Mobile Payments in the United States

Mapping Out the Road Ahead

Darin Contini and Marianne Crowe, Federal Reserve Bank of Boston,
Cynthia Merritt and Richard Oliver, Federal Reserve Bank of Atlanta,
and Steve Mott, BetterBuyDesign

March 25, 2011

==========

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 or the Federal Reserve System.

I. Executive Summary

In January 2010, the Federal Reserve Banks of Atlanta and Boston, through their Retail Payments Risk Forum and Payments Research groups, convened a selected set of key players in this country's emerging mobile payments ecosystem. The goal of the meeting was to facilitate a discussion among all involved parties as to how a successful mobile payments (as opposed to mobile banking) regimen could evolve in the U.S.

Over the past 15 months, the self-named Mobile Payments Industry Workgroup (MPIW)[1] met five times to share information and ideas, discuss the barriers and opportunities resident in mobile payments, and ultimately, to suggest a vision for the building blocks of an efficient and ubiquitous mobile payments environment. Ultimately, the discussions of this group, along with additional industry dialogue and literature research, constituted a body of input to the development of a research paper regarding the future for point-of-sale (POS) mobile payments in the United States.

This paper, drafted by the Boston and Atlanta Reserve Bank payments research teams, does not necessarily reflect the opinions of the Federal Reserve Banks, the opinion of the Federal Reserve Board of Governors, or the opinion of any individual member of the workgroup. Rather, the paper represents the collective views of the authors based on the inputs noted above. The paper depicts the current mobile payments ecosystem in the U.S.; discusses barriers, gaps, and opportunities; and sets forth a set of foundational elements that workgroup participants believe are fundamental to the development of a robust mobile payments environment. This "vision" for the future is built upon the recognition that the current environment faces many challenges and that success will require extensive collaboration between participants to ensure that consumers see a homogenous solution as they do today in other payment channels such as checks, ACH, and cards. Moreover, it must be a solution based on agreed upon standards, rules, and practices that ensure seamless interoperability regardless of the handset, mobile carrier, financial institution, payment network, or merchant location involved in any individual's desired transaction.

The foundational components of success suggested by the work group include:

1. The proposed environment is best defined by the concept of an "open mobile wallet."

2. The mobile infrastructure would likely be based on Near Field Communications (NFC) contactless technology resident in a smart phone and merchant terminals.

[1] Use of the MPIW in this paper represents the existing workgroup or a modified version of the group in the future.

3. Ubiquitous platforms for mobile should leverage existing rails, including the ACH network for non-card payments, and support new payment types that meet emerging needs.
4. Some form of dynamic data authentication would be at the heart of a layered mobile payments security and fraud mitigation program.
5. Standards would be designed, adopted, and complied with through an industry certification program to ensure both domestic and global interoperability, including a standard to ensure that devices used to facilitate mobile payments do not create any electronic interference problems.
6. A better understanding of a regulatory oversight model should be developed in concert with bank and non-bank regulators early in the effort to clarify compliance responsibilities.
7. Trusted Service Managers should oversee the provision of interoperable and shared security elements used in the mobile phone.

During their discussions, the MPIW debated the need for a new entity in the ecosystem directed at assisting the various parties to resolve issues of mutual concern and codify solutions in such a way as to facilitate interoperability and ubiquity. While many members felt that such an entity may be useful in the future, the general sense was that it was too early in the evolution to fully understand how such an entity might be constituted and what its role might be. In the meantime, the MPIW indicated a desire to meet again, perhaps with some additional attendees, to continue to discuss issues resident in the foundational components discussed above.

Additionally, the group discussed the need for an industry "roadmap" that could focus short term investment and accelerate progress. Once again, the general sense was that the complexity of the environment and diversity of participants would make this a daunting task. Efforts to specifically prescribe such a roadmap could create results that are inconsistent with the outcome eventually produced from natural market forces. Therefore, the group decided that defining such a roadmap this early in evolution of mobile payments in the U.S. might stifle innovation.

The benefits of this document and the underlying participative work effort will be revealed by what happens next. This paper is intended to be a vehicle for socializing a concept or model for an efficient, secure, ubiquitous, and convenient mobile payments evolution in this country to a much broader group of industry players. They, in turn, must ultimately agree to support or modify the ideas contained herein as a means of moving forward, recognizing that the opportunity to achieve maximum benefits may be best realized by acting sooner, rather than later.

The ability of the two convening Reserve Banks to organize and facilitate the discussions that led to the publication of this document, in addition to the ongoing and highly engaged participation of a diverse group of mobile ecosystem players, speaks to the potential success of idea-sharing and demonstrates that

collaborative efforts could work. The authors would like to thank all the participants for their engagement and contributions to this work. A note of special thanks goes to Steve Mott of BetterBuyDesign, who contributed heavily to this effort.

II. Introduction

Almost daily a new mobile payments venture is announced that makes it possible for a consumer or business to use mobile phone technology to enable or enhance the payment process. Initially, the focus has been on enabling a mobile device to be used as a browser, accessing existing internet-based banking and retail systems. More recently, attention has turned to the use of an application-enabled mobile phone as a payment form factor, substituting for a check, cash or a card to eventually create a mobile virtual wallet. Financial institutions are testing these capabilities, as are numerous non-banks, including some who operate in the internet space.[2] In some cases, the phone is simply used to initiate a card payment, but in other cases it is used to create a direct transfer to another individual or business using an existing bank-centric clearing and settlement capability (e.g. ACH), or an online payment service provider. Another variation embraces the concept of sending SMS (text) messages via mobile phone carriers, who perform the clearing and settlement function, as experienced in the successful program to funnel aid to Haiti in the wake of its earthquake disaster.

The concept of mobile banking and payments has resonated in many developing countries where lack of a physical banking or payments infrastructure exists.[3] Mobile payments have enabled financial inclusion for individuals and small businesses that are more remote from banks to overcome the limitations of physical transportation and utility systems. Mobile payments have even created a new currency in the form of airtime minutes. The evolution of mobile payments in the U.S. has followed a different path because of the well-defined banking and payments infrastructure already in place in the U.S. As a result, U.S. mobile payments have advanced more slowly; and many pilots, while conceptually interesting and educational, have failed to produce evidence of a currently sustainable business case. U.S. consumers are fortunate to have many different payment methods available to them, so the need for a fully deployed mobile payments alternative is not as obvious. Additionally, the cost of deploying the physical software and hardware elements of a ubiquitous mobile infrastructure is significant and must be justified in the face of uncertain consumer demand.

Nevertheless, there is growing evidence that mobile payments will become a significant element in the U.S. payments landscape in the future. A recent government report estimated that 18 percent of U. S.

[2] For example, Google, Amazon and PayPal, all who accept payments for internet purchases, are involved in mobile payments.
[3] Merritt, Cindy. 2010. "Mobile Money Transfer," Retail Payments Risk Forum, Federal Reserve Bank of Atlanta, September.

households do not have a bank account[4], a key variable in the attractiveness of mobile payments in countries where the majority of the population is unbanked. However, in the U.S. it is not anticipated that the unbanked will be the take-off point for mobile payments. It is likely to be the smart phone user. About 34 percent of U.S. consumers now own a smart phone and that number is growing at a compound annual growth rate of 17 percent[5]. Most large U.S banks offer customized banking applications for smart phones. Contactless mobile[6] technology provides additional capabilities resident in chips that can reduce payments fraud and potentially the cost that merchants bear to ensure their card brands are PCI compliant. Finally, the U.S. continues to become a more mobile society where consumers are motivated to use their time wisely. All of these factors point to the potential success of mobile-based payments and related activities in the future.

Most firms that would benefit from the long term deployment of mobile payments are eager to understand the details associated with successfully deploying a mobile payments infrastructure and accelerating progress wherever possible. Consequently, the Retail Payments Risk Forum at the Federal Reserve Bank of Atlanta[7] and the Payments Research Group at the Federal Reserve Bank of Boston[8] have collaborated to provide a setting for mobile industry participants to meet and discuss ways to move forward. This Mobile Payments Industry Workgroup (MPIW) is comprised of organizations representing the end-to-end mobile value chain. Since early 2010 they have met quarterly to discuss the reality of mobile payments and discern the way forward. Many of the discussions were first time events involving participants who had not previously engaged in face-to-face conversations, yet through this process some agreement has been reached on a number of key variables applicable to a perceived formula for mobile payments success in the U.S.

Present at the meetings were mobile carriers, issuing and acquiring banks, card brands, payments processors, credential manufacturers, trade associations (including merchants), mobile software solution vendors, handset makers, and large online payment service providers. To focus the discussion of "what is possible," the participants learned more about each other's business propositions, engaged in group activities aimed at understanding what cost and revenue factors were present, discussed various barriers to success, and contributed input to a basic set of characteristics that would be common to a successful mobile payments architecture.

[4] FDIC. 2009. "National Survey of Unbanked and Underbanked Households," December.
[5] Javelin Strategy & Research. 2011. "Mobile Wallets: With the New Mobile Network Operator Joint Venture Isis, Are Cards and Cash Ready to go Mobile in 2011?" January.
[6] Contactless mobile and mobile NFC will be used interchangeably throughout this paper.
[7] Hhttp://www.frbatlanta.org/rprf/
[8] Hhttp://www.bostonfed.org/economic/cprc/index.htm

These discussions occurred in a very dynamic U.S. payments environment. Even as the MPIW was meeting, new mobile pilot programs were announced (some involving workgroup participants), the Durbin Amendment to the Financial Reform Act was adopted, other new mobile technologies were launched, and an initial interchange price regimen was proposed by the Federal Reserve Board of Governors. Nevertheless, the focus of the group has been on long run success in the creation of a profitable and ubiquitous mobile payments infrastructure. The chicken and egg challenges of merchant deployment and consumer usage were debated, the roles of banks and telecoms clarified, and different infrastructure models were discussed. Ultimately, it became clear that significant success was likely to come as a result of collaboration directed at identifying necessary standards and encouraging efficient implementations, rather than independent action.

In essence, this paper is intended to be a framework for more widespread industry discussion and debate that could lead to more sustainable progress in improving overall U.S. payments system efficiency and integrity than might occur otherwise. In the sections that follow, we define the composition of the mobile ecosystem, describe a vision for a successful implementation, address the potential benefits and drawbacks of mobile deployment, outline the obstacles and barriers to be addressed, identify the components of an industry business case, set forth key standards issues for discussion, explore various use case scenarios, and propose possible directions moving forward.

Ultimately, the value of this work lies in its overall acceptance and use, recognizing that the payments system environment today, while stable and secure, may be affected by any number of factors, including the broad spate of legal/regulatory activity emanating from Congress, therefore making it difficult to move to a single agenda.

The MPIW realized that there are various terms used in the mobile ecosystem that need to be explained or clarified. Consequently, we have included a glossary of key terms in Appendix I.

III. U.S. Mobile Payments Infrastructure Today

While mobile payments, as opposed to mobile banking, applications have gained notable recent success in other parts of the world, they are just beginning to emerge in the U.S. Mobile payments for physical goods and services (e.g. POS and transit) imply the use of near field communications (NFC) contactless technologies that are not yet prevalent in the U.S., even in the card world. While NFC-like contactless technologies (e.g. barcodes, stickers, micro SD chips) have been appearing in the market recently, the emerging common standard for POS mobile transactions is near field communication (NFC). NFC enables a transmission using a very short-range wireless connectivity technology with the capacity to execute payment transactions, and a secure element that securely stores information such as identity

credentials and financial value. The appeal of NFC is that it is compatible and interoperable with other current systems, e.g. transit and security. In essence, it is not a new technology and works with existing hardware, secure elements and communication protocols.[9] NFC-enabled mobile payments have the potential to be the universal contactless payment technology if necessary stakeholders have the economic incentives to adopt it.

The slow evolution of contactless mobile payments in the U.S. is also indicative of a number of barriers that exist, as discussed in more detail later. As examples, the card networks, issuers, and acquirers have developed robust fraud analytics around mag-stripe technology and NACHA has developed monitoring processes which have mitigated ACH risk to a certain degree. Stakeholders are reluctant to invest in terminals and handsets in the absence of more certainty around changes to the infrastructure and the risk of making the wrong business decisions. The cost for merchants and issuers to invest in new device readers at the POS and for contactless chip-enabled payment devices, including cards, phones, and possibly other form factors, is significant.

Essentially, as discussed below, each primary stakeholder in the mobile payments ecosystem has its own ideas about how mobile payments should be developed and implemented, creating potential conflicts and barriers to development of a ubiquitous, interoperable solution for mobile payments. The market is moving quickly and there are still issues not fully resolved. So, there is benefit to convening the mobile stakeholders regularly to discuss the rules and framework of the mobile ecosystem as it evolves.

Mobile network operators (MNOs) own customer billing infrastructures that they can leverage to add value to existing voice and data services. While financial services such as mobile payments may represent an extension to existing customer relationships, the MNOs are new to financial services and have expressed concern about assuming material credit risk, based on their limited experience in providing consumer protections for financial services. However, the MNOs are experienced in providing subscriber acquisition and authentication, device provisioning, customer support and value added services, all necessary for increasing mobile payments. Additionally, they are a vital enabling technology channel for mobile payments**.**

U.S. financial institutions have not offered mobile financial payments because of a perceived lack of a good business case, although the growth in mobile banking implementations and recent mobile payment trials signal this may be changing. Financial institutions have the opportunity to add value to customer depository services with the addition of mobile technology and realize customer retention benefits as a result. With their long time experience handling payments, addressing customer authentication and authorization requirements, and enforcing Know Your Customer (KYC) rules,

[9] While there are other security options in addition to the secure element, e.g. cloud-based systems, this paper focuses on a secure element embedded in the phone.

financial institutions are well postured to settle payments to a consumer's account and to employ risk management programs that ensure regulatory compliance for money laundering, consumer protection, and other risks. Basically, financial institutions want to remain at the center of a customer's account relationship by issuing payment credentials and applications on the mobile device as they do in the physical payments world today.

Handset manufacturers must produce smart phones capable of including NFC technology and related security software and then pair with the MNOs to provide utility to the consumer. How to handle functionality around locked vs. unlocked phones, authentication, and the ability to use the mobile phone for NFC payments without the network all need to be addressed. Furthermore, technology needed on the handset to accommodate mobile payments is changing rapidly (e.g. SIM, micro SD, NFC sleeves) in order to address security challenges and compliance with MNO and payments certification. Yet, handset manufacturers around the world are beginning to issue standard handsets in volume that will embrace such technology in the next year or two.

