Mobile Payments: An Evolving Landscape

As a relatively new financial service, mobile payments have the potential to significantly change how consumers pay for goods and services. Generally, mobile payments[1] are defined as the use of a mobile device—commonly, but not exclusively, a smartphone or tablet computer—to initiate a transfer of funds to people or businesses. The widespread adoption of mobile payments raises critical issues, including the extent to which financial institutions may lose payments-system market share; the adequacy of legal protections and disclosures received by consumers; and, more generally, how banks can ensure compliance with existing laws and regulations. Although the potential benefits of mobile payments have received considerable attention in the media and trade publications, less scrutiny has been given to understanding the unique risks and supervisory issues raised by this technology. This article describes mobile payments technologies, identifies the risks associated with mobile payments, and discusses the existing regulatory framework that applies to the use of these technologies.

Market Characteristics

The mobile payments marketplace is continuing to expand. More than 87 percent of the U.S. population now has a mobile phone,[2] and more than half of those mobile phones are smartphones.[3] Nearly one-third of mobile phone users in 2012 have reported using mobile devices to make a purchase. Consumers spent over $20 billion using a mobile browser or application during the year,[4] and this number is likely to grow as smartphone ownership increases and mobile payments platforms become more widespread. Mobile payments can be made at the point-of-sale (POS) or to facilitate person-to-person payments. In either case, mobile payments are facilitated by the increasing popularity of smartphones, the availability of POS terminals that are equipped to process transactions using near-field communications (NFC),[5] and the growth of alternative cloud-based mobile payment solutions. At least six NFC-equipped cell phones are for sale in the United States,[6] and 50 percent of smartphones could be NFC-equipped by 2014.[7] Projections for

[1] For purposes of this article, mobile payments do not include payments made using financial institution-sponsored online bill payment services. For a discussion of mobile banking, see Jeffrey M. Kopchik, "Mobile Banking Rewards and Risks," ***Supervisory Insights***, Winter 2011 at http://www.fdic.gov/regulations/examinations/supervisory/insights/siwin11/mobile.htm.

[2] Board of Governors of the Federal Reserve System, "Consumers and Mobile Financial Services," March 2012, at http://www.federalreserve.gov/econresdata/mobile-device-report-201203.pdf.

[3] Javelin Strategy & Research, "Mobile Payments Hits $20 billion in 2012," September 2012 (private study available for a fee; also on file with authors).

[4] Ibid.

[5] NFC is a short range wireless communication using an NFC-enabled payment card or smartphone.

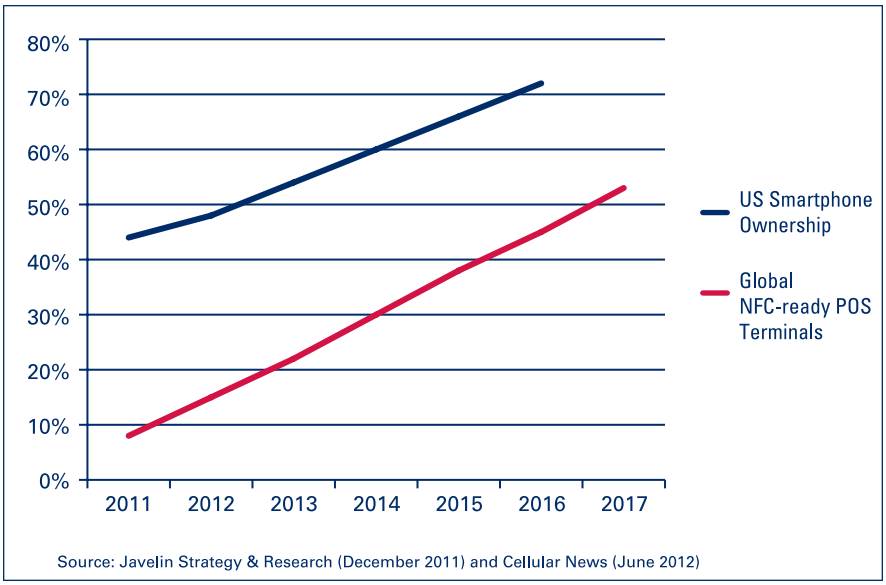
[6] Robin Sidel and Amir Efrati, "What's in Your Mobile Wallet? Not Much," ***Wall Street Journal***, September 26, 2012, at http://online.wsj.com/article/SB10000872396390444180004578016383395015570.html.

