The U.S. REGULATORY LANDSCAPE for MOBILE PAYMENTS

Summary Report of Meeting between Mobile Payments Industry Workgroup and Federal and State Regulators on April 24, 2012

Marianne Crowe, Federal Reserve Bank of Boston,
Mary Kepler and Cynthia Merritt, Federal Reserve Bank of Atlanta

July 25, 2012

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. The authors would like to thank members of the MPIW and representatives of the regulatory agencies for their thoughtful comments and review of the report.

I. Introduction

The use of a mobile phone for payments and related transactions is an emerging channel, and as such has raised questions related to potential gaps in laws and regulations governing these financial transactions. Currently, no one law or governing authority oversees mobile payments. Five financial regulatory agencies (Federal Reserve System (FRS), Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC), National Credit Union Association (NCUA), and the newly created Consumer Financial Protection Bureau (CFPB)), the Federal Trade Commission (FTC), and the Federal Communications Commission (FCC) have some oversight responsibilities depending on the parties and particular issues involved in the mobile transaction. The FCC oversees mobile carrier standards and competition but does not focus on payments made with a mobile phone, while the FTC looks at consumer protection and identity fraud, but much more broadly than financial products and services.

While it is generally understood that current regulations and laws applicable to underlying payment methods (credit, debit, prepaid, ACH) govern mobile payments today, there is still uncertainty about coverage and liability responsibilities, and a desire by industry stakeholders for coordination among regulatory bodies as this new mobile channel develops.

Mobile payment services involve multiple industry stakeholders who may not all fully understand the application of existing laws, regulations, and rule sets. These stakeholders, who represent financial institutions, mobile carriers, and technology service providers, are establishing new business models and delivery methods in the mobile channel where they must determine how best to share the responsibility for consumer protections and regulatory compliance, as well as liability for error and dispute resolution.

Over the course of several meetings between 2010 and 2011, the Mobile Payments Industry Workgroup (MPIW) identified a number of key principles for the long-term direction of mobile payments. One of the key principles is the need for a common understanding in the industry regarding the present regulatory environment. Recently, policymakers have engaged in forums and hearings with industry stakeholders to clarify the state of the industry and determine whether or not regulatory action is currently needed. In light of the heightened attention given the regulatory landscape, the Federal Reserve Banks of Boston and Atlanta convened a meeting with the MPIW and representatives from federal and state banking agencies, the FTC, and the FCC on April 24, 2012,[1] to discuss issues, concerns, and potential gaps in regulatory coverage.

[1] In addition to the federal agencies mentioned above, representatives from the Conference of State Bank Supervisors (CSBS), the Washington State Department of Financial Institutions, and the Massachusetts Division of Banking also attended.

II. Perspectives and Overall Themes

This section highlights several key themes raised in the meeting.

ADEQUACY of CURRENT REGULATORY ENVIRONMENT

The complexity of the regulatory framework for providers of mobile financial services in the United States prompts analysis of potential coverage gaps.

The regulatory environment is segmented into two primary categories; financial institutions comprised of banks and credit unions, and nonbank entities. The United States has a dual charter banking system, with both federal and state chartered institutions. Additionally, non-depository firms or nonbanks engaged in financial services are regulated at the state level. Regulators exercise prudential oversight of banks by conducting supervisory reviews on a regular basis to ensure safety and soundness in the U.S. banking system. With respect to nonbanks that are not engaged in money transfer services, but fill a separate role in mobile payment service models, the Federal Trade Commission (FTC) has authority to bring enforcement actions for unfair or deceptive acts and practices. Finally, the Dodd-Frank Act created the Consumer Financial Protection Bureau (CFPB) in order to consolidate the rulemaking for consumer protections for uniform application to all transactions over an array of firms that provide financial products and services to consumers.

Current mobile payment business models leverage traditional payment sources. For example, in the context of mobile proximity payments where a mobile handset is used to initiate payments, the funding sources consist of credit, debit, and prepaid access (or stored value) payments. Bank card issuers and major card networks collaborate with technology and telecom partners, who provide the platforms and means to send payments data. Consequently, financial institutions, which are empowered to issue payments through traditional channels for clearing and settlement, retain responsibility for the payment providers in these new models.