Trusted Service Managers (TSMs), building on their role in the card world, have emerged as the entity responsible for provisioning credentials to secure elements in mobile phones as a necessary tool to provide the type of transaction security users will accept. Depending on the size and scope of a TSM, other functions may include provisioning/account set-up; ensuring compliance with security requirements for software, hardware, handsets, chips and applications; fraud and risk management; and customer service and support. Customer support might include handling device/service questions and resolution relating to secure element use; developing and maintaining user documentation for best practices; support and assistance for operating system and mobile application software upgrades and mobile vendor certification; lost/stolen/upgraded phone notification to customers; handling billing questions; and reporting fraudulent transactions.

Merchants are critical stakeholders in the chicken and egg equation of mobile payments adoption. Merchants are interested in secure payments at the point of sale, timely settlement, manageable investment in infrastructure, relief from costly data protection inspection obligations, and reasonable interchange for transactions. Without widespread merchant acceptance, it will be difficult for NFC mobile payments at POS to achieve mass adoption.[10] [11] Merchants must plan for and adopt the POS terminal technology necessary to work with wireless devices developed and deployed by the MNOs and handset makers. Depending on the application the merchant may need to interact with a particular bank. When the payments application used in a mobile transaction is a card application, the merchant must

[10] National Retail Federation. 2010. "Mobile Retailing Blueprint: A Comprehensive Guide for Navigating the Mobile Landscape," version 1.0.0. White paper, May.

[11] Merchant Advisory Group. 2010. "Open the Curtains in the Payment System - Merchant Advisory Group Recommendations on the Mobile Transformation Opportunity."

work with an acquiring bank to begin the clearing and settlement process. For ACH at the point-of-sale, the merchant must integrate with an originating FI.

Intermediaries/third party processors and online payment service providers have emerged to provide the enabling technology for mobile financial services or to serve as intermediaries in the payments supply chain. These processors and online payment service providers, mobile software solution vendors, and application and hardware developers are partnering with financial institutions or MNOs for the provision of mobile proximity payments. The third party non-banks see mobile as a new market opportunity and must be included in any infrastructure plans for mobile payments. They may also consider the existing environment too constrained by regulation and entrenched providers and seek to disrupt the payments ecosystem with a new offering.

Consumer demand for mobile technology is very high, but their interest in mobile payments is uncertain due to their lack of experience using mobile devices for that purpose. Consumers have many safe and efficient payment choices in the U.S. so the case for shifting to mobile payments must include new features and value. The rapid advance of electronic payments in the United States is a testament to the fact that ultimately, consumers want payments that are convenient, inexpensive, and secure.

Payment Card and ACH Networks all play a key role in the mobile payments ecosystem, although at this stage of the evolution, each network has chosen a different path to implementation. Some are partnering with mobile carriers to develop new ventures, while others are working with banks and transit authorities to test different or new forms of mobile wallets. NACHA is analyzing its rules to properly route new mobile payment transactions. Regardless of the interim actions, credit and debit card accounts will be critical to the long term success of ubiquitous mobile payments, given their dominant base of customers.

Regulators must participate in the evolution of mobile as the regulatory framework for mobile payments is fragmented with respect to MNO and other third party participation in the provision of payment services. In business model examples where payment flows leverage existing value chains of networks and payment clearing and settlement systems such as the card brands and the ACH, existing regulatory oversight and consumer protections are expected to prevail. However, questions are arising about the legal liabilities and responsibilities of new parties to the payments transaction, which may be governed by agreements between the stakeholders in the value chain. Participants desire clarity of the new regulatory structure and want to know how to be proactive in addressing consumer protection issues such as identity management, cyber-security and prepaid mobile accounts. Dialogue between FI regulators, the Federal Communications Commission (FCC), the Federal Trade Commission (FTC) and the Department of Commerce, *and* with mobile industry stakeholders is necessary to ensure that emerging

mobile payments services are conducted in a way that enhances safety and integrity in U.S. payment systems.

IV. Long-Term Vision For the Future Environment

As the MPIW discussed the future over a series of five meetings, a vision for the long-term mobile ecosystem emerged, in terms of successful business models and the important components of a mobile payments operating framework, such as standards and guidelines. While not all parties agreed in full, a decision was made to intentionally limit the scope of the effort to mobile payments at the point-of-sale. The group acknowledged that the mobile framework is not tied just to payments and that there is a need to look at opportunities to drive m-commerce, including value-added features such as coupons, rewards, clinical services, etc. The group further recognized that mobile has the potential to be a key component in making and/or securing remote payments and authenticating payments made via internet or card (i.e. card-not-present transactions). However, that possibility was viewed as something the group could discuss going forward.

The group opined that the potential societal benefits created by mobile-enabled payments technology, including the potential to reduce payments fraud and expand financial inclusion, portend a future where the mobile phone becomes the consumer's wallet and provides a seamless customer experience. This new mobile wallet will be enabled by NFC contactless technology embedded in the mobile handset so that it can store secure payment and identity information, as well as provide a secure access channel to payment services.

Ultimately, the successful mobile-enabled payments network will leverage a set of common standards and open platforms to ensure global interoperability. In a perfect world, mobile-enabled payments will be as interoperable as card payments are today, where consumers can use cards for payments anywhere in the world. Ubiquity will be achieved by creating a set of standards for payment applications that co-exist in a mobile wallet open to all card (credit, debit and prepaid) networks as well as ACH, that work across all carriers, and are accepted by all merchant POS terminals across all borders.

It is therefore critical for all participants in the future mobile payments environment to work together to design a model for interoperability that has the advantages of the card model and includes global industry standards. While the emergence of competing proprietary offerings encourages innovation, it also bears the risk of creating silos that may impede the development of critical mass needed to ensure a successful payments network. While workgroup participants were not in a position to establish consensus with respect to specific standards, all agree that the long-term vision of a successful mobile payments system in the United States will occur through the creation of mutually agreeable

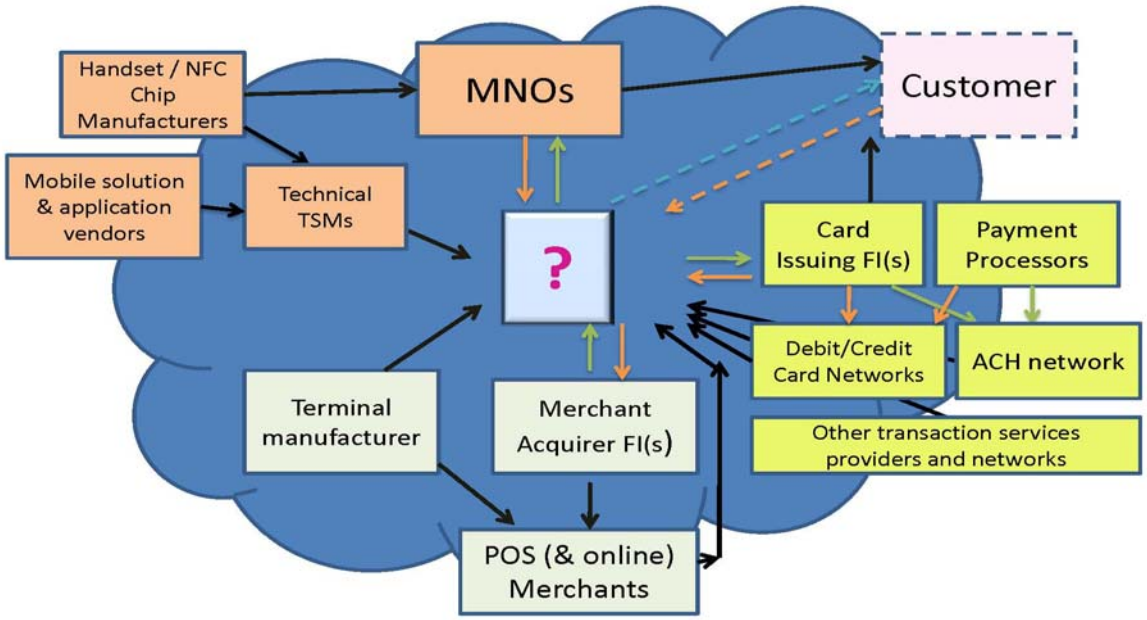
foundational principles. The goal of these principles will be to foster an interoperable mobile payments ecosystem; one that accommodates the customer of any financial institution or mobile carrier, thereby eliminating the need for compulsory customer movement between carrier or card brand (a common complaint today) and allows the customer to use multiple payment methods wherever merchants accept them. It is likely that a mutually agreed upon strategy will be necessary to provide the guidance and incentives to foster the evolution and migration to a ubiquitous mobile environment.

Business models

The major mobile stakeholders must determine the appropriate business model for the mobile payments infrastructure. The decision is complicated by the need to converge payments and mobile communications. The creation of a combined model requires the cooperation of multiple parties, including financial institutions, mobile operators, payment networks, technology service providers, chip and handset makers, and ultimately, merchants and consumers. While the MPIW did not discuss the different models at length, the consensus generally pointed to the possible co-existence of three basic business model scenarios within the mobile payments ecosystem (operator-centric, bank-centric and collaborative). In the operator-centric model the MNO owns the customer relationship for payments made using the mobile phone. In the bank-centric model banks own the customer relationship and mobile payments are processed over traditional payment networks (credit, debit or ACH). Each model could be utilized depending on the type and value of a purchase; the payment venue (e.g. physical POS, remote POS or internet); or other payment scenario.

The collaborative model (see Figure 1) emphasizes the need for an entity that would manage or work with all the parties in the mobile payment ecosystem to facilitate an efficient, holistic environment and provide oversight, business rules and standards for multiple service providers. This entity would serve as a neutral third party to assist other participants in creating a level playing field to facilitate faster and fuller market adoption. On behalf of all participants, it could tackle business issues of mutual need, such as determining the relative liabilities of each party, creating business standards and operating rules for handling customer problems, and leveraging the best practices and expertise of each individual mobile stakeholder.

Figure 1: Collaborative Model



The remainder of this section discusses how the different stakeholders might function with and without a collaborative framework in the mobile payments ecosystem.

Mobile Network Operators, working with partnered handset manufacturers, would continue to control access to the mobile channel and have secure elements configured into their offerings. However, they have limited experience with payment-related application or cryptographic data and while they have extensive account management experience, they have little experience dealing with banking and payment rules and regulations to protect consumers. Without collaboration of some sort, they would need to build new capabilities that go beyond their core business competencies to support mobile devices with broad mobile commerce capabilities; establish thousands of new relationships with financial account holders; and develop complex data centers that comply with industry security standards. Finally, MNOs would have to develop reciprocal agreements for commerce with each other so that account access could travel as easily from device to device as phone numbers do currently. In a collaborative model these elements could be managed by each party agreeing to a central set of guidelines.

Payment Card Networks have existing infrastructures for credit and debit contactless transactions and already perform a rules-making and fee-allocation capability related to card processing and

settlement. However, they lack access to the customer's DDA account and related data. Without collaboration they may not be able or willing to reach agreements about sharing data between competing entities.

Financial Institutions would continue to be at the center of their customers' financial activities, having a more trusted relationship and access to their own customer data, as well as secure data center capabilities that allow them to directly serve existing clients. Consequently, banks are well positioned to move consumers to new technology. However, banks will need the interoperability necessary to handle mobile payments involving other banks' customers and those customers who use different mobile carriers. Otherwise, without an open wallet, an FI would be able to work only with its own customers, unless it had bilateral agreements with other banks and carriers. Absent some scheme that facilitated multilateral relationships, having hundreds of bilateral agreements between banks and MNOs would be inefficient and fragmented, and not work well for mass adoption.[12]

Payment Transaction Processors and Online Payment Service Providers would continue to provide multiple-account payment processing services, perform credit and debit card provisioning and have existing extensive relationships with banks, merchants, credit card networks, pre-paid account service providers and technology providers. They would also have an extensive data support infrastructure to securely handle large amounts of financial and transactional data. While they might be able to provide more agnostic services for handling various credit and debit instruments, without collaboration they would need to establish multiple relationships with mobile carriers and expand relationships with banks to fully service consumer account management.

Mobile Technology Solution Providers, which include mobile payment application developers and TSMs, such as those who provision smartcards, secure elements and NFC chips, have the most experience and expertise with complex technology. While they may have collaborated on technical standards, such as ISO 14443, they have limited experience in dealing with payment rules and regulations to protect consumers. Technology providers would need to develop two-way relationships with carriers and banks, and with each other, since in some cases they are direct competitors.

A successful future mobile payments ecosystem requires an open payments system with interoperable services based on industry accepted formats, and technology standards that allow multiple parties to transact freely, but with some coordination and structure to ensure safety and efficiency within the mobile payments system. A collaborative model could provide stakeholders the opportunity to leverage their respective competencies for the collective good of the payments system overall. However, the number of stakeholders in the mobile ecosystem creates a more complex model that will require time

[12] For example, NACHA rules and ACH operator agreements create the effect of widespread multilateral agreements.

in which to establish industry norms for agreements and standards that will govern the interrelationships and their roles, responsibilities and liabilities. In addition, the MPIW was concerned that excessive coordination can sometimes stifle innovation.

Consequently, the MPIW felt that it was premature to consider such a model in the current market and it was decided to leave this discussion for a later time. Interestingly, a nascent version of the collaborative model was announced in November, 2010, by AT&T Mobility, T-Mobile US and Verizon Wireless, that includes a card network (Discover) and a bank issuer (Barclays Bank U.S.).[13] The joint venture, referred to as Isis™, is chartered to pilot a national mobile commerce network and an NFC mobile wallet. Isis will need to establish the rules of engagement, standards and customer needs within its collaborative effort and plans to have the scope and scale necessary to introduce mobile commerce on a broad basis, hoping to make it available to all interested merchants, banks and mobile carriers going forward.

V. Strategic Fundamentals of the Vision

The U.S. mobile payments market, particularly in the last year, has begun to move down what appears to be an obstacle filled path, absent any shared vision regarding key principles for success. All parties recognize at some level, however, that they share some common goals. Ideally, mobile commerce participants need to be able to flourish equally in the mobile ecosystem. FIs, merchants, payment networks and carriers need to be able to reach their own customers (and potential new customers) with innovative product offerings. Consumers should benefit from products and services that are standard and secure and that make purchase decisions easier for them, while a ubiquitous mobile commerce environment will provide the desired revenue opportunities. Further, through the implementation of common standards, costs can be reduced and integrity of the network increased.