[7] Mercator Advisory Group, "Too Early to Call: Five Mobile Giants," May 2012 (private study available for a fee; also on file with authors).

continued from pg. 3

U.S. smartphone and global NFC-ready POS market penetration are shown in Chart 1.

Chart 1: Smartphone and NFC POS Market Penetration



Source: Javelin Strategy & Research (December 2011) and Cellular News (June 2012)

The four major credit card brands (MasterCard, Visa, Discover, and American Express) offer contactless payment technology at the POS, and at least six major merchants accept contactless payments in their stores.[8] In partnership with MasterCard and Visa, Google introduced a mobile wallet in 2011.[9] A mobile wallet allows users to load payment account information on their smartphones, enabling them to choose the payment option. Depending on the underlying technology, users may wave their smartphones near the POS terminal or communicate their payment credentials through a bar code or other cloud-based solution to make a payment. ISIS (a consortium of three mobile telecommunications providers) is conducting NFC mobile wallet pilot projects in Austin, Texas and Salt Lake City, Utah. According to a 2012 study conducted by *Cellular News*, 60 to 80 percent of U.S. consumers would use a mobile wallet from one of the major brands, such as Google, PayPal, or Apple, if available.[10]

Mobile Payments Technologies

Mobile payments can be initiated using different core technologies, either individually or in combination. As the mobile payments marketplace continues to evolve, it is unlikely that any one technology will become dominant in the near term. Retail merchants do not know which mobile payments technologies consumers will find preferable, creating little immediate incentive for investment in new POS terminals that can accept mobile payments. Similarly, consumers have little interest in acquiring the capability to make mobile payments until merchants accept them, or additional incentives are offered making it worthwhile for consumers to try a new form of payment. The mobile payments technologies increasing in popularity are identified in Table 1.

[8] See Mercator, *supra* n. 7 at 32 and 13.

[9] Pew Research Center, "The Future of Money: Smartphone Swiping in the Mobile Age," April 17, 2012, at http://www.pewinternet.org/Reports/2012/Future-of-Money/Overview.aspx.

[10] "If PayPal Offered a Mobile Wallet, 8 in 10 Consumers Would Use It," ***Cellular News***, June 2012, at http://www.cellular-news.com/story/54726.php.

Table 1: Mobile Payments Technologies

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

Although the emerging technologies identified in Table 1 can facilitate mobile payments, established retail payments channels (automated clearing house (ACH), credit/debit networks, electronic funds transfers (EFT), and intra-account transfers) remain the principal ways mobile payments accounts are funded and transactions settled. The only notable exception is mobile carrier-based payments models, which currently have only limited adoption in the United States. Mobile payments typically require users to provide verifiable bank account information or a prepaid card to establish and fund an account. This allows mobile payments companies to leverage existing banking relationships to verify identities, satisfy federal anti-money laundering (AML) requirements, and fund accounts. Thus, with regard to the transfer of funds, the risks associated with mobile payments should be familiar to financial institutions and their regulators, and the corresponding risk controls are well established.[11]

[11] Michele Braun, James McAndrews, William Roberds, and Richard Sullivan, "Understanding Risk Management in Emerging Retail Payments," *Federal Reserve Bank of New York Economic Policy Review*, September 2008, at www.newyorkfed.org/research/epr/08v14n2/0809brau.pdf.

continued from pg. 5

Understanding and Managing Mobile Payments Risk

Mobile payments present the same types of risks to financial institutions associated with many traditional banking-related products, including Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) compliance, fraud, credit/liquidity, operations/IT, reputation, and vendor management. As is the case with any new product offering, a financial institution should have a review and approval process sufficiently broad to ensure compliance with internal policies and applicable laws and regulations. However, unlike most banking products that allow institutions to control much of the interaction, mobile payments require the coordinated and secure exchange of payment information among several unrelated entities. Making matters more challenging is that much of the innovation in the mobile payments marketplace is driven by entrepreneurial companies that may not be familiar with supervisory expectations that apply to banks and their service providers. Depending on the type of mobile payment, financial institutions may find that the effective management of risks involves partnering with application developers, mobile network operators, handset manufacturers, specialized security firms, and others.

