 2011 meeting included in Federal Reserve Bank of Boston's white paper, *Mobile Phone Technology: Smarter than We Thought*.[44]
January 2013	• Met with mobile security experts to learn their perspectives on key mobile payment risks • Mobile payment security identified as an issue where collaboration is necessary • Formed security sub-group to analyze mobile payment vulnerabilities and authentication requirements
May 2013	• Published new white paper, *U.S. Mobile Payments Landscape – Two Years Later*

[44] http://www.bostonfed.org/bankinfo/payment-strategies/publications/2012/mobile-phone-technology.pdf, November 2012.