While the MPIW project scope has focused on retail proximity payments for goods and services, there are two trends that may modify that approach. First, remote payments and money transfers are beginning to emerge to facilitate person-to-person (P2P) payments and cannot be ignored from a regulatory perspective. Second, growth in nonbank money transfer services is subjecting more nontraditional technology-based companies to state money transmitter licenses and related regulatory oversight.[2]

---

[2] Some payments may not fit neatly into categories of remote or proximity as innovations develop. For example, PayPal services are categorized as money transfers and, accordingly, PayPal is registered in 43 U.S. states, the District

Regulators recognize supervisory elements common to both mobile and Internet environments.

The mobile handset is becoming recognized as an access device for payment initiation rather than as an actual payment method. The mobile device serves as a new channel for existing clearing and settlement methods, while simultaneously relying on traditional funding sources for new payment schemes. This distinction is critical to policymakers' understanding of how best to apply the regulatory infrastructure governing mobile payments and their providers going forward.

Today's smartphones have similar functionality to personal computers. Some consumers use both technologies interchangeably, while others—for example, the underserved—may use smartphones in lieu of personal computers to access the Internet. Regulatory representatives collectively agreed that because the mobile and Internet environments share common characteristics, supervision of payments initiated in both environments also share common elements of risk management.

Regulators have interest in ensuring safety and soundness and consumer protection in the emerging mobile payments environment.

- Existing regulatory guidance provides sufficient governance for existing mobile payment services.

  Regulatory agency representatives agreed that existing regulatory guidance for electronic payments applies to mobile payments. This guidance is offered on an interagency and individual agency basis in the form of online handbooks, advisory letters, supervisory insight letters, and other media to supplement regulation and assist financial institutions' compliance program efforts. Regulatory representatives acknowledged that future guidance should contain distinct language that includes "mobile" to ensure clarity and avoid any ambiguity around payments delivered via the mobile channel.

- Regulators will need to stay abreast of mobile industry trends and developments to effectively monitor the emerging risk environment.

  Regulatory representatives noted that they are currently focused on monitoring mobile payment developments to ensure that existing guidance for examination staff is relevant and applicable to emerging risks that could potentially threaten the safety and soundness of financial institutions providing mobile financial services.

---

of Columbia, and Puerto Rico. PayPal recently introduced payment services at the merchant point-of-sale, but relies on the consumer's existing payment choices for funding rather than issuing its own payment method.

Regulators agreed that mobile payment services, and in particular mobile wallets, have insufficient adoption rates and activity at this time to pose any significant systemic risk issues. Industry participants are working to develop business models that balance the sharing of revenue, liability, and accountability for consumer protections. Until those issues are resolved and the mobile payment market matures, financial institutions will remain the trusted entity and the primary provider of proximity funding payment mechanism(s) in mobile wallets.

- Vendor management in new mobile payment business models is critical to ensuring safety and soundness in mobile retail payment systems.

  Current interagency guidance on management of third-party relationships is extensive and applicable to mobile payments. Financial institutions contracting with nonbank partners and other outsourced relationships are accountable for conducting due diligence and ongoing vendor relationship oversight for their nonbank partners. Financial institutions that establish mobile payments service relationships should refer to existing regulatory guidance.

  The Federal Financial Institutions Examination Council (FFIEC) coordinates federal regulation and supervisory decision making. The FFIEC agencies examine technology service providers as part of the multiregional data processing service (MDPS) program.[3] Organizations subject to this program may pose a systemic risk to the banking system if they suffer operational or financial problems because they process applications for many financial institutions.

NEED for EDUCATION of INDUSTRY STAKEHOLDERS, REGULATORS, POLICY-MAKERS, CONSUMER ADVOCATE GROUPS, and CONSUMERS

With the dynamic nature of mobile payments, ongoing education is critical to advance the knowledge of regulators and to address any areas of concern that arise as business models evolve. Areas of interest include the difference between payments initiated from a computer-based Internet environment and payments initiated from the mobile environment. Specifically, regulators want more in-depth knowledge of data privacy, security, and consumer protections for mobile payment transactions. As technology-supporting mobile payment solutions advance, regulators want a better understanding of the new developments and impacts these innovations may have on the entire risk environment.