Financial institutions should be particularly conscious of the potential and perceived risk of fraud in mobile payments. Customers are more likely to adopt mobile payments if they are confident that the provider, often their bank, has taken appropriate steps to make this service secure by protecting the customer's funds and confidential account information. Encrypting sensitive information stored on the mobile device and providing the ability to disable or wipe the device clean if it is lost or stolen are examples of effective controls that should be carefully considered as part of any mobile payments service. Table 2 identifies the risks posed by mobile payments and briefly describes the challenges in mitigating those risks.

The regulatory expectations for managing mobile payments are generally consistent with those associated with other financial services delivered through more traditional channels. No safe harbors or carve-outs from coverage for mobile payments exist. Thus, mobile payments providers must determine how to comply with existing legal requirements when the application to mobile payments may not be readily apparent. For example, creative solutions may be required to display disclosures on a mobile device's small screen. As not all mobile payments give rise to the same rights, consumers could become confused about which consumer protections apply, or whether they apply at all, resulting in reputation risk. Consumers also may not understand which regulators supervise the parties providing the mobile payments service. Some mobile payments products may provide contractual rights similar to those contained in certain consumer protection statutes; however, these contractual provisions do not have the force of law as described below.

Table 2: Mobile Payments Risks

Category	Risk	Challenge
BSA/AML	Failure to satisfy recordkeeping, screening and reporting requirements intended to detect financial crimes, deter illicit cross-border payments, and prevent terrorist financing.	Ensuring emerging mobile payments models developed (and sometimes managed by third-party service providers) satisfy BSA/AML/OFAC requirements.
Fraud	Failure to prevent or deter unauthorized transactions, the interception of confidential information, or other fraudulent activity.	Ensuring adequate security of account data and other sensitive information and providing methods of "turning off" access to mobile accounts in the event of loss or theft of mobile device. Educating consumers regarding the need to password-protect and otherwise secure their mobile devices.
Compliance	Failure to comply with applicable consumer protection laws, disclosure requirements, and supervisory guidance.	Developing ways to translate disclosure and response requirements to the mobile environment.
Credit/Liquidity	Possible loss from a failure to collect on a credit obligation or otherwise meet a payments-related contractual commitment.	Managing mobile payments credit risk linked to underlying payment type (e.g., credit/debit card, ACH credits/debits, prepaid, EFT, etc.).
Operations/IT	Failure to protect confidential financial information or applications.	Ensuring mobile payments solutions satisfy requirements to safeguard customer information (e.g., Gramm-Leach-Bliley Act) and that such products are developed/configured in a secure manner.
Reputation	Negative consumer experience may reflect poorly on the bank or discourage the use of mobile payments.	Selecting and actively managing mobile payments technology partners and ensuring customer satisfaction with new products.
Vendor Management	Third party may fail to meet expectations, perform poorly, or suffer bankruptcy.	Ongoing due diligence of partner relationships with entrepreneurial companies that may be unfamiliar with operating in regulated environment.

continued from pg. 7

Legal and Supervisory Framework

To date, no federal laws or regulations specifically govern mobile payments. However, to the extent a mobile payment uses an existing payment method, such as ACH or EFT, the laws and regulations that apply to that method also apply to the mobile payment. For example, a mobile payment funded by the user's credit card will be covered by the laws and regulations governing traditional credit card payments. Table 3 provides an overview of selected federal laws and regulations with applicability to mobile payments transactions.

Mobile payments technologies that do not use the existing payments infrastructure would not be subject to laws and regulations that currently cover such payments. In addition, certain mobile payments providers may be subject to the jurisdiction of one or more federal or state regulators