As the MPIW met over the past year, the group's increasingly candid discussions led to a series of shared observations (or shared vision) about the nature of the necessary underpinnings of a successful

[13] On November 16, 2010, AT&T Mobility, T-Mobile USA and Verizon Wireless announced formation of a joint venture chartered with building Isis™, a national mobile commerce network to fundamentally transform how people shop, pay and save. With mobile payments at the core of their offering, they plan to create a mobile wallet that ultimately eliminates the need for consumers to carry cash, credit and debit cards, reward cards, coupons, tickets and transit passes. Isis expects to introduce its service in key geographic markets during the next 18 months. ATT, T-Mobile USA and Verizon Wireless collectively provide wireless services to more than 200 million consumers who will have access to the Isis service. Isis will utilize Discover's national payment network initially, which is currently accepted at over seven million merchant locations in the U.S., to develop an extensive mobile payment infrastructure for the joint venture, and Barclaycard US as the first issuer. See H**http://www.paywithisis.com/#/news/**

future move to mobile NFC payments in the U.S. What follows is the workgroup's assessment of a set of foundational principles necessary to achieve mass adoption of NFC mobile payments in the U.S. These principles will require stakeholders to tightly coordinate efforts to develop a fully integrated end-to-end mobile payments process and represent a set of fundamental "business requirements" for success. The more rapidly they are achieved, the sooner the benefits of mobile payments will be realized.

Foundation Principles

1. Open Mobile Wallet

A successful model for the future should be based on a standard definition of an ***open*** mobile wallet, one that carries broad payment and merchant/marketing value options for consumer choice. Such a platform would embrace a technical architecture that enables the wallet to support a wide range of payment methods and networks, would comply with agreed upon industry business rules and standards, would employ a secure element or container in the mobile phone to interface with the mobile payment applications, and would utilize appropriate wallet protocols and processes, such as the ability for multiple payment applications to share the wallet. The mobile wallet would exhibit all of the flexibility resident in a physical wallet today, including payment-related functions such as loyalty program applications.

Current and planned contactless card/mobile NFC (pilot) deployments are not true mobile wallets by this definition as they offer constrained payment options which limit consumer choice and utility. Since the MPIW views mobile marketing, advertising and promotions, as well as transit, as primary business case drivers for NFC payment deployment (i.e., payment capabilities are a 'qualifying' factor in the business case, but not a 'differentiating' factor), there will be a need to understand and perhaps provide input on or recommend standards for security (including accommodating multiple payment options and applications with multiple secure elements in the handset chip accessing multiple regulated banking networks), privacy, compatibility and interoperability.

2. *Implement a mobile NFC contactless scheme with a specific (embedded) hardware component that may or may not include a micro SD form factor.*

The NFC scheme should be based on an industry standard, capable of supporting all payment methods and networks, able to comply with business rules and standards and reside in a secure container in the mobile phone to interface with mobile payment applications. The contactless NFC solution developed must work globally and in all venues (retail, transportation, as well as ATMs). Contactless payments employing computer chip security and near field communications (NFC or radio wave) technology based on ISO 14443 via mobile devices represent a preferred embodiment of future payments

in the U.S. When used at the POS, the contactless form factor should follow established contactless standards as endorsed by ISO and NFC industry groups, such as SmartCard Alliance, NFC Forum, Mobey Forum, etc. Who would be responsible for designing and developing the solution needs to be determined. Minimum compliance requirements for adoption should include dynamic data authentication, m-wallet contactless functionality and a secure element in the mobile phone.

Utilizing NFC contactless technology for mobile payments assumes that handset manufacturers will commit to putting NFC chips on a large number of new smart phones by some future date. It also assumes that the majority of merchant terminals in the U.S. will simultaneously be upgraded to contactless/NFC. Having some idea of when NFC mobile will be implemented, even without a formal roadmap, would help the merchants plan their investments. Achieving such synchronization, however, will require an extraordinary amount of collaboration, absent a highly participative forum for such discussions.

3. *Establish a ubiquitous platform for mobile payments that uses existing clearing and settlement channels and rails (credit, debit, ACH, prepaid, carrier billing) but allows for new rails as they are developed.*

The existing clearing and settlement rails are the necessary foundation for the mobile payments platform in order to create opportunities for mass adoption and consumer choice. While new payment channels may be created in the future, the MPIW supported the use of existing clearing and settlement systems to exchange payment information and value. Given the ubiquity of the ACH network, and the growing modes and ease of access to it, the ACH option may be critical for supporting a customer's desire to use mobile payments to replace physical cash or check transactions (i.e. non-card transaction) by enabling funds to change hands between parties via direct debit and credit. In addition, merchants who are too small (in sales volume and/or revenue) to qualify for accepting credit/debit cards could use ACH on the mobile phone to accept electronic payments in place of cash or checks.

4. Adopt dynamic data authentication for long-term integrity and security in all card–based transactions and across all channels.

Dynamic data authentication protects cardholder and other payments data by making each mobile payment transaction unique. A valid cryptogram is generated for each transaction, which is then verified when the transaction is authorized. The cryptographic value, including transaction-specific data elements, is validated through the terminal with the network to protect against fraud. The chip device (card or phone) must be present to generate a valid cryptogram, which is verified online or offline when the transaction is authorized. Many issuers already are providing contactless payment cards with dynamic

cryptograms, which is how contactless transactions have improved payment security. Dynamic authentication technology on mobile phones would lower fraud because, absent the sequential codes on the embedded chips, stolen payment card information could not be used to make counterfeit cards or fraudulent online transactions. In addition, the group noted the possibility that this technology could, over time, be applied to the card-not-present venue.

5. *Develop and adopt a global interoperable platform in the U.S. for standards and certification of payment methods for an open mobile wallet, applications, NFC, etc. Leverage existing standards where possible.*[14]

Using a special carrier-issued chip in the phone, consumers currently enjoy the ability to use their mobile phones on a global basis. Adding payment functionality to the phone, however, presents a number of challenges, particularly in the area of compatible standards. There are several existing mobile standards bodies such as GSMA, GlobalPlatform, ETSI (European Telecommunications Standards Institute) and the NFC Forum. Differences in what each standards body addresses and gaps in coverage for mobile payments will need to be identified and resolved, particularly where there is no overarching standard today, as is the case for a TSM in the U.S. Standards for implementing a secure element structure and technology must also be developed to ensure that a secure platform is open and works with multiple applications in the mobile wallet.

Absent a coordinating body, the industry will be hard pressed to analyze applicable global standards and the impacts to the different industry stakeholder groups, determine if changes to the standards are needed to accommodate contactless/NFC mobile payments and what the timeline and resource requirements would be. For the near-term (3-5 years) there is likely to be a wide array of initiatives to be aware of, provide input to, and consider incorporation of for deployment and operation in the U.S.

Full-NFC deployment will involve several infrastructure elements (e.g., a variety of secure elements in handset chips; multiple payment options with separate regulatory requirements in open wallets; management of security and operational services; etc.).

The industry will also need to consider how to address configurations other than full-NFC, such as micro SD cards or NFC stickers that perform lightweight implementations of NFC transacting. Some view these 'NFC-lite' deployments as preceding full-NFC in the U.S., and there are notable pilots involving banks underway and planned. Others view NFC-lite deployments as more likely to continue to occur after full-NFC attains critical-mass adoption, filling in with limited functionality, but sufficient security for users of less-advanced handsets, (i.e. backwards compatibility for awhile). The former view might relieve the industry from expending efforts that distract or dilute mapping out the infrastructure

[14] See Appendix IV for a discussion on current standards activities.

requirements for full-NFC, but the latter view raises the perennial need for the industry to figure out how to accommodate users who lag behind the technology adoption curve.

Finally, additional standards may need to be developed or modified to ensure that the NFC RFID chip communication does not interfere with other wireless network communication. The CTIA can potentially conduct tests to address this issue within its existing device certification initiatives; and improve clarity of member-driven initiatives for device certification. Working with CTIA members, terminal vendors, financial services providers and regulators, such as the FCC, the MPIW could assist in development of a comprehensive consumer, merchant and ecosystem-wide education and monitoring program.

6. Regulatory Clarity

Mobile transacting will cross over domains covered by multiple regulatory agencies—the Fed/FDIC/OCC/NCUA for banks, the Department of Commerce for identity protection, the FCC for wireless carriers, and the FTC for consumer product protection.[15] The MPIW wants to understand sooner rather than later the regulatory focus and oversight regimen of each agency in the mobile payments world, as well as the applicability of current regulations and laws to the mobile environment, in order to avoid potential missteps as they proceed to develop mobile payments solutions. This was viewed by all parties in the MPIW as a key priority for the Fed to initiate and initial steps have been taken to begin dialogues with these agencies. A workgroup assigned to identify regulatory gaps, with supporting resources beyond the original MPIW membership, would assist in such an effort.

7. Trusted Service Managers should oversee the provision of shared security elements used in the mobile phone.

There are several companies that manufacture secure elements. The TSM role would be to manage and control the provision of the secure elements in the mobile phones. The TSM may also perform other account management functions as discussed earlier.

Focusing on the core principles discussed above, the MPIW indicated a desire to continue meeting following a period of broader review of these principles by all stakeholders in the industry. The sense was, that absent any other inclusive industry forum, the continuation of the MPIW, perhaps in some expanded form, would benefit the stakeholders in the mobile ecosystem by providing a venue for the group to begin resolving some of the barriers and issues related to the list of foundational elements in order to successfully incorporate them into a mature system. For example, obstacles that need to be

[15] The new Consumer Finance Protection Bureau (CFPB) may ultimately weigh in on consumer protections for mobile payments.

resolved over the next 3-5 years to achieve true commercial adoption of NFC payments at retail POS may include commercial availability and widespread adoption of smart phones containing NFC chips; secure element resolution (ownership, standards, etc.) and implementation; identification and resolution of technical and business risk and security issues; agreement on the best business models; implementation of contactless readers at an acceptable number of merchant locations; agreement between regulatory agencies on regulatory requirements, assignment and changes (even if the regulatory changes have not yet been legislated); consumer and merchant education plans; etc. Many of these activities will likely need to be completed in overlapping periods, with some dependencies.

The MPIW also discussed the concept of developing an industry roadmap for moving forward, perhaps as a vehicle to clarify direction and encourage faster adoption of necessary change. Typically, such a roadmap might document a detailed explanation of the potential barriers to mobile payment adoption and recommend approaches (with cost/benefit analysis) to address them. A roadmap might also include best practices for the technology (hardware, software, terminals, chips); security (EMV[16] or something similar), dynamic data authentication, secure element (what is in the secure element and how is information involving payment credentials protected, etc.); interoperability; vendor/application management, vetting and certification; consumer relationship management (including enrollment, service and support for phone usage, recovery if lost or stolen, problems if bad applications downloaded); liabilities (who is responsible for exception handling and problem rectification); fraud and risk management practices to address consumer and merchant security; and regulatory protection and education.

In its fullest form, a roadmap could also discuss consumer use from an academic, non-competitive basis. It could identify the consumer value proposition, which is critical for achieving broad adoption. It could address ways to understand what motivates consumers and how to convince them of the benefits of switching payment methods. The roadmap could highlight ways to develop a viral marketing program to build mass adoption. Obtaining a better sense of consumer and merchant preferences and concerns would enhance the roadmap. In other industries, as well as payment associations such as NACHA, roadmaps are augmented by shared surveys directed at various stakeholders, which in this case would be consumers and merchants.

Ultimately, the workgroup felt that it would be premature to try to develop a roadmap that would influence the broad range of mobile payment stakeholders. The mobile payments industry is in its early stages of development in the U.S. and is characterized by experimentation and pilots which typically inform longer term thinking. Moving too early to determine common ground, establish standards, and

[16] EMV is used today in other countries for card payments. The MPIW discussed briefly the possible intersection of EMV with mobile payments in the U.S. For a more detailed discussion, see Appendix II.

develop rules of exchange could stifle innovation and reduce consumer choice. Further, certain key elements of the mobile payments infrastructure are still in pilot phase globally, implying that the adoption of standards (such as NFC standards) may, in some cases, still be a work in progress. In essence, the group felt that attention would be better focused on some selective barriers and issues in the short term and that an industry roadmap might better be approached in the longer term, if market forces produce inefficient outcomes.

Finally, the workgroup touched on another key issue - the role of the consumer helping to secure the future mobile environment. The group felt that future discussions should also include a plan to get consumer buy-in on shared responsibility for risk management. Unlike what unfolded with e-Commerce, where "zero liability" policies by the primary card brands produced a flood of repudiated transactions and so-called 'friendly-fraud' (along with a black market in stolen mag-stripe card credentials often fed by irresponsible cardholder behavior), the mobile venue needs to be *better*. That is, consumers need to buy-in to their role in ensuring a secure, private and efficient payments system and correct the bad habits they developed online. Consumer education related to security is critical for them to understand and know how to identify fraud risks on their end, assist in fraud prevention, and use the security tools that will be available to them in the mature mobile environment. Collaborating in some form to provide such education is a topic that needs to be addressed. Ultimately, the educational process must be coordinated, supported and, potentially enforced within the mobile ecosystem with a goal of helping consumers understand why they should upgrade to more secure handsets and employ best practices for usage in order to protect themselves and the entire mobile payments ecosystem from harm.

VI. Potential benefits of contactless mobile payments ecosystem

The creation of a contactless mobile payments infrastructure in the U.S. would provide a number of definable benefits, including improved fraud reduction capabilities, improved cost efficiencies for merchants and issuers, better data privacy, international compatibility, and reduced risk of settlement.

Fraud reduction

The contactless mobile platform, replete with chip capabilities, can take advantage of the intelligence of the chip and the resultant layering of security tools to provide security features not present in today's mag-stripe environment where skimming and counterfeit production are prevalent. The contactless mobile solution provides the framework for the enhanced security present in the EMV chip+PIN card environment, while also introducing new security layers unique to the mobile phone, including password protection to operate the mobile phone and access applications securely embedded in

the phone. Once at the mobile menu, access to individual mobile banking and payment applications can be further password protected. The EMV chip-based card, which can be replicated in the mobile chip, (although standards for contactless EMV must still be developed), contains individual account credentials, which can remain encrypted to the reader while an authorization is in progress (in some robust implementations). The PIN is also encrypted between the card and the reader, adding a second authentication factor dynamically to the transaction authorization.

