Update on the U.S. Regulatory Landscape for Mobile Payments

Summary of Meeting between Mobile Payments Industry Workgroup (MPIW) and Federal and State Regulators May 7, 2014

Susan Pandy
Director, Payment Strategies
Federal Reserve Bank of Boston

August 18, 2014

Susan Pandy is a Director in the Payment Strategies Group at the Federal Reserve Bank of Boston.

The author would like to thank members of the MPIW and the participating agencies for their thoughtful comments and review of the report. The views expressed in this paper are solely those of the author and do not reflect official positions of the Federal Reserve Bank of Atlanta, the Federal Reserve Bank of Boston, or the Federal Reserve System.

I. Introduction

A guiding principle of the Mobile Payments Industry Workgroup (MPIW)[1] is the need for a common understanding of the regulatory environment for the mobile payments industry. Key concerns relate to what regulations and laws govern mobile payments funded by underlying payment methods (e.g., credit, debit, prepaid and ACH); how knowledgeable alternative payment providers are, particularly start-ups, with banking laws for consumer protection and privacy, Know Your Customer (KYC),[2] Bank Secrecy Act (BSA),[3] data security, money transmission, and risk compliance; and how to address differences in U.S. regulations related to consumer protections, disclosure requirements and error resolution provisions.

The MPIW held an initial meeting with regulators in April 2012[4] to discuss the above-mentioned issues, concerns, and potential gaps in regulatory coverage of mobile payments in the United States and gain a better understanding of regulatory agencies' current concerns related to mobile-initiated payment transactions. The meeting resulted in several findings: 1) the regulatory environment was adequate for mobile payments at that time; 2) education was needed for industry stakeholders, regulators, policymakers, consumer advocate groups, and consumers; 3) consumer protection needed to be addressed; 4) potential gaps might exist for new payment entities; and 5) mobile payments could impact financial inclusion.

On May 7, 2014, the Federal Reserve Banks of Boston and Atlanta convened a second MPIW meeting with representatives from federal and state agencies.[5] The purpose of the meeting was to discuss the status of: 1) the state of the U.S. mobile payments landscape; 2) the regulators' role in mobile; 3) agency coordination around mobile payments; and 4) mobile payment issues related to security, the role of non-bank solution providers and start-ups, and data privacy. The payments security discussion touched on

[1] For more information about the MPIW, visit http://www.bostonfed.org/bankinfo/payment-strategies/mpiw/index.htm.

[2] **Know Your Customer** (KYC) refers to due diligence activities that financial institutions and other regulated companies must perform to ascertain relevant information from their clients for the purpose of doing business with them. KYC rules are derived from the USA PATRIOT Act Customer Identification Program for financial institutions, which sets out rules and regulations requiring financial institutions to thoroughly and properly identify, verify, and authenticate new customers opening accounts, in order to better keep tabs on the money flowing in and out of America's banks and financial institutions.

[3] The Currency and Foreign Transactions Reporting Act of 1970 (which legislative framework is commonly referred to as the "Bank Secrecy Act" or "BSA") requires U.S. financial institutions to assist U.S. government agencies to detect and prevent money laundering. For more information see http://www.fincen.gov/statutes_regs/bsa/.

[4] For the meeting summary and participating agencies, see http://www.bostonfed.org/bankinfo/payment-strategies/publications/2012/us-regulatory-landscape-for-mobile-payments.pdf.

[5] Federal bank regulators at the meeting included the Federal Reserve Board of Governors (the "FR Board") with representation from legal, consumer and community affairs, banking supervision and regulation, and Reserve Bank operations and payment systems; U.S. Department of Treasury (Treasury); Federal Deposit Insurance Corporation (FDIC); Office of the Comptroller of the Currency (OCC); Consumer Financial Protection Bureau (CFPB); Financial Crimes Enforcement Network (FinCEN); and the National Credit Union Administration (NCUA). State bank regulators included the Conference of State Bank Supervisors (CSBS) and the Massachusetts Division of Banks (representing CSBS). The Federal Trade Commission (FTC) was also present.

recent high profile data breaches, the impending rollout of EMV[6] in the U.S., and announcements of multiple industry efforts to develop tokenization standards.