Table 3: Laws and Regulations That Apply to Mobile Payments Transactions

Law or Regulation / Description	Coverage	Applicability to Mobile Payments	Key Obligations / Other Information
Electronic Fund Transfer Act (EFTA) / Regulation E[12] *Establishes rules for electronic fund transfers (EFTs) involving consumers.*	Generally includes any "transaction initiated through an electronic terminal, telephone, computer, or magnetic tape that instructs a financial institution either to credit or debit a consumer's account." This includes transactions such as debit card transactions, direct deposits and withdrawals, and automated teller machine (ATM) transactions. The regulation generally applies to financial institutions, but certain provisions apply to "any person."	Applies when the underlying payment is made from a consumer's account via an EFT.	The rule establishes consumer rights to a number of disclosures and error resolution procedures for unauthorized or otherwise erroneous transactions. The disclosures include upfront disclosures regarding, among other things, the terms and conditions of the EFT service and how error resolution procedures will work.
Truth in Lending Act (TILA) / Regulation Z[13] *Establishes rules regarding consumer credit; intended to help consumers understand the cost of credit and compare credit options.*	Generally applies to "creditors" that offer or extend credit to consumers and includes both open-end and closed-end credit products, including credit cards.	Applies when the underlying source of payment is a credit card (or other credit account covered by TILA and Regulation Z).	Creditors are required to provide disclosures to consumers describing costs; including interest rate, billing rights, and dispute procedures.
Truth-in-Billing[14] *Requires wireless carriers to provide certain billing information to customers.*	Applies to wireless carriers.	Applies when mobile payment results in charges to mobile phone bill.	Wireless carriers must provide clear, correct, and detailed billing information to customers. This includes a description of services provided and charges made.

[12] 15 USC § 1693 et seq., 12 CFR 1005.

[13] 15 USC § 1601 et seq., 12 CFR 1026.

[14] 47 CFR 64.2401.

Law or Regulation / Description	Coverage	Applicability to Mobile Payments	Key Obligations / Other Information
Unfair, Deceptive, or Abusive Acts or Practices (UDAP) under the Federal Trade Commission (FTC) Act /Unfair, Deceptive or Abusive Acts or Practices (UDAAP) under the Consumer Financial Protection Act of 2010[15] *Prohibits "unfair or deceptive acts or practices in or affecting commerce."*	Applicable to any person or entity engaged in commerce. Made applicable to banks pursuant to Section 8 of the Federal Deposit Insurance Act.[16]	Applies to all mobile payments regardless of underlying payment source.	Prohibits "unfair or deceptive acts or practices in or affecting commerce." The Dodd-Frank Act also added the concept of "abusive" practices to "unfair" or "deceptive" ones, and gave the Consumer Financial Protection Bureau (CFPB) authority to further define abusiveness.
Gramm-Leach-Bliley Act (GLBA) Privacy and Data Security Provisions[17] *Establishes rules regarding consumer privacy and customer data security.*	The privacy rules and data security guidelines issued under GLBA apply to "financial institutions," which include depository institutions as well as nonbanks engaged in financial activities.	Applies when a financial institution handles information of a "consumer" or "customer."	Financial institutions are required to provide consumers with certain notices regarding the privacy of nonpublic personal information and allow them to opt out of certain types of information sharing. The GLBA data security provisions give guidance on the appropriate safeguarding of customer information.
Federal Deposit Insurance[18] or NCUA Share Insurance[19] *Protects funds of depositors in insured depository institutions and of members of insured credit unions in the event of failure of the institution.*	Applies to "deposits" and "accounts" as defined in laws and regulations of the FDIC and National Credit Union Administration. These include savings accounts and checking accounts at banks and share accounts and share draft accounts at credit unions.	If the funds underlying a mobile payment are deposited in an account covered by deposit insurance or share insurance, the owner of the funds will receive deposit or share insurance coverage for those funds up to the applicable limit.	Deposit insurance or share insurance does not guarantee that a consumer's funds will be protected in the event of a bankruptcy or insolvency of a nonbank entity in the mobile payment chain.

Note: This table is not exhaustive, and other laws, regulations, and policies may apply.

[15] 15 USC § 45(a); 12 USC § 5536(a)(1)(B).

[16] 12 USC § 1818.

[17] 15 USC § 6801 et seq.; 12 CFR 332 (FDIC privacy rule); 12 CFR 364 App. B (Interagency Guidelines Establishing Information Security Standards, as published in FDIC's rules).

[18] *See* 12 CFR 330.

[19] *See* 12 CFR 745.

continued from pg. 9

(e.g. including federal bank regulators, the Federal Communications Commission, and the Federal Trade Commission).[20]

Looking Forward

In the payments business, banks have traditionally served a variety of intermediary roles between merchants and consumers to facilitate non-cash payments. Banks issue payment cards for customers, process payments for merchants, manage credit/settlement risk for pending transactions, and provide a key link to the payments networks. In the near term, the majority of mobile payments in the U.S. marketplace will be funded by the customer's bank account, and financial institutions will continue to play a key role in facilitating mobile payments. However, as mobile payments evolve, non-bank mobile payments providers may start to capture greater market share from financial institutions and alter bank/customer relationships. Financial institutions should not assume their place in the new mobile payments marketplace is assured because they are an integral part of the existing payments infrastructure. Non-bank mobile payments providers are devising ways to streamline the current payments system and reduce transaction costs by limiting the role banks play in mobile payments or eliminating them from segments of the payments process altogether.