Adding mobile data, such as location awareness, phone numbers or carrier accessed device IDs (e.g. MSISDNs or MDNs), can enhance account data, which banks use for risk management and the passing of encrypted tokens and PINs. Among cooperating stakeholders in the mobile ecosystem, utilizing all the data fields and information available with the mobile transaction end-to-end can logically and technically make the mobile transaction even more secure.

The mobile phone can also be used as a security tool for financial payments made at the physical POS and over the internet. The customer is always available, real-time, during a mobile payment transaction. If a network or issuer wished to authenticate customers with a real-time SMS challenge question, application or phone call, it could do so.

Furthermore, in addition to dynamic data for authentication, the mobile channel can support the other big fraud reduction initiative in the U.S.: preventing fraudulent transaction accounts from being set-up using credentials that might have been exposed (credit card numbers, demand deposit accounts, social security numbers, etc.). Better account set-up requires improved registration and enrollment processes, with higher levels of identity verification accessibility and utilization. The enrollment process for mobile banking and payments applications, including NFC provisioning and set-up with device-internal protections, could materially improve the registration and verification process. The additional enrollment process supplements the FI's own account-sign-up mechanisms and enables a much broader set of data about the enrollee to be collected.

It will be important to measure fraud reduction resulting from the use of a mobile phone vs. other payment methods to see how much mobile helped to reduce fraud. This may be difficult to do if companies are not willing to be transparent and share their fraud numbers and costs. Bank and other trade associations such as the ABA and AFP collect fraud data from surveys. The CTIA has a voluntary requirement for its members to complete an annual survey and report anonymously so perhaps they could help collect mobile fraud data through a survey.

With proper changes in regulations, this broader set of data has the potential to be shared within the mobile ecosystem. Full NFC implementations, augmented by encryption that works with the secure elements embedded in the phone, make superior payment account and user ID protections readily available. Ultimately, this benefit can result in both lower PCI compliance costs and lower fraud losses.

The MPIW can help maximize the opportunities for overall fraud reduction by working with the players to develop and implement fraud reduction standards for the entire environment that avoid the possibility of the network safety relying on the lowest common denominator. In addition, the group can work with the other parties to enforce standards and pursue bad actors.

Merchant cost efficiency

The one-time cost of conversion to mobile payments may be viewed as a barrier (as described in the next section), but the ongoing and future benefits may be substantial. For example, mobile may provide an opportunity for merchants to reduce PCI inspection costs over time,[17] and reduce the costs and risks of storing sensitive data, as mag-stripe data exposure is eliminated. Short-term or one-time costs, including costs arising from merchant liability to issuers for accounts compromised from data breaches (in a mag-stripe/open-credential paradigm), are projected by some merchants to exceed the actual costs of fraud in the future if the industry stays with a mag-stripe standard. Many large merchants acting unilaterally are adamant about ensuring consumer payment choice, and appear to be prepared to support a number of alternative payment systems that take advantage of mobile and contactless capabilities. This includes advanced commitments and investments by merchants in chip+PIN for both offline and online transacting, which signals a growing understanding of the long-term business requirements.

Lower issuer costs

In the mobile payments environment, card issuance costs can be reduced by electronic downloads replacing expensive physical card distribution programs over the long-term. However, plastic cards are expected to co-exist with mobile phone payment options for several years, which will impact cost savings. And, current VISA and MasterCard rules require issuing of cards along with mobile accounts, so customers will carry cards and phones for a few more years. Costs to access TSMs and secure elements, uncertain at this time, must also be factored in. However, customer validation and activation can be simplified through more efficient, fully digital, and more secure (through the Global Platform standard) payment account provisioning, set-up and maintenance via the mobile channel. This would, in time, offset costs associated with phasing out mag-stripe cards. Loading cards to the mobile wallet will be less risky. Lost phones can be secured and remotely deactivated in ways that cards, wallets and purses cannot be, and there is evidence that consumers are much more attentive to the status of their phones. (Industry research states that it takes a consumer 4-8 hours to realize he lost his wallet, but only one hour to realize his phone is lost.) This can reduce fraud from lost payment accounts and make restoration of payment capabilities much faster and easier.

[17] See Visa Europe announcement at 'Hhttp://usa.visa.com/download/merchants/bulletin-tip-020911.pdfH.'

Data privacy

The mobile channel can give a consumer the ability to opt-in or -out of applications and services offered by sellers and advertisers on a timely, case-by-case basis to control and limit access to private information. This requires the mobile channel to have effective and efficient regulatory check-points and roadmaps to ensure that the consumer has sufficient protections. Mobile can also have the broader benefit of triggering a proactive national agenda to drive toward consumer protections that lend themselves to individual preferences, versus universal blocks or hurdles that waste expense and effort to disable when circumstances warrant. Once again, standards developed collaboratively and orchestrated by a central party can enhance the data privacy process.

International compatibility with a chip+PIN standard

Implementing the international chip+PIN standard (or some yet to be defined alternative) generates additional benefits for the NFC mobile phone by making mobile transactions more fraud resistant. Ongoing mobile EMV pilots in Europe demonstrate continued evolution toward that end. Considering a near-term deployment of contactless chip+PIN mobile in the U.S. allows us to anticipate change and move in lock step with the rest of the world.

Economies of scale and cross selling

Mobile NFC technology is also being considered in non-payment and non-banking venues, such as transit and health care. As a result, investments in mobile payment technology may be shared over time, creating better economies of scale that will drive down the cost of future mobile solutions. The convenience and efficiency of the tap-and-go format can support many other applications that provide value-added services. Examples include high volume, high speed ticketing in transit venues; tap-and-go for parking meters, parking lots, and vending machines, and a variety of health care applications (e.g. making integrated, approved and authenticated purchases of medical products and services for insurance-defined accounts like Flexible Spending and Health Saving Accounts). Integrating rewards programs (from banks, merchants and third parties) can efficiently and effectively be orchestrated via mobile NFC wallets and applications as well—potentially increasing ROI for those programs.

Consumer convenience, security and efficiency

Surveys continue to show that consumers want to save time. Tap-and-go payment schemes can overcome the limitations and inefficiencies of 'self-checkout' and turn it into a sought-after mode of transacting, particularly when coupled with emerging shopping applications where the phone is used as a scanning device and barcode reader. Education programs can help consumers and small businesses understand that mobile technology has the potential to provide an even safer environment than exists today if implemented correctly. Consumers also want payment choice, and if possible, ways to consolidate all the cards in their physical wallets.

Increased relevance of marketing, promotions and advertising

The current one-way, one-size fits all broadcast-mode of buyer-seller interaction can be replaced with one-to-one, integrated communications and location-aware, real-time capabilities of mobile transacting. Services will need to be somewhat customized to reach different consumer demographics, since digitally oriented younger adults are more willing to opt-in to highly personalized services and commercial interactions, while older adults may avoid them. Recognizing that there are existing marketing regulations, use of the mobile channel for more extensive marketing may create gaps. Therefore, developing a regulatory roadmap will ensure that the industry invests wisely and appropriately to develop services that work in the interests of buyers and sellers without jeopardizing consumer protections. A properly guided mobile marketing, promotion, and advertising environment may create efficiencies and improvement in relevance, and convert wasted costs and investments into profitable new transaction streams that benefit participants in the mobile ecosystem.

VII. Obstacles to Implementation[18]

Despite the exciting business prospects and other benefits of transacting payments by mobile phone, there remains a significant amount of skepticism about how necessary, and how affordable, the transition to mobile NFC payments and, logically, their extension to EMV or similar standards, will actually be. The convergence of several major changes in the payments environment might finally be wearing down this traditional reluctance to change the status quo. Ironically, the unexpected attraction to mobile NFC increasingly appears to be the catalyst to finally moving from the mag-stripe paradigm to a payment system more fitting to today's digital economy and lifestyle. How and why this is happening makes a great study in consumer preferences and technology transformations.

At least four obstacles to implementation of a mobile NFC payment option with the breadth of impact thought by some to change the entire payments paradigm must be addressed and resolved:

- Cost of deployment
- Lack of adoption for contactless with cards
- Disruptive changes in the status quo for existing payments parties
- New revenue models and how to fund the changes necessary to create the mobile ecosystem

[18] See *Appendix III* for Steve Mott's perspective of contrasting views on what motivates participants in the U.S. mobile payment ecosystem.

Cost of deployment

The biggest obstacle to any transformation is the cost of the change. Upgrading the existing payments infrastructure from mag-stripe to smart cards and PINs has long been resisted by both FIs and merchants due to the apparent lack of a business case for the necessary investment. However, there is a growing sentiment that the conventional 'wisdom' about chip+PIN might have changed due to the need for global interoperability, as well as increased interest in moving to contactless payments on mobile phones.

One key factor about the lack of justification for shifting to chip+PIN might be the realization that the costs of PCI compliance (and clinging to mag-stripe) could soon exceed the costs of actual fraud. Ironically, merchants, who bear most of the costs of attempting to comply with these card credential protections, and who are increasingly exposed to financial liabilities to compensate issuers for mag-stripe fraud from data breaches, would pay more to avert mag-stripe fraud than issuers experience from the fraud itself. So, *any* substantive innovation in payments seems likely to devolve quickly from whether to replace mag-stripe to what technology to replace it with and how fast. Mobile NFC advocates make the case that their technology can facilitate this transition in a number of ways, and may prevent the need for a substantial build-out for chip+PIN contact cards in the process for the U.S.

Contactless advocates, including most big merchants, some of whom have already deployed terminal systems capable of supporting contactless chip+PIN technology, argue that the rest of the world is making steady progress moving to contactless. However, because of the overlap between the card world and mobile payments, some mobile stakeholders believe that it will be necessary to support both contact and contactless options in cards for some time, which if the market proceeds in that direction, will be more expensive.

Slow market adoption of contactless to-date

Why should the U.S. also consider moving to NFC on mobile phones when the first generation of contactless has by some accounts been a disappointment?[19] Three reasons stand out for the apparent slowness in consumer adoption. First, consumers don't really have an incentive to try or use contactless, vis-à-vis their other, familiar payment modes. With respect to more than half the cards issued, consumers aren't aware they can *do* contactless. Additionally, it is difficult for consumers to figure out which merchants accept this format. Finally, banks have done little in the way of promotion, and have done a poor job of explaining to consumers that they will be *safer* with contactless.

[19] In the marketplace since 2004 with an estimated 70 million cards and fobs available for use in 150,000 merchant locations, but too few transactions to report so far.

The concept of mobile NFC is thought by many to address these constraints to consumer adoption by being fun to use, accessible to almost anyone with a mobile phone, and supportive (if the payment 'wallet' is open) of a multitude of payment choices, including prepaid for the un- or under-banked. Mobile devices can offer *added* security by providing more information to augment verification and integration of 'full' NFC, where the radio-wave chip and antenna enable the NFC application to interface with the secure element in the device's chipset. Two-way NFC capabilities may also offer another way for consumers to receive and redeem offers, promotions and coupons from merchants and third-parties—including many innovative exchanges based on location-awareness of mobile devices.[20]

The card networks primed the pump for merchant adoption of first-generation contactless payments, subsidizing the costs and deployment of several hundred thousand terminals, largely in the expectation that contactless would prove faster at checkout, cleaner to handle and therefore a good alternative to cash payments at the counter. But for the most part, the only payment options available are signature-based credit and/or debit, replacing cash transactions that typically cost less than a nickel to process with a signature-card transaction that costs $.15 to $.75 or more. This has not incented merchant support (such as prompting and assisting consumers to try the mechanism out). Additionally, merchants want to see equipment that looks the same and doesn't require retraining staff. Mobile stakeholders must work harder to identify a compelling need for merchants to accept contactless payments.

It is worth noting that as of February, 2011, industry estimates indicated there were 70 million contactless devices (mostly cards) and 150,000 contactless merchant terminals in the U.S. Despite the obstacles, this evolution of contactless cards at POS has been valuable, preparing and providing the industry with the experience needed to move to the next phase of contactless payments with mobile phones.

Merchants, from a variety of recent reports and publications, appear to have high expectations for the coming transformation in the payments environment. In particular, they are pushing for more payment choices with contactless, and pricing that better reflects the common view that mobile contactless—by virtue of being capable of greater safety and efficiency—should cost less than problem-prone mag-stripe payments. In the new consciousness of the raft of recent consumer-protection and merchant-assisting legislation, lower costs should be reflected in more advantageous pricing to merchants and lower purchase prices to consumers.

The NFC deployment configuration supports this new perspective by making an open payment wallet possible; even merchant-provided payment options (e.g., private label, store-card based, stored value) could be offered. That gives the consumer a full set of payment choices, and the possibility of enjoying automated rewards and loyalty benefits managed by the NFC/chip interaction.

[20] It is expected that offers, promotions, and coupons will also be distributed over mobile data channels.

The big inducement for merchants with mobile NFC contactless goes beyond the basic payment transaction. Two-way communications between the customer and the merchant enable more value-added innovations such as location-aware prompting to visit a store; identification of the consumer upon entering the store (to receive customized offers and promotions); facilitation of product promotions and coupon exchanges while shopping; and even a faster and more convenient self-checkout. And while it is fair to speculate that the mobile NFC version of contactless will engender much more merchant support, it is not possible at this time to estimate the revenue benefits associated with this concept.

Mobile NFC also enables the marketplace to bypass an aging, interim technology deployment (EMV contact cards) and focus investment resources on where the market appears to be headed in the future. This opportunity to save money and time should enable the new, mobile payments 'ecosystem' to build out a robust and efficient infrastructure that can benefit all parties.

Ingrained Consumer and Merchant Payment Habits

Perhaps the greatest barrier to change in the U.S. payments system over the past thirty years has been the consumer's comfort with the status quo. Check usage has just begun to decline over the past decade and even then at a reluctant pace. It took a decade to get consumers to utilize ATMs in meaningful numbers. POS systems were technically feasible in the early 1970s, but did not come into meaningful use for two decades. A significant number of beneficiaries still do not select direct deposit of government benefit payments and legislation may be required to achieve the last mile of change.

Merchants have understandably geared their changes to respond to consumer demand, not lead it. The cost of investments in new technology at the point-of-sale and the need to retrain staff to use new technology are clear deterrents to unnecessary change. These forces also tend to maintain the status quo.

Further, in the face of stiff competition, the banking industry has moved over the years to giving away most services (with the exception of credit carrying fees), offering them free of charge to the consumer; and focusing instead on charging for exceptions. Such practices have become a comfortable norm, making it difficult to use pricing as an incentive or disincentive to evoke change.