II. State of the U.S. Mobile Payments Landscape and MPIW Initiatives

The meeting began with a brief overview of trends, activities, and challenges in the mobile payments ecosystem, and the current status of MPIW initiatives, including its security subgroup. To level-set the discussion, a mobile payment was defined as: *the use of a mobile device to make a proximity or remote purchase at a retail point-of-sale (POS), for transit, person-to-person (P2P) money transfer, ticketing, online goods and services, or digital content. Mobile payments are funded via credit or debit card, prepaid account, bank account, or a charge to the consumer's mobile phone bill.* Results from the Federal Reserve Board of Governor's (FR Board) Division of Consumer and Community Affairs (DCCA) March 2014 survey *Consumers and Mobile Financial Services 2014* showed slow growth in mobile payment adoption in the U.S.[7] However, the study also showed that mobile is becoming a channel for financial inclusion[8] based on increasing ownership of mobile phones and smartphones among the unbanked or underbanked,[9] and increased use of prepaid products.

Mobile payment solutions continue to evolve, leveraging technology platforms including near field communication[10] (NFC), cloud, and quick response (QR) codes. The number of diverse stakeholders and solution providers has created many opportunities, but also a highly fragmented market. Other challenges to consumer adoption include privacy and security concerns, the need to address EMV migration,[11] and lack of interoperability and standards. Addressing security and privacy issues is critical, as the progress

[6] EMV is a global specification for credit and debit payment cards based on chip card technology that defines requirements to ensure interoperability between chip-based payment cards and terminals. The primary use for these chip-based cards is to perform payment transactions. The encrypted dynamic data supplied by the chip provides a higher level of protection against counterfeiting than magnetic striped cards. For more information, see http://www.emvco.com.

[7] Available at http://www.federalreserve.gov/econresdata/mobile-device-report-201203.pdf.

[8] "Financial inclusion" is defined as promoting access to and use of safe, affordable financial products and services, and educating consumers about ways to become fully integrated into the banking system. Availability of banking and payment services to the entire population without discrimination is a prime objective of financial inclusion public policy.

[9] The Federal Deposit Insurance Corporation (FDIC), in the *2011 FDIC National Survey of Unbanked and Underbanked Households* (September 2012) defines the "unbanked" as households where no one has a checking or savings account and the "underbanked" as households with a checking and/or a savings account that has used non-bank money orders, non-bank check cashing services, non-bank remittances, payday loans, rent-to-own services, pawn shops, or refund anticipation loans (RALs) in the past 12 months. Throughout this report, the term "underserved" will be used to collectively refer to the unbanked and underbanked, unless otherwise specified.

[10] Near Field Communication (NFC) is a standards-based wireless communication technology that allows data to be exchanged between devices that are a few centimeters apart. NFC-enabled mobile phones incorporate a smart chip (a secure element) that allows the phone to store payment application and consumer account information securely and use the information as a virtual payment card. NFC payment transactions between a mobile phone and a POS terminal use the standard ISO/IEC 14443 communication protocol currently adopted by EMV and U.S. contactless credit and debit cards that allows the mobile phone to emulate a physical contactless card.

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

of the mobile ecosystem hinges on trust and transparency. While the complex mobile payment process may increase the risk of compromise, there are opportunities to leverage the unique mobile phone identifiers, location-based services, and related technologies (such as encryption, tokenization, and EMV) to enhance authentication and security for mobile payments.

III. Role of Regulators in Mobile Payments[12]

A. Federal Bank Regulators

Federal Reserve Board of Governors (FR Board)

The FR Board has a strong interest in maintaining a safe and efficient payment system that will help support economic activity and promote the smooth implementation of monetary policy. As a bank supervisor, the FR Board seeks to ensure the safe and sound operation of banks and to protect the rights of consumers. In light of its responsibilities, the FR Board is closely following developments in mobile payments.