[3] See the FFIEC program for MDPS organizations at http://ithandbook.ffiec.gov/it-booklets/supervision-of-technology-service-providers/multi-regional-data-processing-servicer-program.aspx.

Consumer advocates can be an influential group with law and rule makers. However, they appear to need more education on the mobile payments environment. The MPIW can educate and build relationships with both consumer and trade groups by providing use cases and fielding consumer advocate group questions in future themed MPIW meetings.

FinCEN[4] should be included in any education efforts because prepaid access is a payment method that is increasingly used in the mobile channel.

The mobile payments industry wants to be better informed of the role of the FCC and its supervisory authority. Because the FCC does not have supervisory authority over the underlying forms of mobile payments, clarification is needed on the FCC's role and interest in mobile payments solutions. The FCC can provide this clarity by participating in future MPIW meetings where regulators are present.

Mobile payment stakeholders need to be well-versed in the security models used in mobile solutions, as evidenced by the debate over the adequacy of security in the different mobile payments business models. Industry agreement on the underlying principles for a secure mobile environment, along with the potential for industry-driven standards, will go far to buoy the reputation of mobile payments solutions. This should also enable secure mobile payments solutions to be developed independently of the underlying technology.

CONCERN for CONSUMER PROTECTION

The FTC, which is charged with protecting consumers from fraud, deception, and unfair business practices in the marketplace, has monitored consumer protection issues arising from developments in mobile technology for close to fifteen years.[5]

---

[4] FinCEN is a bureau of the U.S. Department of the Treasury. FinCEN's mission is to enhance the integrity of financial systems by facilitating the detection and deterrence of financial crime. See http://www.fincen.gov/.

[5] The FTC has held multiple workshops examining consumer issues associated with mobile internet and data technology. Most recently, on May 30, 2012, they held a workshop to explore the challenges of providing consumers with clear and conspicuous disclosures regarding marketing and privacy practices on mobile devices. The FTC has also brought numerous law enforcement actions as well as issuing policy guidance, obtaining settlements from several companies, requiring them to implement comprehensive privacy programs for their internet and mobile services. The FTC has also issued a staff report highlighting the lack of meaningful privacy disclosures associated with mobile applications directed at children.

Since 2008 the FTC has held three workshops specifically examining mobile payments. The most recent workshop was held on April 26, 2012, and focused on three primary areas where consumer protection challenges may arise with the increasing use of mobile payments: dispute resolution, data security, and privacy. The Commission plans to issue a report regarding the workshop shortly.

The FTC has jurisdiction over many companies in the mobile payments ecosystem, including hardware manufacturers, operating system and application developers, data brokers, loyalty program administrators, and advertising companies. The FTC's jurisdiction also extends to telecommunications providers when they are not engaged in common carrier activities. Thus, mobile phone operators engaging in payment functions such as direct-to-carrier billing are also under FTC jurisdiction. With respect to certain nondepository financial service or product providers, the FTC shares joint enforcement jurisdiction with the CFPB.

The CFPB is charged with ensuring that all types of firms engaging in the provision of financial services to consumers comply with applicable consumer protection rules, laws, and regulations. The CFPB would like to understand how the mobile environment changes the consumer payment experience, and if all the current consumer protections and processes to handle billing and fraud disputes are still in place. The CFPB wants to ensure that consumer protections advance concurrently with new mobile payment services, particularly with respect to clear and easily understood disclosures at account enrollment, complaint handling, and error resolution. The CFPB stressed the importance of awareness before engagement of new mobile services.

The CFPB will apply the assessment methodology currently used to review disclosure practices in other financial services. The agency plans to review the effectiveness of disclosure practices in new mobile payment business models to ensure that consumers have sufficient information for appropriate contacts in the event of account discrepancies; assess how disclosures are distributed to consumers; and evaluate how each party to the model handles error resolution issues and liabilities.

IMPACT of NEW MOBILE PAYMENT ENTITIES on REGULATION

Increasingly, nonbank entities from diverse industries, including online payment providers, social networks, and money transmitters, are engaging in mobile payments. They may be subject to different rules and regulations depending on the type of products and services they provide. If they participate in mobile wallet services, they may be subject to the rules and regulations of the underlying funding sources (for example, Reg. E for debit and prepaid, Reg. Z for credit card). If they provide prepaid access on the mobile phone and enable P2P transactions, they are subject to state money transmitter license requirements.