Finally, over the last fifty years, new payments options have been developed, but virtually no options have been eliminated. The consequence of this approach is inefficiency as a wide range of payment solutions continue to be supported, and even enhanced at the margin, despite apparent inefficiency.

Faced with these existing norms, consumers and businesses don't have a compelling need for changes in payment methods. Similarly, financial institutions faced with many competing investment opportunities in the wake of the economic crisis are not actively pushing change. As a result, progress in realizing a ubiquitous mobile payments ecosystem in the U.S. is likely to be relatively slow unless a

paradigm shift occurs in a key variable, such as fraud experience or regulatory change, or development of a truly new functionality that does not exist in current payment methods.

Revenue Uncertainties

Regulatory impacts are cutting away at many sources of card revenue and the market practices that make this revenue possible. Therefore, it is natural for the conventional payment industry providers to be concerned about the need to make incremental investments in a market in which timing of benefits is unknown, and about the uncertainty over whether they will be able to achieve the same position in the new payments paradigm that they had in the old, given the pressure on fees and the onslaught of new, non-bank competition.

Convergence of the wireless and banking sectors creates another perceived threat to revenue stability. It is assumed that both carriers and banks believe they own the mobile payments customer, provide the bulk of the value for mobile payments, and are attracted by the possibilities of increasing revenues related to transacting over phones. There is, at least, the potential for rivalries between the two powerful industries and many calls for cooperation in order to produce an efficient payment capability with fair compensation and return on investment for building out the necessary infrastructure.

Merchants, however, appear to be adamant about not wanting *two* big contenders in the payments 'food chain.' Instead, they point out that mobile payments ought to be safer and more efficient with the combination of both sources of data and network security from both industries, and that this lower risk and cost should be reflected in more attractive pricing *for the merchants.* Merchants propose a shift from the prevailing view that payment fees should constitute the financial foundation for a mobile transaction system, to a new perspective that payment capabilities might establish the *basis* for a new payment paradigm infrastructure, but not be the primary revenue model per se.[21]

Many of the participants in the old and the new payments ecosystem have expressed support for the development of a visionary infrastructure and a regulatory roadmap to help chart out what infrastructure, market practices and technology requirements can be expected and approved so that they can make the incremental investments needed that will be justified by viable business cases that are exposed to no surprises or undue risks.

Reaching such collaborative and enlightened cooperation will be a substantial challenge and might require a steady, sure hand from regulators from both the banking and the wireless industries to ensure an even playing field. Moreover, it is important to reach a quick consensus on what is required, and what

[21] National Retail Federation. 2011. "Mobile Retailing Blueprint: A Comprehensive Guide for Navigating the Mobile Landscape," January. The blueprint describes new ways for buyers and sellers to interact more efficiently and more gratifyingly with mobile NFC—setting the stage for revenue models based on mobile marketing, promotions, and advertising.

should be shared and non-competitive in the infrastructure, in order to develop and approve cross-industry standards to make certain the new, mobile digital payment system for the 21st century is even more reliable, ubiquitous, and robust than the one it will be replacing.

VIII. Conclusion

This document is a work product stemming from the discussions of a Mobile Payments Industry Workgroup that was organized and convened by the payments research teams at the Federal Reserve Banks of Boston and Atlanta. While the ideas expressed in this document about a future success path for mobile payments in the U.S. are not directly attributable to any single member, they do represent a shared view of the participants about a way forward. Yet, even as the group met over a fifteen month period, many participants engaged in formative, independent partnership efforts to announce pilot initiatives to begin the exploration of mobile payments opportunities in this country. In many cases, the underlying concepts of these pilots are consistent with the vision expressed in Sections IV and V of this document; in other cases they are not. But, in all cases these independent efforts signal an appetite to pursue mobile payments as an important future strategy for payments efficiency, security, and convenience.

In essence, the concepts expressed in this paper represent a good entry point into the evolving mobile space that could create a more sustainable and efficient ecosystem through collaboration and sharing wherever possible. Group members ultimately thought that this could be a better way of doing business- agreeing early in the process on ways to build a highly ubiquitous and interoperable ecosystem model, while still competing fiercely on customer facing products and services. Moreover, by collaborating on key issues such as standards and rules of engagement, the sense was that the U.S. would be better positioned to be a part of a global mobile payments system that recognizes the flexibility and mobility of the phone as a payments instrument.

In other countries where mobile has emerged more rapidly, a central body from government, or one sponsored collectively by key private sector stakeholders, has helped organize and direct collaborative solutions. In some small way, the facilitating efforts of the two Reserve Banks noted above represents a microcosm of the benefits of having a central entity with no apparent “skin in the game” work with industry leaders to advance discussions. By providing administrative and thought leadership, the convening Reserve Banks were able to maintain a level of momentum that has resulted in this work product being developed in what, by industry standards, is a relatively short period of time. More importantly, though, the organizations that participated as members of this work group remained engaged throughout, while clearly expressing their independent views on very difficult key issues. Many of the

participants were meeting face to face for the first time and consequently the group went through a "getting to know you" period that eventually led to a willingness to share more openly for the benefit of a long term outcome desired by all. The need to establish a more enduring collaborative industry body is a decision that lies ahead, following a period of industry experimentation. Similarly, the benefits of establishing a cohesive industry roadmap for the future are yet to be determined, based upon the future identification of meaningful barriers to progress.

Ultimately, the value of this workgroup's efforts will be measured by what happens next. Clearly, there are many more parties who will need to support the ideas set forth in this document, including the benefits of a central coordinating entity to work on behalf of all parties to create a roadmap for the future. Forums for engaging these parties may need to be established. This can only be achieved through broad circulation of the ideas in this paper and a decision by significant market leaders to foster further collaborative work. Existing industry trade groups and membership organizations will need to be an important part of this process. While there are notable precedents of success with such collaborative endeavors in the U.S. and overseas, there is also a long list of initiatives that ultimately failed because parties did not see the tradeoffs of independence and collaboration as beneficial. In many of these occasions, the underlying concepts never came to market or never achieved maturity because the obstacles to success could not be removed through independent efforts.

Yet, the opportunities and benefits of doing business differently with mobile payments in this country seem significant and the obstacles to success do seem daunting. Working together to pursue a common high level vision does appear to promise lesser investments over time by all parties and more rapid accrual of benefits than other options. Moreover, through enlightened collaboration, we all might benefit from the perceived view that if we get mobile payments right, it can be the entrée point to making other financial transaction services safer and more efficient. Beyond that, figuring out how to master fully flexible, digital and real-time transacting in payments and banking services might generate ways to bring more security and efficiency to other transactional domains, such as health care, government licensing, and even voting.

APPENDICES

I. Glossary of Mobile Terms

II. Cost of Converting to EMV in the U.S.

III. Elements of a Mobile Payments Business Case

IV. Mobile Payments Standards in the U.S.

APPENDIX I - Glossary of Mobile Terms

Term	Description
APRU (Average Revenue per User)	• Commonly used financial benchmark measuring the average monthly revenue per mobile subscriber
CDMA (Code Division Multiple Access)	• Technology for digital transmission in which multiple frequencies are used simultaneously with each user having a unique code • Each group of users has a shared code and only users associated with that code can understand each other • Used to send voice, data, and signaling data (such as dialed telephone number) between mobile phones and cell sites • Used in several countries including the U.S. and S. Korea
Contactless Card/Device	• Use of either radio frequency (RF) or infrared technology to allow a payment card or mobile device and the POS terminal to communicate or transact without physical contact • Contactless technology is popular with mass transit, road toll and physical security access applications which require fast transaction speeds. • Consumer holds the contactless card, device or mobile phone in close proximity (2-4 inches) to the merchant POS terminal and the payment account information is communicated wirelessly via radio frequency (RF)
Cryptogram	• A numeric value that is the result of data elements entered into an algorithm and then encrypted; commonly used to validate data integrity.
DDA (Dynamic Data Authentication)	• Protects cardholder and other payments data by making each mobile payment transaction unique. A valid cryptogram is generated for each transaction, which is then verified when the transaction is authorized. The cryptographic value, including transaction-specific data elements, is validated through the terminal with the network to protect against fraud and skimming. The chip device (card or phone) must be present to generate a valid cryptogram, which is verified online or offline when the transaction is authorized.
Downloadable Mobile	• Program residing on a mobile device

Application	• May be pre-installed by the MNO or handset manufacture but usually downloaded by the end-user, either via MNO or FI, or directly from the mobile phone store
EMV – Europay, MasterCard, Visa Specifications (EMV)	• Technical specifications and standards developed jointly by Europay International, MasterCard International and Visa International outlining the interaction between IC (integrated circuit) chip cards and terminals to ensure global interoperability • Standard for interoperation of IC (chip) cards and IC capable POS terminals and ATMs to authenticate credit and debit card payments • Purpose of EMV standard is to allow secure interoperation between EMV compliant IC cards and EMV compliant credit card payment terminals globally • EMV based credit card payment systems improve security (with associated fraud reduction), and the possibility for better control of 'offline' credit card transaction approvals • IC card systems based on EMV are known also as chip and pin
GSM (Global System for Mobile Communication)	• The most widely used digital standard for mobile or telephony • Open, digital cellular technology used to transmit mobile voice and data services • Has international roaming capability, allowing users to access the same services when travelling abroad as at home in over 210 countries
ISO 7816	• ISO standard for chip cards with contacts. The EMV standards are built on ISO 7816.
ISO 14443	• ISO standard for contactless chip cards • ISO 14443 defines two types of contactless standards: Type A (Philips Mifare) and Type B (Motorola) • Type C (Sony) is also widely used in Asia Pacific, but not yet formally adopted by ISO
ISO 18092	• ISO standard for NFC
MMS (Multimedia Messaging Service)	• Standard for mobile messaging systems that enables message to include multimedia objects such as images, audio, video, and rich text as well as plain text in SMS
Mobile Banking	• Access to bank information such as account balances and recent transactions via a mobile device

	• Includes informational and transactional services, including bill pay, funds transfers, alerts
Mobile Bill Pay	• Ability to set up and pay for various bills via a mobile device • Mobile bills could be paid through mobile banking or through a third party or mobile operator
Mobile Ecosystem	• A complex set of interconnected entities and relationships which interact to form a stable functioning payments system • Ecosystem includes all payment system participants in the mobile payments environment, including financial institutions, money service providers, handset makers, technology service providers, mobile network operators, merchants and consumers, etc.
Mobile Marketing	• Provision of advertising for mobile transaction services
Mobile Payment	• Payment initiated from a mobile device. Mobile phone is involved in the initiation and/or confirmation of the payment • Payer may or may not be 'mobile' or 'on the move' • Mobile phone facilitates payment between the two entities in a C2B payment
Mobile Parking (m-parking)	• Type of m-payment • Ability to pay for car parking using a mobile device, typically via text messaging or possibly with a downloadable application
Mobile Commerce	• Purchase of digital content such as ringtones and music, or physical goods in the same way a consumer would purchase over the internet • Analogous to an e-commerce transaction
Mobile Coupon	• Token, typically issued as a marketing or sales promotion, that can be redeemed at a participating physical or digital merchant • Typically an incentive in the form of a discount on purchase goods • Can be considered a subset of m-marketing, although the coupon itself may represent a cash value and may therefore be more directly transactional
Mobile RDC	• Use of camera-equipped mobile phones for check image capture as a stand-alone application or as part of a broader mobile banking solution

Mobile Remittances	• P2P mobile transaction that crosses national borders
Mobile P2P	• Person-to-person mobile payments • Transfer of funds from one individual to another via a mobile device within the borders of a specific country • Uses SMS to send text messages with payment instructions to third parties, such as the bank accounts of customers, suppliers, or family members • P2P payments very popular in developing countries through service providers such as M-Pesa in Kenya and Smart Communications in the Philippines
Mobile Ticketing	• Ability to pay for , load and store mass transit tickets electronically on a mobile device
Mobile Top-up	• Transferring funds from a funding source (bank account, credit card, etc.) to top-up minutes on a prepaid mobile account • Minutes may be used as an equivalent for cash, allowing the mobile account to become a stored value 'wallet'
Mobile Wallet	• Software application loaded onto a mobile phone to manage payments made from the mobile phone • Can centrally and simultaneously store multiple applications managing customer account/transaction information with financial providers, public transit agencies, or third part entities such as health clubs, schools, and office or apartment buildings • Can also be used to hold and control a number of other applications (for example, payment and loyalty), in much the same way as a physical wallet holds a collection of physical cards • On-device storage technology allowing for the controlled and secure partitioning of information such as payment cards, coupons, mass transit tickets and medical information
Mobile Web	• Version of internet created to be accessed on mobile phones. Also know as mobile internet.
MNO (Mobile Network Operator	• Also known as mobile carrier, the telecommunications business that provides mobile phone service to end-users • Has its own frequency allocation of the radio spectrum • Has the required infrastructure required to provide mobile phone service
MVNO (Mobile Virtual Network Operator)	• Business that provides mobile phone service but does not have its own frequency allocation of radio spectrum or all of the infrastructure required to provide mobile phone service
Mobile originated SMS billing	• Payment method via SMS where the payee originates the payment by sending an SMS text message to the customer

Mobile terminated SMS billing	• Payment method via SMS where the intended payee closes the payment by receiving one or more SMS messages
NFC (Near Field Communications)	• Wireless technology enabling communication between devices over a short distance • Used in mobile POS payments solutions • Short range, high frequency, standards based wireless communication technology which enables the exchange of data between devices in close proximity (less than two to four inches distance) • An extension of ISO 14443 RFID proximity-card standard that combines the interface of a smartcard and a reader into a single device • Communication occurs when two NFC-compatible devices are brought within four centimeters of one another • NFC can operate in one of two modes: passive or active • NFC contactless transactions clear over existing credit card or bank payment networks, not over wireless networks • Because transmission range is so short, NFC-enabled transactions are inherently secure
NFC Sticker	• A token containing RFID technology, allowing for the transfer of information between the token/sticker and the reciprocal contactless reader (e.g. mass transit access gate, contactless POS terminal, etc.)
OTA (Over-the-air provisioning)	• Transportation of messages wirelessly and without landline • Method of distributing new software updates to mobile phones or provisioning handsets with the necessary settings with which to access services such as MMS or WAP
POS (Point of Sale)	• Location where a transaction occurs, which is usually a retail store or similar venue, including public transportation, taxi cabs, restaurants, etc. • Equipment used by the merchant to complete the payment transaction
Premium SMS	• An SMS message for which the sender pays a higher fee than normal to cover the expenses for a good or service delivered
Proximity mobile payment	• Payment to a physical merchant that is initiated from an NFC-enabled mobile phone held in close proximity to the merchant's POS equipment