The Legal Division is involved in dialogs with banks, mobile payment providers, and other government agencies with respect to legal issues related to mobile payments. These issues include the sufficiency of legal protections for mobile payment users and the security and confidentiality of payment information that is transmitted and stored. The primary goal of these discussions have been to better understand developments in mobile payments, to evaluate applicable rules and potential gaps, to identify specific problems that may be solved by a rule or statutory change, and to identify laws or regulations that may present barriers to innovation.

The Division of Consumer and Community Affairs (DCCA) considers the potential of mobile technology to affect consumer finances and consumer financial behaviors. They monitor trends in consumer use of mobile technology for payments and banking and how the technology affects services for the underserved, including how it may influence real-time consumer decision-making. The aforementioned *Consumers and Mobile Financial Services 2014* study shows that mobile payment adoption has been constant, but use of mobile payments at POS, in particular, has nearly tripled among smartphone users since the initial study in 2012, possibly driven by convenience and a shift in consumer perception of security.

The Division of Banking Supervision and Regulation (BS&R) has led efforts to identify information technology issues in the financial services industry that represent increasing risk, emerging risk, or

[12] The agency activities outlined and discussed in this section are not comprehensive of all federal and state agency activities.

changing regulatory mandates or guidelines. BS&R focuses mainly on risk management for banks to ensure their safe and sound operation. BS&R is concerned with fraud and security and the inter-connectedness of mobile technology with the payment system through different channels and using different technology platforms. BS&R examines banks as potential providers and users of mobile financial services (MFS). Reviews include compliance with the BSA and anti-money laundering (AML) expectations for banks. The focus has expanded to include security and fraud, which requires ongoing monitoring and current technical expertise to keep pace with changing technology.

The Division of Reserve Bank Operations and Payment Systems (RBOPS) works to promote the efficiency and safety of the payments system and, to that end, actively tracks emerging payment technologies and the risks associated with payment, clearing, and settlement systems. RBOPS works with other departments and federal agencies to analyze emerging payments, including mobile payments. It conducts a triennial study of payment trends[13] and, since 2011, has administered an annual survey on government-administered, general-use prepaid cards[14] in accordance with the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act).[15]

Federal Deposit Insurance Corporation (FDIC)

The FDIC is an independent agency that was created by Congress to maintain stability and public confidence in the nation's financial system by insuring deposits, supervising financial institutions, and managing receiverships. The FDIC's Committee on Economic Inclusion (ComE-IN) provides the agency with advice and recommendations on initiatives aimed at bringing the underserved into mainstream financial services. The ComE-IN has established a Mobile Financial Services (MFS) subcommittee to examine how mobile phone technologies can help increase financial inclusion among the underserved. The Division of Depositor and Consumer Protection and ComE-IN are interested in the potential use of mobile technology for accessing financial services. FDIC staff presented a whitepaper, *Assessing the Economic Inclusion Potential of Mobile Financial Services*, at the April 2014 ComE-IN meeting.

The FDIC also conducts a bi-annual *National Survey of the Unbanked and Underbanked Households*, which is scheduled to be deployed again in 4Q 2014. The agency plans to conduct qualitative research

[13] Available at http://www.frbservices.org/files/communications/pdf/research/2013_payments_study_summary.pdf.
[14] 2013 *Report to the Congress on Government-Administered, General-Use Prepaid Cards* is available at http://federalreserve.gov/publications/government-prepaid/pdf/2013_Prepaid_Cards_FINAL.pdf. The 2014 *Report to the Congress on Government-Administered, General-Use Prepaid Cards* is available at: http://www.federalreserve.gov/publications/other-reports/files/government-prepaid-report-201407.pdf.
[15] The Dodd-Frank Act (Pub. Law 111-203, H.R. 4172) brought significant changes to the American financial regulatory environment that affects all federal financial regulatory agencies and almost every part of the nation's financial services industry. Available at http://www.gpo.gov/fdsys/pkg/PLAW-111publ203/html/PLAW-111publ203.htm.

through focus groups and interviews to learn how the underserved view and use MFS, to identify the features of MFS that could make banking services more appealing to them, and to gain knowledge of consumer preferences and decision-making behaviors. In addition, the FDIC has published several articles about mobile technology.[16]

Office of the Comptroller of the Currency (OCC)

The OCC is an independent bureau of the U.S. Department of the Treasury. Its primary mission is to charter, regulate, and supervise all national banks and federal savings associations. It also supervises the federal branches and agencies of foreign banks to ensure that they operate in a safe and sound manner and are in compliance with laws requiring fair treatment of their customers and fair access to credit and financial products.