In economic terms, the elimination of an intermediary in a transaction between two parties is known as "disintermediation." Banks could increasingly find themselves displaced by non-banks in the mobile payments marketplace. This evolution could result in the gradual disintermediation of banks as the primary provider of mobile payments. This disintermediation could take several forms. One possible scenario may be a consolidation of the intermediary roles served by banks in the payments process. Nowhere is this more evident than in the payment card acquiring business where it is not unusual to have five or more banks involved in a single card payment.[21] In an alternative payments model such as PayPal, the non-bank mobile payments provider assumes at least three of these bank roles (that of issuing, acquiring, and sponsoring

[20] The FDIC, Office of the Comptroller of the Currency, Federal Reserve Board, and National Credit Union Administration supervise depository institutions and examine them for compliance with applicable laws and regulations. The Consumer Financial Protection Bureau (CFPB) has consumer protection, examination and enforcement jurisdiction over certain nonbank institutions that offer consumer financial products and services and over depository institutions with more than $10 billion in consolidated assets. The CFPB has sole rulemaking authority for most financial consumer protection laws, including the EFTA and TILA and, as such, is instrumental in the regulation of mobile payments, whether through direct supervision or rulemaking authority. The Federal Communications Commission (FCC) has jurisdiction over wireless carriers and is responsible for the Truth-in-Billing rule. Mobile payments products that include wireless bill charges as a payment method may be subject to the FCC's authority. The Federal Trade Commission (FTC) has authority to investigate and take enforcement actions under the FTC Act against almost any entity engaged in commerce, with the exception of entities carved out from FTC jurisdiction, for example, depository institutions and common carriers such as wireless providers. The Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Department of the Treasury, is the administrator of the Bank Secrecy Act.

[21] In the U.S. marketplace, there are at least five distinct roles served by banks involved in processing a single credit/debit card transaction: (1) an issuing bank that holds the customer relationship and authorizes payment; (2) an acquiring bank responsible for providing access to the payment networks; (3) a merchant business bank that holds the funds collected on payments; (4) a settlement bank that moves money among the issuing/acquiring banks; and in some cases (5) a payment card sponsoring bank used to manage bank payment card programs.

banks), thereby removing those banks from the payments process and reducing their business opportunities.

Another potential result of bank disintermediation is a loss of access to key customer data. This can occur as customers provide account credentials to an alternative payments provider to fund an account that will be used to pay for all, or a portion of, a transaction. In this scenario, the alternative payments provider and the merchant control the actual exchange of payment transaction data. Banks may never see the total value of the transaction or even know the true identity of the entity receiving the payment. Thus, detailed transaction data used to identify potential anomalous transactions or provide customized content and product offers may no longer be available to the banks in some alternative mobile payments models. It is the value of this direct connection to the customer and transaction information that is driving these new products and partnerships, as banks consider the implications of ceding this important nexus to non-bank mobile payments providers.

Conclusion

Mobile payments are poised to become an important part of the payments landscape. However, it is unclear when they will achieve popular acceptance and what forms they will take. The majority of industry observers predict a three-to-five year timeframe, and that a limited number of mobile payments models will exist in the marketplace. Both predictions appear well-founded.

The fundamentals of payments risk management should remain constant and, as emphasized in this article, banks offering mobile payments need to ensure compliance with existing laws and regulations. This is particularly important when banks are working with non-bank third-party providers that may not be knowledgeable about the regulatory environment in which financial institutions operate. As a result, banks' oversight of third-party relationships will become increasingly important as mobile payments evolve.

Robert C. Drozdowski
Senior Technology Specialist
Division of Risk Management Supervision
rdrozdowski@fdic.gov

Matthew W. Homer
Policy Analyst
Division of Depositor and Consumer Protection
mhomer@fdic.gov

Elizabeth A. Khalil
Senior Policy Analyst
Division of Depositor and Consumer Protection
ekhalil@fdic.gov

Jeffrey M. Kopchik
Senior Policy Analyst
Division of Risk Management Supervision
jkopchik@fdic.gov