Remote mobile payment	• Payment initiated from a mobile phone to a recipient (person or device) where the recipient is not in the immediate area
RFID (Radio Frequency Identification)	• Automatic identification method that relies on storing and remotely retrieving data using devices call RFID tags or transponders • An RFID tag can be attached to or incorporated into an object to identify using radio waves • RFID tag contains an IC (integrated circuit) to store and process information and an antenna to receive and transmit the RF signal between devices (e.g. mobile device and a POS reader)
SD Memory Card /micro SD chip	• Secure digital memory card for removable memory in mobile devices • Used as a means of adding additional memory • Micro SD chip is a much smaller version of the SD memory card, which is now being used as a bridge to add contactless memory to mobile devices not equipped with means to interface with contactless POS terminals via RFIC and perform lightweight implementations of NFC transactions
Secure Element	• Platform where applications can be installed, personalized and managed, preferably over-the-air • Combination of hardware, software, interfaces and protocols that enable secure storage and use of credentials for payment, authentication and other services • Location of the security components, including confidential information, within the mobile phone • Location can be the SIM, a separate secure chip in the phone, or an external plug-in card
Short code	• Special shortened telephone numbers used mainly to address SMS and MMS messages from mobile phones • Widely used for such things as TV voting, ordering ringtones, charity donations, requesting product information, and mobile services such as SMS search services • Also known as short numbers or Common Short Codes (CSC)
SIM (Subscriber Identity Module)	• Removable smart card within a GSM mobile phone • Securely stores the service-subscriber key (mobile user account) used to identify a mobile phone to the network • Configured with information essential to authenticating a GSM mobile phone, allowing a phone to receive service whenever the phone is within coverage of a suitable network • SIM card allows users to change phones by removing the SIM card from one mobile phone and inserting it into another mobile

	phone • SIM card can be partitioned to store multiple forms of data • Can be used to host applications such as mobile banking applications
SMS (Short Message Service)	• Service for sending messages of up to 160 characters to mobile phones • Communications protocol allowing the interchange of short text messages between mobile phone devices
TSM (Trusted Service Manager)	• Neutral trusted third party intermediary or service provider that manages downloads of applications to mobile wallets • Securely distributes and manages contactless services for the application service providers' customers using the MNO networks • Provides a single integration point to all mobile operators for financial institutions, transit authorities and retailers that want to provide a payment, ticketing or loyalty application to their customers with NFC-enabled mobile phones • Owner/manager of the master key that controls the Secure Element platform. This allows the TSM to control and authorize service providers to install applications on the SE • Provides services to manage the secure download and life-cycle management of the mobile NFC applications for the FIs, transit authorities and retailers • Does not participate in any contactless transactions using NFC devices • Key functions include interconnecting with MNOs and application service providers; enrolling new customers; updating user interfaces; managing customer databases; managing application lifecycles; managing value-added service such as ticket reloading; and guaranteeing end-to-end security
2D Barcode	A 2D (two-dimensional) barcode is a graphical image that stores information both horizontally -- as one-dimensional bar codes do -- and vertically. As a result, 2D codes can store up to 7,089 characters, significantly more than the 20-character capacity of a one-dimensional barcode. 2D barcodes enable fast data access and often used in conjunction with smart phones. The user photographs a 2D barcode with the camera on a phone equipped with a barcode reader. The reader interprets the encoded URL, which directs the browser to the relevant information on a Web site. This capability has made 2D barcodes useful for mobile marketing.

UICC (Universal Integrated Circuit Card)	• Chip card used in mobile terminals in GSM and UMTS networks • Ensures the integrity and security of all kinds of personal data • Typically holds a few hundred kilobytes
UMTS (Universal Mobile Telecommunications System)	• A third generation (3G) cell phone technology using CDMA as its underlying air interface
USSD (Unstructured Supplementary Service Data)	• Messaging technology unique to GSM phones • In contrast to SMS, which is a store-and-forward delivery system, USSD provides a continuous online session • Associated with a real-time or instant messaging type phone service • Response times are generally quicker than those used for SMS • It is a popular platform for mobile banking in South Africa
WAP (Wireless Application Protocol)	• Open international standard for applications that use wireless communication • Principal application is to enable access to the internet from a mobile device
WAP Browser	• Provides the basic services of a computer based web browser but simplified to operate within the limitations of the mobile phone • Program on mobile device that facilitates access to the mobile or 'real' internet from the mobile device • Commonly used web browser for small mobile devices such as cell phones.

APPENDIX II - Cost of Converting to EMV in the U.S.

In 1998, the Tower Group conducted a detailed study of the cost of converting to EMV *contact* cards.[22] The total costs—most of which would have to occur at and with the POS systems—were calculated to be $12.8 billion. That year, total bankcard fraud, as affecting the banks, was estimated to be less than $1 billion—about a nickel per $100. So it was difficult to make a business case on those numbers.

Yet the rest of the world was proceeding apace with planning deployment of EMV chip+PIN specs, which Europay (now a part of MasterCard), MasterCard, and Visa had developed and contributed as a global standard just a few years before. The specification provided for interoperability and synonymous security for encrypted chip card and PIN credit, debit and stored value payments.

Europe was experiencing much higher rates of fraud than the U.S. due to the lack of ubiquitous and cost-effective telecommunications infrastructure needed to conduct reliable and fast real-time authorizations. The U.S., on the other hand, enjoyed the world's best communications infrastructure. But there was still a lingering realization that eventually, if the rest of the world went to EMV chip+PIN, and the U.S. stayed with mag-stripe, payments fraud would migrate to the U.S., and U.S. travelers and merchants would be disadvantaged by not being able to transact with smart cards. At one point, Visa and MasterCard even proposed mandating the use of chip cards by 2005; that mandate never materialized.

By 2001, Tower Group re-checked its study on switchover costs to chip+PIN.[23] This time the total was $13.4 billion. Merchant costs—adding in the need to accommodate the fast-growing online market—were projected to be three-fourths of the costs (bank authorization system upgrades accounted for 17% and bank network upgrades another 8%). Once again, there was no compelling business case.

Fast-forward to late 2009, when the Smart Card Alliance estimated total U.S. card fraud losses in 2007 at a still-modest $1.7 billion, but indicated that total fraud was dramatically underreported, citing an estimate by the Mercator Advisory Group that adding in all merchant costs and the associated costs such as data breach forensics, lawsuits, undetected fraud, and misclassified issuer losses, the total cost might be more like $16 billion, much of which was borne by merchants.[24] A Kansas City Federal Reserve paper, written by Rick Sullivan in 2010, estimated payment card fraud of about $3.7 billion (using 2006 data), adding in the often unreported merchant costs![25]

[22] Tower Group. 1998. "Smart Cards in the U.S.: An Infrastructure Cost Analysis," June.
[23] Iacobuzio, Theodore. 2001. "Smart Cards in the U.S.: An Infrastructure Cost Analysis (Redux)," Tower Group, February.
[24] SmartCard Alliance. 2009. "Fraud in the U.S. Payments Industry: Fraud Mitigation and Prevention Measures in Use and Chip Card Technology Impact on Fraud," October.
[25] Sullivan, Richard J. 2010. "The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options," Federal Reserve Bank of Kansas City, *Economic Review*, Second Quarter, pp. 101-132.

Importantly, the Alliance warned that retention of the mag-stripe on cards and POS readers would begin to dilute the fraud reduction benefits for countries that deployed EMV chip+PIN. Moreover, the growing dangers of data breaches, with big surges in compromised mag-stripe credentialed accounts, would inevitably require something other than a 'do-nothing' response.

In 2010, Javelin Strategy & Research echoed these concerns with their updated estimate of the cost of converting to chip-based contact cards (perhaps EMV, perhaps not) at $8.6 billion.[26] One of the lingering deployment cost factors remains deployment of PIN-pads and terminals to cover the estimated 60-70% of retail, card-accepting locations that don't have them yet. In the Javelin report, part of the motivation for moving to chip cards has now become the need for a true end-to-end encryption solution to data breach generated fraud and the growing costs and specter of PCI compliance. For example, by mid-2010, estimates to upgrade existing merchant locations that already process PIN-debit to comply with new PCI requirements might cost upwards of $20,000 per store.

The most important argument for EMV contactless is that it could be materially cheaper to implement than contact cards. For example, in the convenience store industry, two-thirds of the outlets pump gas. The average store incurs an average of $700 of card fraud per year. PCI compliance costs $1600 annually—making that a stretch for business case justification all by itself. Outfitting the pumps with remote smart-card/PIN readers would cost an estimated $50-60,000 per store/gas station.[27] With some 8% of retail sales in this retail vertical, EMV contact cards represent a huge hurdle. But contactless phones, communicating to inside the store via a Wi-Fi hotspot, could wind up costing less than $5000 per store.

Some estimates suggest that EMV contactless could cost merchants as little as half the expense of deploying contact card readers (although banks and networks would likely experience little change in their conversion costs). However, to accommodate foreign travelers coming to the U.S. with EMV contact cards, a reasonable number of ATMs, travel venues, entertainment centers and food service facilities likely would need to accept the contact version, and U.S. issuers would still have to issue contact cards to U.S. travelers abroad.

[26] Javelin Strategy & Research. 2010. "End-to-end Encryption, Tokenization and EMV in the U.S.," January.
[27] National Association of Convenience Stores estimate. 2010.

APPENDIX III - Elements of a Mobile Payments Business Case, *by Steve Mott*[28]

Changing the way people pay is difficult enough in any era, given the stability, predictability and fiercely preserved status quo the U.S. card payments system has achieved over the past half-century. By introducing technology (two-way NFC mobile handsets with chip-based security) that departs from the plastic card paradigm and can simultaneously become a catalyst for elimination of the magnetic-stripe infrastructure, the embryonic mobile 'ecosystem' discussed here is propelling an unprecedented disruption in business models—one that has old and new payments providers scrambling to come up with viable business cases.

The contention between old and new, legacy and future, and conventional versus value-added depicts the divergent interests of the mobile ecosystem as the participants jockey for position. Fundamentally, this is a $300 billion industry[29] in which many established companies such as Visa, MasterCard, their big bank members, Amex, Discover, processors like First Data, Global Payments and TSYS, equipment manufacturers, and thousands of Independent Sales Organizations (ISOs), and many others (including consulting companies, law firms, and industry organizations) have profited substantially for decades.

New entrants, which include non-traditional payments companies with considerable presence such as PayPal, Intuit, Apple, and Google in addition to the giant wireless carriers (ATT, Verizon, T-Mobile and Sprint) and the handset manufacturers and application providers, are moving concertedly into the space with new technology innovations and business models. Consumers—especially smart phone users—appear to have put themselves up for grabs, constantly pushing and testing the borders of the walled garden of payments. And merchants, which have moved to the forefront of the discussion due to their singular role in deciding which of these innovations for mobile checkout at POS to embrace, are wielding unprecedented influence in both political and economic elements of this transformation.

Such robust participation suggests the dawning of a new 'payments' ecosystem, from which many more 'parties' will contend for portions of the emerging new revenue models for mobile transacting. If the new paradigm is chip-based contact cards, as many expect, the infrastructure replacement cost could easily be in the $8-12 billion range—75% of which would logically be borne by merchants in terminal upgrades.[30]

One of the lingering deployment cost factors remains deployment of PIN-pads and terminals to cover the estimated 60-70% of retail, card-accepting locations that don't have them yet. Online deployment of PINs is viewed as much easier, with most of the EFT networks and several of the big

[28] This section is adapted from a series of articles written by Steve Mott, Principal, BetterBuyDesign, 2009-2010.
[29] McKinsey & Co. 2009. "Payments Industry Roadmap."
[30] Javelin Strategy & Research, 2010.

processors now adopting software-encrypted PIN-debit capabilities. No additional infrastructure is needed by consumers, merchants or issuers in order to process these transactions over the internet.

Perhaps for the first time in this country's conversion to electronic payments, the sustaining business case appears unlikely to be made principally on garnering new transaction fees or reducing payment processing costs. Rather, it will likely be made by wholly different cost avoidance and revenue drivers altogether. And several external influences are converging to suggest that the new ecosystem will be driven far more by new revenue drivers than 'tolls' for doing payments.

What follows is a general discussion of the elements to a business case, as well as an assessment of the potentially important business case ingredients for the major players in the ecosystem. At this time, it is very difficult to place meaningful estimates on the potential value of each business case element. This will become more possible over time as various pilots are performed, new regulations are finalized, and new technology is unveiled. However, it is important to recognize that the factors discussed below be evaluated as part of a holistic business case assessment both by individual firms and, perhaps, by industry overseers as part of an effort to understand any public policy issues that may emerge. It is also important to note that while few have demonstrated a clear business case for the full adoption of a mobile NFC payment infrastructure in the U.S. to date, the vast range of announced pilots are evidence of widespread interest and anecdotally, many key players are sensing that the time is near.

External Influences on the Business Case

There are a number of disruptive changes occurring in the world of payments today that are upsetting the status quo, and continuing to push conversations about new payments technology, such as incorporation of mobile phone payments, to the over-arching issue of the need to overhaul/replace the existing mag-stripe infrastructure:

1. Security issues with mag-stripe/stolen credentials

Funding terrorist operations with stolen credit card and debit card credentials—which can be easily obtained from hundreds of black market websites for often less than a dollar—raises questions about how long the U.S. can persist in supporting current mag-stripe technology, when chip-based security for credentials is the standard for every other developed country in the world.

NFC payments, using a contactless chip in the handset that houses secure elements that protect account credentials, and communicates them securely through the NFC chip and antenna to the terminal, represents a new payments paradigm. Current and future cost avoidance opportunities and future reputational risk costs stemming from a move from mag-stripe to a mobile

based NFC world should become part of any business case analysis. Data associated with this move can be gleaned from current and proposed initiatives in other countries.

2. PCI compliance requirements and costs

Recent merchant association estimates (most recently from a survey by the Merchant Advisory Group in October 2010) project the amount of money merchants have spent to-date on trying to comply with PCI data protection requirements to be $20 billion or more, with annual costs expected to exceed $2.5 billion by 2014—more than the reported bank cost of payment card fraud itself. If accurate, such an investment would have easily paid for conversion to chip and pin technology. Merchants are uncharacteristically motivated to abandon the mag-stripe paradigm in order to rid themselves of this burden alone.