The OCC's Payment Risk Policy (PRP) group was created in early 2013, as part of the Chief National Bank Examiner's Operational Risk Division, to provide payments system supervisory guidance and help form a comprehensive view of the payment system, including wholesale (use of centralized payment systems and clearinghouses) and retail (ACH, prepaid, mobile, and digital) payment processes. The PRP group is also analyzing the mobile payments market and evaluating the need to expand existing guidance to be more risk- and principles-based to encompass the increasing range of technologies, and is working with other financial regulatory agencies to develop consensus on any guidance specific to mobile.

PRP generates internal, educational resources for its examiners and senior management. The OCC also recently issued risk management guidance[17] for financial institutions (FIs) that use third party service providers in general, but could apply to mobile services as well. In this way, the OCC supports proactive risk management practices by banks. The PRP also wants to develop metrics (e.g., using data from bank reporting, industry publications, and forums) to identify major payments issues and trends in the payments landscape, which will be shared with its banks and contribute to examiner guidance. The OCC will continue to analyze specific rules to determine whether there is a need to expand these rules to incorporate newer payment technologies.

[16] See *Mobile Monitoring* "FDIC" section for other links.
http://www.fdic.gov/regulations/examinations/supervisory/insights/siwin12/mobile.html.
[17] See OCC Bulletin 2013-29, available at http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

Consumer Financial Protection Bureau (CFPB)[18]

The CFPB was created in July 2010 by the Dodd-Frank Act and began operating in July 2011. It has broad consumer protection responsibilities over multiple consumer financial products and services, including deposits, prepaid products, and money transfers. The CFPB also has rulemaking and interpretive authority for the federal consumer laws most relevant to mobile financial services.

The Electronic Funds Transfer Act (EFTA),[19] as implemented by Regulation E (Reg. E), applies to mobile banking or mobile payment transactions made via electronic fund transfers using a consumer's asset account. The Truth in Lending Act (TILA), as implemented by Regulation Z, applies to mobile payments when the underlying payment is made using a form of covered credit such as a credit card. Currently, transactions from prepaid card accounts are not covered under either regulation, but the CFPB plans to release prepaid card account regulations before the end of 2014.

The CFPB's Card and Payments Markets Division regularly meets with industry stakeholders to understand business models, gather intelligence to understand the payments market, and identify potential regulatory or policy gaps. In this way, the CFPB is evaluating whether there is a need for mobile-specific rules. The agency noted three main concerns around mobile: 1) disclosures, 2) error resolution (particularly for new stakeholders), and 3) security. The pending prepaid rule is expected to include disclosures that are intended to work with mobile as well.

One way the CFPB conducts engagement and outreach with the industry is through its *Project Catalyst*.[20] The Catalyst team holds "office hours" to allow companies of all sizes to exchange information with the CFPB's subject matter experts on an informal basis. It is researching small dollar loans, savings, alternative underwriting, and digital currencies. The CFPB also issued a Notice of Policy regarding its authority under Section 1032(e) of the Dodd-Frank Act to use time-limited waivers to test disclosures (e.g., online-based disclosures and account opening processes).[21]

---

[18] On June 11, 2014, the CFPB issued a press release announcing the launch of an RFI to collect information about mobile financial services and products from the industry, including mobile access to the underserved, real-time money management, customer service and privacy concerns, and data breaches. Responses are due the first week in September. The RFI can be found at http://files.consumerfinance.gov/f/201406_cfpb_request-for-information_mobile.pdf.

[19] The Electronic Fund Transfer Act was passed by the U.S. Congress in 1978 to establish the rights and liabilities of consumers as well as the responsibilities of all participants in electronic funds transfer activities. The act was implemented in Federal Reserve Board Regulation E. Available at http://www.federalreserve.gov/boarddocs/supmanual/cch/efta.pdf.