Often, new start-ups engaging in the provision of transfer services lack adequate knowledge of state licensing and regulatory compliance requirements. State licensing fees for some of these new businesses may be cost-prohibitive. Therefore, they may not obtain licenses for all the states in which they operate. As a result, some start-ups may fall outside of the regulatory purview. State regulators, through the Conference of State Bank Supervisors (CSBS), recently created a more uniform application and expanded their nationwide licensing system for mortgage lenders and originators for use to facilitate online multistate licensing for money transmitters and other nonbank financial services providers. The expansion launch occurred on May 1, 2012. Additionally, CSBS and the Money Transmitter Regulators Association are creating a nationwide cooperative supervisory system for the regulation of money transmitters. The multistate agreement would provide for coordinated multistate examination of money transmitters.

Industry stakeholders want regulatory guidance on how to address risk management and security for new mobile technologies (e.g. hardware-based NFC (near field communication) at Point-of-Sale (POS), and software-based barcode apps for POS, remote payments, m-commerce, and P2P). Any guidance should include how information is protected end-to-end through the mobile payment channel and be technology-agnostic.

Use of direct carrier billers (DCBs) also raised concerns with the regulators. Direct carrier billers are intermediaries that handle payments for digital content between consumers and merchants by charging a consumer's mobile phone bill. In this case the consumer is not a customer of a financial institution. Regulators need to understand the differences in scope and risk before considering any new regulations for this business model. Industry regulatory discussions should monitor potential growth of bill-to-mobile services, particularly if this market starts to accept higher value digital purchases or moves to the physical POS venue.

Both the diversity of models and the emerging nature of the mobile payments landscape demonstrate that regulation should not be one size fits all. Depending on the mobile payment business model or use case, the need and level of regulatory oversight may differ. For example, in a partnership between a bank and a mobile carrier, bilateral agreements define who 'owns' the customer, and which party is responsible for error resolution and liability. In this scenario it is clear to whom the regulations apply. As the market evolves towards interoperability and relationships between multiple parties become more transparent, it may be confusing for regulatory bodies to assign responsibility for owning and protecting specific components of the consumer mobile payment transaction.

FINANCIAL INCLUSION AND OTHER GOVERNMENT AGENDAS

The goal of financial inclusion is to help low and moderate income (LMI) and underserved consumers enter the financial mainstream. Emerging technologies such as mobile may decrease costs to the underserved, but ultimately it is important to move the underserved into the banking system for financial management, financial literacy and security of financial transactions. In other countries, governments are more involved in implementing mobile payments for the underserved. Is this a policy issue for the United States to consider?

Prepaid access is expanding from card and Internet to the mobile device. Smartphone ownership growth for underserved consumers is higher than other consumer groups because of the low cost and PC-like functionality of today's modern mobile handsets. As such, many of the underserved are migrating directly from cash-based payments to mobile (prepaid) accounts. This group is a growing portion of the U.S. population and represents our most vulnerable consumers who need to be educated and protected under Reg. E. For mobile prepaid accounts to be viable, they need to incorporate government-issued payments, such as EBT and tax refunds, as well as other payment methods including general purpose debit cards. Is there a need for more regulatory guidance in prepaid than other payment methods because of the higher use of prepaid cards/accounts by underserved consumer segments? Consumer advocates are watching developments in prepaid card and mobile closely.

Participants raised two other concerns. Regulations for prepaid access and the costs to develop prepaid programs may deter banks from participating in this market segment. This may reduce the opportunity for low income consumers to obtain competitive and affordable services. If financial inclusion is a government concern, should these regulations be reviewed?

The FDIC and Treasury are looking at mobile payments for the underserved, but they have no specific current initiatives.[6] The MPIW does not have a targeted objective for mobile financial inclusion, but both the Federal Reserve and Treasury are interested in finding opportunities for mobile solutions to support the underserved.

Other possible areas where the government might consider a more active role: encouraging prepaid mobile for transit; and promoting a more unified move to EMV standards for card-based and mobile payments in the U.S.