NFC payments securing account credentials from the handset chip to issuer authentication in a widespread deployment has the potential to greatly reduce merchant PCI issues. Those aspects of PCI compliance that can be satisfied by a robust mobile implementation should be factored into a business case assessment.

3. Endemic Fraud

Most payment card fraud containment activities in the past five years have related to PCI compliance, rather than attacking the sources of fraud,[31] leaving the industry with an ambient issuer fraud rate about $.05 on $100 in spend. That means absolute fraud losses continue to grow with volume, and if merchant and third party fraud losses are counted in the conventional estimate of about $2 billion in ambient card fraud (U.S. issuers only), future fraud losses could be 5-10 times that amount with all parties' losses counted in.

It is getting more difficult to justify continued investments in tweaking the mag-stripe infrastructure—versus investing in stronger, more digitally capable technologies—such as full NFC payments using secure elements and electronic wallet functionality. Future estimates of growth in fraud losses need to be a part of the business case, as opposed to historic costs[32].

4. Exported fraud

[31] VISA submission to the Federal Reserve in anticipation of the proposed rulemakings regarding the Durbin Amendment to the Dodd-Frank Financial Reform Act, fall, 2010.

[32] In late 2009, when the Smart Card Alliance estimated 2007 total U.S. card issuer fraud losses at about $1.7 billion, but indicated that total fraud was dramatically underreported, citing an estimate by Mercator that adding in all merchant and associated costs such as data breach forensics, lawsuits, undetected fraud, and misclassified issuer losses, the total cost was closer to $16 billion --much of which was borne by merchants.

By clinging to mag-stripe, the U.S. also forces overseas deployers of chip+PIN cards to retain the mag-stripe on the cards they issue so that their customers can use them when in this country. Similarly, merchants overseas must prolong use of mag-stripe terminals to accept cards from U.S. customers. In effect, the U.S. is 'exporting' fraud to overseas issuers and merchants; yet few U.S. issuers are converting to EMV so far, and Visa and MasterCard are still non-committal on how fast they might support a conversion to EMV.

EMVCO has completed its initial contactless specification but needs to ensure that it conforms to generic use and interoperability, while Visa and MasterCard state their conversion plans and aim for the same kind of compatibility.

5. Regulatory impacts on signature-based card rates and pricing practices

The Durbin Amendment to the Dodd-Frank Financial Reform Act could result in outcomes that reshape debit card economics and competitive practices. For example, some suggest that in aggregate, the prospects for continued use of signature debit will dim in favor of PIN-debit. An estimated cut of 75% of interchange rates, to a cap of $.12 per transaction, may challenge existing business models for alternative payments in place today. Also, the current regulatory impetus seeks more competitive debit network access choices for consumers and merchants.

In open wallet configurations, where multiple payment types and networks can be accommodated, NFC payments can satisfy emerging requirements for broader payment choice. Final regulations on interchange and options will create a new business case environment for some of the critical parties that may carry over to the mobile environment.

6. Technology shift in consumer behavior

A persistent move is underway to on-the-go, real-time, mobile transacting as part of a versatile digital lifestyle for the young, including a new cohort of mobile bankers. Downloading of applications on increasingly sophisticated smart phones, coupled with the opening up of payment networks (e.g., PayPal, Visa, Intuit, MasterCard, etc.) for applications development, portends unprecedented opening of access for payment transactions. Mobile handsets have begun replacing wallets and pocketbooks with younger and tech-savvy consumers, and offering break-through utility and innovations in lifestyle.

While NFC-'lite' architectures (e.g., micro SD) may satisfy some of the utility of these innovations today, there is growing evidence of a concerted move to full, two-way NFC-enabled handsets—which will both accommodate digital lifestyle enhancing applications and support the commercial innovations discussed below. Use of mobile NFC solutions in symbiotic non-payments

areas will have an "improved economy of scale" effect on payments applications that could bring about improved unit costs.

7. Technology cost improvements.

In growing technology markets, prices characteristically improve over time as sales volume grows and standards are adopted. Because of the state of the mobile evolution in Europe and elsewhere, NFC standards are emerging and terminal manufacturers are deploying systems that already contain elements to support various types of non-mag-stripe card offerings, as well as mobile NFC. In fact, some U.S. merchants have already deployed such capture devices, while others have such plans, and still others are positioned to add on new technology.

This implies that the business case for merchants may not be as daunting as predicted in the whole. If so, the chicken and egg problem of customer demand and ecosystem ubiquity may diminish.

8. Improved buyer-seller interactions at POS

A slower growing economy overall, with little opportunity to raise prices when so many consumers (and businesses) are struggling financially, has propelled merchants to pursue new business models that improve on the poor historical results they have experienced with 'broadcast-mode' advertising, marketing and promotions, such as free standing coupon inserts in newspapers or store circulars. Instead, they are determined to use mobile technology to influence new customers to sample their stores, spend once they get in stores, try products the merchants (and manufacturers) are pushing, and exchange information that helps attract, grow and retain the relationship over time.

Two-way NFC enables real-time, location-aware interactions that combine shopper behavior and history with tailored, one-to-one promotions and integrated loyalty programs. As a result, some merchant groups are advocating a concerted move to contactless technology—bypassing the costs of deploying contact cards where possible. Moreover, the merchant business case for mobile is significantly enriched, if not substantially justified, by the marketing opportunities resident in mobile payment alternatives.

These influences taken together will shape which business models will survive or get traction in the decade ahead for the key participants in the evolving mobile payments ecosystem. In particular, if the U.S. payments market is indeed beginning to migrate to chip secured account credentials and PIN verification of cards at merchant terminals/network interconnections (whether based on the EMV standard

or something perhaps better), there will be many doubts about what interim technologies to invest in until or unless a new payment paradigm takes hold.

But there are fundamental conflicts that exist at the level of basic business interests of many participants in the new ecosystem that further complicate the decision on whether and to what extent to cooperate in a symbiotic sharing of new, non-competitive infrastructure. The differences in the business case pros and cons for the major participants are themselves revealing of the complexities inherent in transitioning a previously isolated business model to a more holistic one that can support the need to scale to huge volumes, provide security in ubiquitous retail environments, and interoperate in a seamless and transparent fashion. Replicating those attributes will be a daunting task.

Conventional Payments Stakeholder Business Challenges

Starting with the existing, conventional payment card transaction providers—banks, bankcard associations/networks, processors, and terminal providers—for whom the status quo—recent regulatory changes in interchange and banking fees notwithstanding—has produced a sustaining and substantive business opportunity, participating in the emerging mobile ecosystem presents unusual business case challenges.

Banks

Twenty years ago, banks depended primarily on interest rate arbitrage for the bulk of their earnings. Today, more than two-thirds (cite?) of bank revenues come from an assortment of fees, charges, and other pricing for services. Tomorrow, banks will earn billions less from consumer fees and pricing (e.g., on checking account overdrafts), and an estimated 75% reduction of interchange revenue on debit cards. Pressures are expected to mount to lower merchant costs for credit cards as well. For the top 10 banks, which control over 90% of credit card revenues, and get 20-30% of overall payment revenues from credit cards, the economics of the signature-based payment cards status quo is declining dramatically. So a lot is riding on making sure that bankcard payment options make it into new venues like mobile.

Implementing EMV contactless could be materially cheaper to implement than contact cards in some retail sectors that have resisted any wholesale change at POS. For example, in the convenience store industry, two-thirds of the outlets pump gas. The average store incurs an average of $700 of card fraud per year. PCI compliance costs them $1600—making that a stretch for business case justification all by itself. Outfitting pumps with remote smart-card/PIN readers would cost an estimated $50-60,000 per station (according to the National Association of Convenience Stores). With some 8% of retail sales in this retail vertical, EMV contact cards represent a huge hurdle. But contactless phones able to communicate into the store via a Wi-Fi hotspot could cost less than $5000 per store.

The banks, and their card payment associations, argue that they already provide consumer access through hundreds of millions of existing payment accounts, and merchant acceptance at 8 million locations. Moreover, they have global networks that already scale to huge volumes and generations of risk management experience. So the business case for their participation in mobile NFC payments is: 'use what's already there' and adapt the existing infrastructure to evolving needs. The question, of course, is at what level of economics for what participants? And whether they will manage a chip+PIN paradigm with more flexibility and balancing of compensation than exists with the mag-stripe model.

Bigger banks experience an intensity of reactions from these influences, owing to both the considerable money they have historically made on signature-based, mag-stripe cards—at least until the coming year—and the investments made in both online and mobile banking and card use. Smaller FIs face a quandary of their own, contrasting a keen and growing desire to be relevant to the digital savvy, under-35 cohort of financial services customers, and the need to find a way to obtain infrastructure services to allow them to do mobile banking, mobile payments, mobile marketing, and—prospectively—chip and pin. Those are daunting choices and investments to make at a time in which industry wide debit card revenues might drop by $15 billion or more.

Payment Networks

While fundamentally aligned with their bigger banking members, Visa and MasterCard as public companies are increasingly driven by the mandate to drive more transactions across their networks—even if they come from non-banks/non-members. Step-by-step, these publicly traded payment networks have pushed into prepaid, contactless, P2P payments and more recently, versions of NFC-based payments, doing pilots with both bank members and non-banks. And, they are not as impacted financially by the regulatory changes sweeping the current payment card business. So, it is logical to expect them to be at the table for any consideration of mobile payments infrastructure and business opportunities.

What is not so certain is the business case for the ecosystem's use of their networks, and ascribing to their network rules and requirements. After decades of exerting material influence over industry pricing, the mobile payments paradigm in the new regulatory environment appears to be seeking different revenue models going forward—particularly those where the mobile handset interaction in merchant locations fosters real-time, location- and customer-aware decisions on purchases, and where big and powerful non-banks (e.g., wireless carriers) are key players.

Closed-loop charge card companies like American Express and Discover stand to play intermediary roles in architecting new variations of mobile payments, as recent market initiatives indicate. Because they have nearly the same merchant acceptance 'pipes' as the credit card payment networks, and can offer national access for tens of millions of consumers with their payment cards, they can be a factor in any new business calculation. For them, the business case is new transaction volumes from potentially new

customers who utilize them for mobile applications, with merchants still willing to pay prevalent credit card transaction fees.

Non-profit payment networks such as the ACH network and other PIN debit networks also provide payment utilities for their financial institution members of all sizes. Volume is also important to these networks as they develop rules to balance the appropriate amount of innovation with risk management for the benefit of their FI members, which enable valuable solutions for their clients.

Processors

Payment card processors are a lynchpin to the existing infrastructure, but will be called upon to make major changes to their network configurations—particularly to accommodate passing encrypted account credentials through their terminals and networks straight through to chip and pin implementing issuers. This is not a trivial task. For example, in order to minimize the deployment changes required in processor environments overseas when EMV was implemented, Visa and MasterCard have temporarily permitted use of static authentication of chip card transactions (rather than dynamically generating unique data) and decrypting the account credentials at the merchant terminal so they could pass through the processor network to the issuers. Similarly, processors were given two-and-a-half years longer to become PCI compliant than their big merchants were, meeting these requirements only by mid-year 2010 as mandates.

Like the payment card associations, the key economic driver is the *volume* of the transactions, versus the interchange fee rate. So as long as processors can derive a business case for making the infrastructure changes, they would be largely indifferent as to what type of payment was being generated. Moreover the liability shift that accompanies robust implementation of chip and pin would largely make processors' lives easier, and perhaps lower cost due to the reduction in charge-back and other exception handling costs.

But, with some exceptions, many processors have remained silent on the much-discussed mobile 'transformation', and have focused on preserving the funding levels that the payment card industry has historically generated, for as long as possible. That is perhaps understandable in a part of the business that has borne the brunt of price compression from both merchant discount fees and the associations' pass-through of acquirer fees for many years. Their clear concern: how many of which alternative payment types and technologies must they tool-up to support?

Terminal Manufacturers

For several years now, higher end POS terminals have spawned a rich array of functionality to support PIN-debit, prepaid, ACH, barcode, and even biometrically authenticated applications. A standard terminal now contains hundreds of potential applications that need only simple downloads or on-site programming to activate. Such application-migration now extends to EMV contact card reading

capabilities, as well as vanilla contactless tap-and-go radio signaling. Attaching a full-NFC reader to these terminals is fairly straightforward, and can cost about $300. Some recent quotes for both EMV contact card and contactless combination readers are around $400 per terminal, if deployed together. For these participants of the ecosystem, change is usually a good (and profitable) occurrence.

Such forward-thinking infrastructure planning has been embraced by some of the nation's biggest merchants. For example, Wal-Mart, BestBuy and HomeDepot—among others—are currently able to accept EMV contact cards around the world, and Wal-Mart has publicly predicted EMV transactions in the near-term (BestBuy and HomeDepot were also early adopters of contactless tap-and-go). Meanwhile, hundreds of smaller merchants in U.S. states along the Canadian border are already accepting EMV card payments from their foreign shoppers using cards issued by Canadian banks.

The sticky problem with terminals, however, is the business case for getting the millions of smaller merchants to upgrade their terminals. For example, there are roughly 400,000 merchants still using Verifone Tranz330 terminals which were first introduced in the mid-1990s. These terminals have limited applications for largely mag-stripe only transactions, and subject the system to much inefficiency—like the ability to commit rudimentary fraud (e.g., with forced draft capture). Many of these merchants are likely to protest even POS upgrades that cost them only a few hundred dollars—just as they have resisted PIN-debit pads over the years, even though the additional monthly cost is typically less than a dollar.

Merchant Requirements

A primary but until recently reticent player in any payment ecosystem is the merchant base. Perhaps emboldened by a recent surge of support from Congress, regulatory agencies and the courts and with an unusual sense of unanimity, U.S. retailers have largely embraced the mobile transformation—partly as a way forward from a payments business model largely unchanged over decades, but mostly as an opportunity to gain one-to-one relationship connections with customers, and truly drive incremental, competitive sales.

To that end the National Retail Federation introduced a report in mid-2010 (updated in January 2011) called the *Mobile Retailing Blueprint*, containing an extensive list of innovations that NFC-enabled and other mobile payments could bring to the retail sector.[33] At the end of 2010 the Merchant Advisory Group published a set of policy and infrastructure recommendations to put their spin on what should be done implement the Blueprint as soon as possible.[34] Among the suggestions: focus deployment on EMV contactless, bypassing EMV contact card deployment where possible, to avoid transitional investments in technologies that will not be essential in the future.