[20] Project Catalyst's mission is to support innovators in creating consumer-friendly financial products and services through 1) engagement with the innovator community, 2) participation in initiatives that inform our policy work, and 3) staying on top of emerging trends to remain a forward-looking organization. See http://www.consumerfinance.gov/projectcatalyst/ and to subscribe to updates, write projectcatalyst@cfpb.gov and in the subject line, write "subscribe."

[21] Congress gave the CFPB authority to provide certain legal protections to companies to conduct trial disclosure programs. This authority can be used to help further the CFPB's statutory objective to "facilitate access and innovation" in the markets for consumer financial products and services.

National Credit Union Administration (NCUA)

As a regulator and insurer, NCUA's goal is a strong, safe credit union system; hence it is focused on enhancing the capacity of NCUA and credit unions to manage risk. NCUA will continue to provide more clarity in guidance to examiners and credit unions and consistency in agency practices. As it relates to adoption of new technology, such as online and mobile banking, mobile remote deposit capture, and social media, credit unions need to implement controls commensurate with the risks involved, in particular, ensuring the security and stability of these service delivery channels.

Recently, NCUA formed a mobile payments workgroup to increase examiners' understanding of mobile banking and payments. It is creating guidelines for credit union examiners to help them flag particular issues for follow-up by a specialist. The guidance is due for release in 4Q 2014.

B. State Regulators

Conference of State Bank Supervisors (CSBS)

The CSBS is the coordinating body for state banking regulators, whose regulatory responsibilities span state-chartered and state-licensed bank and non-bank financial services providers. This includes state regulators with licensing and supervisory authority pursuant to state money transmission and money service laws that govern the activity of money transmitters, check cashers, and other non-depository businesses. Its discussions with states have indicated growing consumer use and industry interest in mobile payments and mobile banking. Additionally, discussions among state regulators have identified the emergence of virtual currency companies and activities as an area of intersection with state financial services regulation. Earlier in 2014, CSBS announced the creation of an Emerging Payments Task Force comprised of state bank commissioners to review emerging payment issues, including mobile payments, virtual currencies, and payment system modernization. The Task Force plans to complete its analysis by March, 2015.[22]

The CSBS Emerging Payments Task Force, in coordination with State Securities Administrators, issued model consumer guidance[23] and is planning a public hearing to address legacy systems (e.g., ACH, check), innovations in payments (e.g., mobile) and virtual currencies. One goal of the hearings is to respond to the challenges faced by start-ups who must comply with different state laws by developing a more coordinated and consistent framework. It also aims to deliver information (e.g., model laws, regulations) that will modernize how the payment system is viewed. The Task Force expects to share its

[22]For more information, see http://www.csbs.org/news/press-releases/pr2014/Pages/pr-022014.aspx.
[23]*Model State Consumer and Investor Guidance on Virtual Currency* (April 23, 2014). Available at http://www.csbs.org/legislative/testimony/Documents/ModelConsumerGuidance--Virtual%20Currencies.pdf.

legal and regulatory model for payments with its peers, particularly related to money transmission and regulation of virtual currencies.

C. Other Federal Agencies

U.S. Department of Treasury (Treasury), Office of Consumer Policy (OCP)

The OCP leads Treasury's work to ensure that every American has access to safe and affordable financial products and services, and clear information that enables individuals to make sound financial decisions. The office is engaged in policy development in the areas of consumer financial education and capability, emerging payments platforms, technology to improve consumers' financial choices, systems to ensure privacy and data security, and related topics.

The OCP focuses on financial inclusion,[24] particularly as Treasury is the largest issuer of prepaid cards for various government entitlement programs. Its primary concern is how low-to-moderate income (LMI) consumers and the underbanked interact with the financial services system, including banks and non-banks. The OCP also seeks to better understand how the mobile phone and other technology-based tools can be leveraged to help recipients of federal payments (e.g., Temporary Assistance for Needy Families (TANF), child support) to make better financial decisions and manage their money. It created the Financial Empowerment Innovation Fund[25] to support development of related endeavors to help families manage their daily financial lives.