The benefits of mobile, such as economic inclusion, consumer choice and access to data, and potentially enhanced security, coincide with government agendas on financial inclusion and promotion of broadband use. Industry stakeholders may be able to proactively avert additional regulation by making regulators and other government agencies aware of the benefits of the mobile channel for payments, and how these benefits can coincide with government agendas.

[6] The U.S. Department of the Treasury recently launched the MyMoneyAppUp Challenge to help Americans gain the tools and information they need to be smarter financial consumers in partnership with the D2D Fund and Center for Financial Services (CFSI). They are seeking new ideas from the public for mobile applications to empower Americans to shape their financial futures everyday – even while on the move. For more information, see http://mymoneyappup.challenge.gov/.

III. Opportunities and Challenges

Opportunities

Neither the regulatory agencies nor industry stakeholders see any immediate need for additional regulation. Clarification of existing regulations and their applicability to mobile payment service providers can increase understanding at the policy level, dispel misperceptions and focus collective energies on potential risk vulnerabilities in the mobile channel.

State and Federal regulatory authorities with oversight of firms engaged in mobile payments should collaborate to develop an effective risk management plan that considers the mobile payment process holistically. A strong risk management process for all new elements/channels will demonstrate that financial institutions have adequate information to assess their risks and conduct sound reviews of their mobile solution vendors.

Bank trade associations want to learn more about mobile payments to enhance their efforts to educate their memberships and facilitate participation and competition on behalf of financial institutions. Continuing dialogue between Federal and State regulators and the financial services community can provide outreach and education, define business strategies and influence more effective risk management.

As business and technical advancements in mobile payment services evolve, the collective regulatory community welcomes ongoing dialogue with the mobile payments industry experts to better understand the emerging mobile payments environment.

Challenges

Consumer education is needed to increase understanding of the security requirements for mobile payments. While surveys confirm consumers are concerned about security in new services, they continue to engage in risky online and mobile service behaviors. Consumer sentiment reflects lack of familiarity with mobile payments.

Vendor and partner management in new mobile payment business models is critical to ensuring safety and soundness in mobile retail payment systems. Current interagency guidance on financial institutions' management of third party relationships is extensive and applicable to mobile payments.

IV. Next Steps

The MPIW plans to continue to meet on regulatory issues with the governing agencies as the mobile payments market matures. The MPIW will use these meetings to educate the regulators about mobile payment developments and associated risk mitigation initiatives in order to avoid unnecessary or over-reactive regulation. Through ongoing discussions, the intent is that regulators will be able to share their early insights and concerns about mobile payments with the MPIW, while hearing stakeholders' input and perspectives on future potential policy and regulatory decision-making. MPIW members will continue to identify the appropriate individuals responsible for addressing legal and regulatory issues in their respective organizations for participation in these meetings.

If the MPIW members are interested, the Federal Reserve representatives will coordinate an education session on the primary regulations (Reg. E, Reg. Z, BSA, etc.) that cover traditional funding methods (credit, debit, prepaid access, and ACH) and their impact on mobile payment processes, risks, security, liabilities, consumer protection and consumer choice.

The MPIW plans to develop tools to educate regulators. The tools will help regulators identify mobile payment areas where they should focus their efforts to ensure that any new guidelines or regulations reflect the multiple models and methods. The MPIW will:

- Document use cases (for business models and consumer payment flow) with principles of risk and security identified.
- Conduct a gap analysis to compare the mobile payment environment to existing payment methods by mapping various mobile payment methods, business models and solutions to existing regulations, focusing on how specific regulations apply to mobile security, risk, consumer protection and liability.
- Develop a glossary of terms for mobile payment methods, models, and technologies with contextual examples
- Review what specific industry organizations such as NACHA, PCI, the card networks, and others are currently doing to address mobile payment regulations.

The MPIW will also develop a communication strategy to reach out to a broader group of representatives with regulatory and policy-making authority, including the FFIEC agencies, FTC, FCC, congressional liaisons, Treasury, consumer advocacy groups, and bank trade associations. This strategy will provide education which may inform rule-making and encourage collaboration for developing consistent and effective guidance on mobile payments to address current confusion and create a formal framework for potential changes.