[33] National Retail Federation. 2011.
[34] Merchant Advisory Group. 2010.

Most importantly, though, the merchants active in contactless and NFC mobile payments implementation seek an 'open wallet' configuration, where consumers can load as many payment choices as they want, and merchants can search for the payment options they prefer in the transaction session. Such choices would include standard credit and debit account options, but would not be restricted—as they are today for the most part—from doing PIN-debit, prepaid, merchant private label, or even ACH transactions. Transactions from third parties—PayPal, BlingNation, Obopay, Western Union—could co-exist with those from the traditional payment brands. There is even talk of cross-merchant acceptance of closed-loop, private label, merchant-provided credit and prepaid options

Such new requirements from such an important part of the mobile payment ecosystem foretell a much more competitive environment for transacting than has ever existed before, and makes the notion that both banks and carriers could build their business cases mainly on joint assessments of payment fees a much less likely route for tomorrow's revenue model. In other words, the business case for NFC payments must go beyond the payments component.

Other Ecosystem Participants

New participants in the mobile payment ecosystem (e.g. wireless carriers, application providers/markets, handset makers, security providers, system integrators, trusted service managers, etc.) all have their own revenue and profitability objectives. Until very recently, they expected some portion of payment fees to drive the business case for their participation. While much of the arms-length jockeying between banks and carriers for ecosystem support over the past two to three years concerned which industry would charge the fees (to merchants) and how those fees might be divided up, the recent merchant 'activism' (and apparent exploration of market alternatives) has changed the nature of the 'conversation' toward who provides what value, and what is fair compensation for that value.

Wireless Carriers

Three of the big carriers announced a joint NFC initiative (called Isis) in conjunction with Discover and BarclaysCard in November 2010. Details were sparse, but the idea was that the built-in NFC wallet would be restricted to carrier-specified payments, and the carriers—rather than banks—would earn the interchange portion of merchant fees. Several reports on Isis concluded that besides aversion to any restrictions on payment choice, some merchants were disappointed that a new revenue model that improved on the interchange convention had not materialized.

If nothing else, this announcement put the payments world on notice that some big players with deep pockets wanted to participate. The carriers' ability to package and bundle services built around heavily marketed handsets demonstrates their ability to steer consumers to more and more advanced services. Whatever the fate of Isis might prove to be, carriers appear likely to be important for the front-

end outreach necessary to spur consumer adoption. Moreover, Isis fueled consideration that, while carriers were clearly seeking new sources of stable revenue for a wireless business that underwent constant price compression, the other assets they brought to the mobile table were very important to factor in to the ultimate business case. Certainly their ability to operate huge networks undergoing rapid change, and their ability to incorporate relentlessly evolving technology with persistent risk management challenges made them a worthy partner for mobile commerce.

The biggest revelation was the possibility that carriers, who collect unique handset identification numbers, the cell phone number associated with a registered account, a location over a specific network, and other verifying data, could become valuable fraud mitigation partners with banks, which know a purchaser's registered account number, associated authenticating information, bank account history and behavior, and usage patterns. In combination, mobile payments could be materially safer than any other payment mechanism, and the properties of end-to-end digital transmission and authentication points could make mobile payments more efficient as well. Regardless of all the above motivations, carriers stand to handle and charge for more traffic across their networks than experienced in traditional non-mobile payments systems.

Application Providers/Marketers

Any observer of the explosive phenomenon of Apple iPhones and their cavalcade of applications (including dozens of payment utilities for both consumers and merchants) can see where the mobile payments market is headed. While Apple itself operates as a walled garden (including a set of NFC patents), the application provision market for open Google Android, Blackberry and other handset operating systems ensures that complete payment choice—and self-sufficiency—is a safe bet among smart phone users (28% of the marketplace at year-end 2010).[35]

For some of these companies (e.g., PayPal, BlingNation, Obopay, and Western Union), capturing incremental payments *is* the business model, and garnering payment fees drives the business case. For the most part, these companies gain merchant and bank acceptance at slightly lower fee levels than standard signature-based cards. In a post-Durbin world, however, there is no certainty that these base-level rates will prove sustainable. So even they will need to find other sources of revenue in the value they add.

For online marketers morphing to the mobile environment, such as Google, marketing sources of revenue—i.e., paid searches, lead generation fees, linked advertising, etc.—promise to be as rich as on the internet. In fact, in their previous payments foray for the online market (Google Checkout), the search goliath attempted to make payments transparent to the advertising and marketing propositions—a useful analogy for mobile, perhaps.

[35] Composite estimates of CTIA, ABI Research and other industry research firms.

Moreover, the ability to add real-time, location-aware, one-to-one granularity to essentially 'blind' online interactions offers the potential for much higher fees and profits from results superior to those online. Such optimism is borne out by the surging number of mobile coupon tests being conducted in the marketplace. Initial results of user take-up appear very encouraging for all participants—including merchants which appear willing to pay high rates for consummated purchases than can be demonstrated as incremental and/or taken from competitors.

Technology Providers

Most of the other components of the mobile payments ecosystem sell infrastructure and/or related services to the others. Such technology includes handsets, security components, communications and systems integration, and even shared-services configurations such as Trusted Services Managers (TSMs). Most of these participants are dependent upon a fully secure, two-way NFC paradigm becoming commonplace in the next 2-3 years. Accommodating secure payments is viewed as an essential baseline service that will attract the consumer to other high-value activities, and that, in turn, will further increase demand for their products and services.

To some degree, these participants can 'prime-the-pump' for new infrastructure. For example, Nokia's announcement in late 2010 that all of its smart phones from 2011 forward would be full NFC-enabled help dilute skepticism that an NFC critical mass would ever appear. Google's recent announcement that Android 2.3 would support NFC payments, coupled with reports that millions of NFC-enabled phones were already in the Android pipeline, further buoyed confidence and expectations in this ultimate baseline configuration for mobile payments.

To-date, mobile technology providers tend to embed their products and services in packages crafted by the carriers, and more recently by Apple, Google, and Microsoft—as these computing companies expand their presence into the mobile marketplace. The real costs of this technology (e.g., full NFC components for GSM handsets is believed to cost an incremental $5-$10) is often not visible to the public, but must be accounted for in a business case for *some* member of the mobile payments ecosystem. But that business case does *not* have to be based on payments functionality alone.

Regulatory Road Map/Shared Infrastructure Decisions

All of these uncertainties make business planning precarious, and companies hesitant to invest. So representative constituencies of *all* of these participant groups have asked the Fed to coordinate with other regulatory agencies (such as the FCC and FTC) and provide a 'regulatory road-map' of what functions, activities, and implementations would be viewed as permissible over the next three to five years. These mobile payments ecosystem players are also asking for clarity on what infrastructure can/should be shared on a non-competitive basis.

For example, security is certainly a foundation for market cooperation, as evidenced in TSMs for smart cards worldwide. But other business services that might be critical to market adoption in the U.S., such as standardized contracting among 16,550 banks and credit unions, 5,000 wireless carriers, and millions of merchants, notification services for lost handsets and even (perhaps especially) coordinated risk management are all under consideration.

So the foundational notion that has emerged is to compete on the marketing and personal service value propositions—but not on generalized transaction capabilities. In this sense, payments become a *qualifying* factor for standardized applications and components of shared infrastructure that protect everyone, but the mobile marketing, advertising and promotional components become the bases for *differentiation* (and therefore competition). As such, mobile marketing services become the heart of the business case for NFC payments. (Note: This is really a good point. Let's see if we can incorporate it in the new vision part of the document also.)

Thus, the mobile marketing business case drivers—mostly still to be determined in an empirical way—should be viewed, and researched, as part of a brand new theoretical construct. Under this construct, payment choice, with open and/or interoperable mobile wallets, will enable the market to set its own prices—in all likelihood as a function of actual costs. And superior customer value in facilitating efficient and effective transacting should engender contributions (financial or otherwise) from both buyers and sellers for the new value they receive. Whether that value materializes as purchase commitments from consumers, or incremental purchase bounties from merchants, the specific mechanism is less important than the concept that real value provided will find a path to fair compensation.

APPENDIX IV – Mobile Payments Standards in the U.S.[36]

Mobile payments require multiple industry participants to work together. If collaboration is difficult, adoption will be delayed. Difficulty may arise because the industry is made up of many small participants who are heterogeneous and have very different preferences, because there is a culture of distrust, or because of legal restrictions. All of these issues play a role in the evolution of mobile payments.

Because there are over 16,000 banks and credit unions but just four major mobile carriers (who account for nearly 90% of the handsets used) in the U.S., industry-wide agreements on technology standards and business policies are very difficult to coordinate and negotiate to reach consensus. Bilateral negotiations between a single bank and a single carrier are much easier, but the market share of customers having accounts with both the bank and the carrier for any given pair of institutions is likely to be small, lowering the value of any resulting agreement. The number of parties involved in each transaction: a mobile carrier, a handset manufacturer, a payment network, a mobile software vendor, a bank, a merchant, and a consumer also make it more difficult. The parties must agree on who is responsible for verifying the consumer's identity, resolving disputes, handling customer service, etc.

Coordination problems may be exacerbated by the possibility that the significant players (banks and mobile carriers) both consider the users to be their customers and therefore may want to "own" the relationship with the customer and the rich set of information that mobile payment services yield.[37] And even though four mobile carriers dominate the wireless market, there are 5,000 wireless carriers in the U.S. in total. Nearly all are small, localized carriers that serve customers in rural areas of the country. The FCC does not want those rural carriers to disappear as the industry evolves, so it will be important to integrate them into the mobile ecosystem.

Open industry-wide standards, involving all stakeholders, are necessary to achieve mass adoption of mobile payments. The alternatives are not simple. For instance, mobile carriers could offer payment services without the involvement of banks, perhaps by limiting consumers to pre-pay accounts or by offering consumer credit themselves. Alternatively, a single carrier could contract with a single bank to offer payments services. These types of approaches are feasible, but they face serious hurdles. Limiting consumers to pre-pay accounts reduces the attractiveness of the product, and offering credit services brings carriers into an unfamiliar industry at a large scale, with important regulatory obligations. To succeed on a large scale by contracting with a single bank, consumers must agree to transfer their financial relationship across institutions, something they are often hesitant to do.

[36] Excerpts from Crowe, M., M. Rysman and J. Stavins. 2010. "Mobile Payments in the U.S. at Retail Point of Sale: Current Market and Future Prospects." Federal Reserve Bank of Boston Public Policy Discussion Paper, No. 10-2.
[37] McCarthy, B. 2008. "Mobile Payments: The Linchpin of the Mobile Commerce Economy," White Paper, First Data.

The U.S. is making important progress in developing an industry standard for the technical details for how mobile payments might work, thus overcoming substantial negotiation costs in this regard.

Current Mobile Standards Efforts

The development of open industry-wide standards through collaboration of industry stakeholders may be the best path towards successful adoption of mobile payments. Importantly, an open standard for mobile payments is under development currently. The financial industry standard-setting group ASC X9 is developing U.S. standards, and ISO is developing an international version of the standards. [38] The X9 and ISO standards will specify how a mobile phone securely formats messaging and data elements and delivers that information over payment rails. Any bank, mobile carrier, or other vendor that develops its service in compliance with the standards would be able to participate in the mobile payments market. At this stage, prospects for the ultimate development of mobile payment standards appear to be strong, although their readiness is at least 18 months away. However, developing a standard does not ensure that it will be adopted.

Although standards are currently in place for the transmission of data either remotely or by proximity from a mobile device to allow for mobile commerce, gaps exist and need to be addressed in order to provide an efficient and secure mobile commerce environment. While ISO 14443 describes the physical characteristics of proximity hardware and NFC standards enable the exchange of data wirelessly, the following work efforts are underway to address the gaps.

ISO TC68/SC7/WG10 Mobile Banking / Payments (International)

The ISO study group, convened by the U.S., has identified areas for development of an international standard and will be formally developing standards for the following areas:

- Mobile person-to-person payments, involving a financial institution intermediary
- Life cycle management of banking/payment applications
- Banking alerts
- Banking account Inquiries
- Banking solicitations and offers
- Payer to the secure element authentication
- Discovery of device capabilities
- Technical report on business oriented security requirements

[38] ASC X9 (Accredited Standards Committee X9) is an industry nonprofit association composed of members of the financial services industry. ISO (International Organization for Standardization) is a network of national standards institutes of 162 countries, one member per country. It is the world's largest developer and publisher of international standards.

For the new work item, the group recognized that Payments break down into two broad areas, proximity and remote. There is a consensus that models for point-of-sale payments will heavily leverage the standards in place for NFC contactless payments. The workgroup will set new standards for "Life Cycle Management of Banking/Payment Applications" as well as "Person to Person" payments, including remittances, focusing on mechanisms that leverage clearing and settlement through established banking channels. These standards will include messaging between parties as well as bill and invoice payments.

For banking the workgroup will focus on three areas: "Alerts," "Inquiries" and "Solicitations/Bank Offers." Each will leverage existing standardized technologies, e.g. Short Message Services (SMS), Instant Messaging (IM) and Really Simple Syndication (RSS). For authentication, the workgroup will develop standard interaction models for "Payer to the Secure Element," standard means for the identification of "device capabilities", and document "business oriented security requirements" for sound banking practices.

X9.112-3 - Mobile Commerce (Domestic)

The mobile environment accumulates numerous risk factors, such as: unattended terminals, card-not-present transactions, untrustworthy platforms, and persistent wireless connections. Further, the mobile network operator (MNO) infrastructure may not provide sufficient security that can be relied upon by the financial services industry. From a security perspective mobile commerce suffers all of the same vulnerabilities as the internet and wireless environments combined; and from a business perspective it encompasses three disparate industries: financial services, mobile telecommunications, and manufacturing mobile platforms.

Areas within scope of this standard include but are not limited to the following:

- Mobile transactions, including sending and receiving messages for payments, banking, and commerce
- Mobile payments for person to person (P2P), person to business (P2B), and small business to business (SB2B), including credit card, debit card, and electronic funds transfer (EFT) transactions

Areas not in scope because they are addressed by other ANSI or ISO standards include: PIN Management and Security; Biometric Information Management and Security; Key Management and Security; and mobile marketing (e.g. advertisements, coupons, loyalty programs, catalogs).