U.S. Department of Treasury, Financial Crimes Enforcement Network (FinCEN)

FinCEN's[26] mission is to enhance the integrity of financial systems by facilitating the detection and deterrence of financial crime through administration of the BSA. FinCEN is responsible for safeguarding the financial system from money laundering and for combatting terrorist financing (CTF). Its regulatory approach to new payments such as mobile is "activities-based," which means that businesses that engage in relevant activities are not exempt from regulations whether the business venue is mobile, online, or brick and mortar. This approach ensures consistent treatment, reducing the likelihood of introducing systemic risk to the payments system. To support this risk-based approach, FinCEN gathers information

[24] Financial inclusion is defined as promoting access to and use of safe, affordable financial products and services, and educating consumers about ways to become fully integrated into the banking system. Availability of banking and payment services to the entire population without discrimination is a prime objective of financial inclusion public policy.
[25] For more information, see http://www.treasury.gov/connect/blog/Pages/Introducing-the-Financial-Empowerment-Innovation-Fund.aspx.
[26] See http://www.fincen.gov/.

about the threats to and vulnerabilities of various systems to determine how to mitigate money laundering and terrorist financing risks. Risk issues are further discussed within its Bank Secrecy Advisory Group.

As part of its outreach efforts, FinCEN continues to engage with the new payments sector. It encourages start-ups, including their engineers and computer science professionals, to understand their AML/CTF responsibilities and work to incorporate regulatory requirements for AML/CTF in the design phase of their mobile/digital solutions.

Federal Trade Commission (FTC)

The FTC's mission is to prevent business practices that are anticompetitive, deceptive or unfair to consumers; enhance informed consumer choice and public understanding of the competitive process; and accomplish this without unduly burdening legitimate business activity. The FTC addresses payment industry issues using the same principles as when approaching other industries, applying principles in Section 5 of the FTC Act[27] that outline unfair and deceptive[28] acts or practices (UDAP). The overriding theme of UDAP is disclosure of clear and accurate information and informed consumer choice.[29]

The FTC Bureau of Consumer Protection, Division of Financial Practices, has broad authority to protect consumers in the areas of unauthorized charges, data security, and privacy.[30] Many FTC enforcement cases have been against companies for "cramming"[31] (unauthorized transactions on consumer mobile phone bills, a common occurrence among certain subscription services). The FTC has also brought actions related to in-app purchasing on mobile phones in which children use their parents' phones to make purchases within gaming apps without the informed consent of the parent or the accountholder, resulting in disputed charges.[32]

IV. Perspectives and Key Discussion Issues

While the findings from the May 2012 meeting continue to be monitored, the May 2014 meeting focused on challenges related to prepaid products, mobile wallets, and payments security.

---

[27] See http://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf.
[28] "Deceptive" refers to omissions of material fact, or misrepresentations.
[29] The FTC is primarily concerned with whether or not the consumer has the opportunity to make a choice, particularly when considering privacy.
[30] The FTC held a workshop in June 2013 on mobile security, *Mobile Security – Potential Threats and Solutions*.
[31] Cramming occurs when a consumer receives unsolicited text messages for digital information, e.g., horoscopes, celebrity trivia, etc., resulting in multiple charges to a consumer's mobile phone bill.
[32] For more information, see http://www.mediapost.com/publications/article/217470/apple-to-refund-325-million-for-kids-in-app-pur.html.

A. Barriers to Offering Prepaid Accounts

Banks and money service businesses have had to comply with CIP (Customer Identification Program) rules[33] to identify and verify all customers using prepaid as an access device since 2012. This applies to any provider or seller of prepaid and to any kind of customer. Companies employ multiple methods to comply with the CIP rules. Compliance with CIP rules for the underserved, or those who are not currently part the banking system, may be more challenging and require more work (and therefore more cost) than compliance for those customers who are already banked. Therefore, the decision of whether or not an FI (or money service provider) chooses to offer prepaid products specifically aimed at the underserved would likely incorporate this cost of doing business into their business case analysis.

Leveraging the Treasury Direct Express prepaid account is somewhat limited. Because Treasury is the sole source issuer for the Direct Express prepaid account, only Treasury can reload it. This prevents the account from being funded from any open, general purpose credit or debit sources, restricting its ability to serve as a true mobile wallet, although Direct Express plans to offer a mobile app in 2015.[34] Solution providers asked if Treasury could expand the range of options or features available through the Treasury prepaid account. One barrier is that Treasury is required by Congress to offer Direct Express accounts to unbanked federal benefit recipients at a reasonable cost. Allowing outside funding sources could make the program more costly to administer, as well as more complex for recipients who may not have experience managing a bank account or may have had a bad experience in the past.[35]

B. Mobile Wallets

Recent years have witnessed a proliferation of self-defined mobile wallet solutions in the market. The expanse of solutions raises the question as to whether the industry needs a set of wallet standards, including a mutually agreed upon definition of what comprises a mobile wallet and a standard security framework that coordinates shared requirements of multiple wallet business models that may co-exist. Not understanding what comprises a mobile wallet and how to use it securely is hindering adoption. Participants agreed that industry stakeholders, not regulators, should determine how the wallet should work and explain why it is compliant, based on security requirements, guiding principles, and best practices they develop. Regulators want to apply "principles-based management" to mobile wallet

[33] Under the USA Patriot Act, all financial institutions must verify the identity of individuals wishing to conduct financial transactions. The law requires financial institutions to develop a **Customer Identification Program** (CIP) appropriate to the size and type of its business. The CIP must be incorporated into the bank's Bank Secrecy Act/Anti-money laundering compliance program. For more information, see http://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_011.htm.

[34] It should be noted that state and local government offices also disperse funds using prepaid cards and many issuers of the smaller programs offer mobile-friendly services like mobile text and mobile bill-pay.

[35] Also, 53% of Direct Express cardholders are Supplemental Security Income (SSI) recipients. The SSI program has asset limitations which could make recipients reluctant to add outside funds for fear of losing eligibility.

solutions and plan to increase their understanding of the various mobile wallets and evolving technologies by meeting with the respective companies.

C. Payments Security: EMV and Tokenization

Security continues to be an important topic for all participants, who discussed several security approaches, including EMV, authentication, and tokenization.

Some regulators asked why adoption of EMV has been slow in the U.S. compared to other countries. Each industry group has had to address different challenges, which were not easy to coordinate across the payment system. For example, financial institutions had to decide whether to invest in performing massive card reissuance programs to convert customers to EMV, or convert more slowly, starting with international travelers and handling other cards as they expired. While some larger merchants had already made the investment to implement EMV-capable POS terminals as part of planned terminal upgrades, others still had to factor the cost of terminal upgrades into their plans. The Reg. II debit card transaction requirements for dual routing further complicated EMV adoption because without an open chip card standard, the card brands had their own common AID (application identifiers) for chips to handle dual routing. However, once the card brands made their common AIDs available, activity continued. Lastly, adoption of EMV is still a choice that each payment stakeholder needs to make. Aside from the card networks' mandate to implement EMV or risk the liability shift that will begin in October 2015, it is up to individual organizations to decide if and how much of that risk they want to take as they plan their migrations to EMV. Until the majority of payment industry stakeholders are fully EMV-ready, the U.S. cannot achieve the full benefits that EMV offers for card present fraud.

EMV benefits include enhanced security through dynamic card authentication, cardholder verification, and transaction authorization for card present transactions. However, some MPIW participants noted that EMV by itself only addresses some steps in a card/mobile payment transaction and should be considered part of a multi-layered approach to end-to-end payment security.

When other countries, such as the United Kingdom and France, adopted EMV for card present transactions, fraud shifted to card-not-present (CNP) online commerce. There was also concern that fraud would travel cross-border to the U.S. where EMV was not yet implemented. Early EMV adopters had to back-track to address CNP fraud, but despite concerns that the U.S. could experience a similar shift, participants commented that the U.S. payments industry has an opportunity to learn from other experiences and begin now to implement preventative measures, such as tokenization.

The tokenization concept has been around for years, but interest in applying it as a security solution has recently increased with the growth of mobile and cloud-based technology payments. Basically, tokenization uses random, digital characters to replace the primary account number (PAN) and other payment account credentials. Tokenization supports a multi-layered approach to payment security by removing sensitive payment account information from parts of the transaction flow and removing responsibility for storing and transmitting the data from the merchants. Tokenization also benefits merchants by minimizing compliance requirements with the Payment Card Industry Security Standards Council Data Security Standard (PCI SSC-DSS).[36]

D. Regulation E Considerations for Mobile Payments

Participants asked the regulators for an explanation of the definition of an "access device" under Reg. E and the requirement for paper receipts.

The ambiguity exists around what constitutes an access device in the context of mobile/digital wallets, where a non-bank initiates the payment transaction but does not hold or own the cardholder's account being debited (i.e., decoupled debit). Reg. E defines the access device as something used to initiate debit card transactions processed over existing payment card networks, such as a contactless device that may be a physical card or included and accessed through a mobile phone. In the example of the decoupled debit mobile transaction, Reg. E would apply.

The group also asked the regulators to consider addressing current paper receipt requirements for POS transactions under Reg. E, which requires receipts for all transactions over $15 be made available at the time the transaction occurs. Are there acceptable mobile or electronic mail methods to deliver POS transaction receipts that still fulfill Reg. E requirements, despite not being physical, paper receipts? The CFPB indicated that Project Catalyst participants are currently discussing this issue and evaluating the constraints under the Electronic Signatures in Global and National Commerce Act (E-SIGN) Act.[37]

V. Agency Coordination and Cooperation

All the banking agencies participate in joint efforts to update guidance. The Federal Financial Institution Examination Council (FFIEC) is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the FR Board, FDIC,

[36]The PCI Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards, including the Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) requirements. For more information, see https://www.pcisecuritystandards.org.

[37] For more information, see http://www.gpo.gov/fdsys/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf.

NCUA, OCC, and CFPB, and to make recommendations to promote uniformity in the supervision of financial institutions. The CSBS is also represented through the State Liaison Committee.

All of the bank agencies are represented on the Treasury interagency group that is looking at emerging payments. Some also participate on international groups that look at payments, including: the International Organization of Securities Commission (IOSCO) and Basel.[38] FinCEN facilitates the International Financial Action Task Force (FATF) and leads ongoing discussions and work on new payment methods, although the focus of the FATF is AML/CFT.[39]

VI. Conclusion

The focus of the regulatory agencies related to mobile payments has not changed much since the initial meeting in April 2012. The agencies continue to support the need for consumer protection, the security and efficiency of the payments system, data security and privacy, and accessibility. Government agencies also recognize the potential for mobile to enhance financial services, particularly for the underserved population. To this end, the agencies continue to monitor new non-bank developments in this evolving ecosystem and collect and analyze information from the industry, with the help of surveys and other sources.

The industry and regulators are still trying to come to a common understanding about the different mobile technology solutions and how they impact the payments system. Progress has been made over the last two years in terms of more interaction between regulators and the industry to better understand the business models and solutions, as well as relevant regulatory requirements and the potential need for new regulations or modification of existing regulations in the mobile payment space.

There is much value to be gained from continued discussions between regulators and industry stakeholders in order to provide a secure and efficient payments system and to ensure secure delivery of value to the market. The MPIW will continue to research and analyze mobile payment initiatives, follow trends and risks, and apprise industry stakeholders, regulatory agencies and other relevant government entities of our findings through meetings, whitepapers, and briefings.

[38] Basel is a committee within the Bank for International Settlements (BIS). It is the primary global standard-setter for the prudential regulation of banks and provides a forum for cooperation on banking supervisory matters. Its mandate is to strengthen the regulation, supervision, and practices of banks worldwide with the purpose of enhancing financial stability. For more information see http://www.bis.org/bcbs/.

[39] For more information see www.gafi-fatf.org.