FEDERAL RESERVE BANK OF BOSTON™

BRIEF

Mobile Payments Industry Workgroup (MPIW)[1] Leadership from 2010 – 2017: Adapting to a Changing Landscape

November 20, 2017

By Susan Pandy, Ph.D., Director, Payment Strategies

The MPIW was established in 2010 to convene industry experts in the mobile payments ecosystem and has met several times annually since then. The goal of these meetings has been to share information and ideas and to discuss barriers and opportunities in mobile and digital payments. These discussions supported the vision for a long-term U.S. mobile payment ecosystem by assessing business models, regulatory frameworks, and industry standards and guidelines. The MPIW also followed key trends in security and authentication technology, consumer and merchant adoption, and shifts in stakeholder perspectives. Through its meetings, publications, and networking, the MPIW has helped to influence and educate the industry to accelerate the progress towards merchant acceptance and consumer adoption of mobile payments.[2] In the eight years since its inception, the MPIW has witnessed considerable change in the mobile/digital payments landscape that is worth reviewing to illustrate the extensive progress that has occurred and the role that the MPIW has played.[3,4]

Early Years of NFC and QR-Code-Based Mobile Wallets: 2010-2013

Initially, the MPIW focused on challenges and opportunities related to implementation of near-field communication (NFC)[5] technology for retail mobile payments at the point-of-sale (POS). Use of NFC technology for mobile payments was nascent and faced many challenges related to cost, complexity, and ownership in its efforts to garner broad industry support. It required issuers, merchants, and others to embrace new hardware (terminals, mobile devices) and software; and to form new business relationships with non-banks, e.g., mobile network operators (MNOs). Provisioning of payment credentials to a secure element (SE)[6] on the mobile device owned by the MNOs was complex and required the involvement of a trusted service manager (TSM).[7] Softcard[8] and Google Wallet were early examples of NFC-based mobile wallets. Softcard was owned by three of four largest MNOs in the U.S.

In 2011, the use of QR codes emerged as another platform to support mobile payments at the POS with solutions from Starbucks, PayPal, LevelUp, and others. QR code mobile app payment solutions were less

[1] The MPIW was created by the Federal Reserve Bank of Boston Payment Strategies group and the Federal Reserve Bank of Atlanta Retail Payments Risk Forum. For more information, see http://www.bostonfed.org/bankinfo/payment-strategies/index.htm.
[2] See Appendix C for a list of MPIW publications from -2017.
[3] See Appendix A for an illustration of the evolution of the mobile/digital payments landscape from 2006 to 2017.
[4] See Appendix B for a comparison of MPIW guiding principles in 2012 versus 2017.
[5] 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.
[6] A secure element is a tamper resistant microcontroller capable of securely hosting applications and their confidential and cryptographic data (e.g. key management) in accordance with the rules and security requirements established by trusted authorities.
[7] A trusted service manager (TSM) acts as a neutral broker that sets up business agreements and technical connections with mobile network operators, phone manufacturers or other entities controlling the secure element on mobile phones.
[8] Softcard (previously ISIS) was owned by AT&T Mobility, Verizon Wireless, and T-Mobile USA.

costly to implement and enabled merchants to incorporate loyalty and rewards programs, which continue to play an important role in incentivizing consumer mobile payment adoption.[9]

The MPIW followed the trends of NFC and QR code-based mobile wallets throughout the early years and produced whitepapers detailing the use cases and transaction flows, assessment of risk, and overview of the security considerations.

Mobile /Digital Payments: 2014-2017

Starting in 2014, the MPIW began to assess tokenization models for mobile/digital payments as well as the potential vulnerabilities related to card-not-present (CNP) fraud attacks. A pivotal transformation in mobile/digital payments occurred in 2014 with the introduction of the *EMV Payment Tokenization Specification* (EMV spec)[10] and its first implementation with the launch of Apple Pay. At that time, the MPIW organized a special meeting on the topic of tokenization with participation by relevant industry experts. The MPIW then conducted research to understand the various approaches to tokenization in the market – security or acquirer tokenization and payment tokenization.[11] Payment tokenization has been innovative in removing the cardholder's primary account number (PAN) from the end-to-end transaction flow and replacing it with a static token. Issuers are responsible for authenticating cardholders during the NFC "Pay" wallet (Apple Pay, Android Pay, and Samsung Pay) enrollment process before a token is issued to a user's mobile device.

MPIW discussions also highlighted progress with consumer authentication methods including biometrics (e.g., fingerprint, voice, and iris scanning), enhanced smartphone capabilities (e.g., device ID, geolocation, and microphone), behavioral analytics, machine learning, and an enhanced EMVCo 3-Domain Secure protocol (v2.0).[12] This progress has been consistently challenged by more sophisticated fraud threats and attacks. As a result, industry stakeholders have been encouraged to take a multi-layered approach to security. And while multifactor authentication[13] remains important, the industry is shifting towards risk-based authentication[14] models that can leverage large amounts of data to enhance fraud analytics and risk-based decision-making. Additionally, merchants realized they needed to manage fraud from their e-commerce and m-commerce channels separately.

The release of the 3DS 2.0 specification in October 2016 was an important development to mitigate CNP fraud by offering several improvements over 3DS 1.0 to help reduce fraudulent transactions. 3DS 2.0 supports app-based authentication and integration with digital wallets, incorporates contextual data

[9] For more information on loyalty and mobile payment adoption, see Tavilla, E. (2017, April 6). *Rewarding Loyal Customers to Increase Mobile Payments Adoption*. Available at https://www.bostonfed.org/publications/payment-strategies/rewarding-loyal-customers-to-increase-mobile-payments-adoption.aspx.

[10] Payment tokenization refers to the process of replacing sensitive payment credential data (i.e., account number) with a surrogate value that has no exploitable value and as outlined in the *EMV Payment Tokenization Specification*. EMVCo (2014, March). *EMV Payment Tokenization Specification – Technical Framework*. Available at http://www.emvco.com/specifications.aspx?id=263.

[11] For more information about tokenization and the difference between security (acquirer/processor) and payment tokenization, see Crowe, M., et. al. (2015, June). *Is Tokenization Ready for Primetime? Perspectives from Industry Stakeholders on the Tokenization Landscape.* Available at http://www.bostonfed.org/bankinfo/payment-strategies/publications/2015/tokenization-prime-time.pdf.

[12] 3-Domain Secure (3DS) is a secure communication protocol used to enable real-time cardholder authentication directly from the card issuer to improve online transaction security and support the growth of e-commerce payments.

[13] Multifactor authentication requires more than one method of consumer authentication to verify the user's identity for a login or other transactions, such as something the user knows (password), something the user has (security token), and something the user is (biometric verification).

[14] Risk-based authentication (RBA) examines contextual information to verify the consumer's identity (e.g., IP address, geolocation), which device is being used (e.g., device type), and whether or not the user's behavior is consistent (e.g., login frequency and attempts).

elements and risk-based decision-making, and supports payment tokenization. Enrollment was a pain point with 3DS 1.0, which required the customer to enroll during the purchase process, interrupting the shopping experience and leading to high rates of shopping cart abandonment.[15] With 3DS 2.0, customers do not need to enroll.

The concerns related to fraud shifting to CNP payments with the migration to EMV chip at POS prompted the MPIW to conduct an analysis of several mobile CNP payment models and associated risks and mitigations, resulting in a whitepaper published in 2016: "*Getting Ahead of the Curve: Assessing Card-Not-Present Fraud in the Mobile Payments Environment*."

The growth of smartphone adoption in the U.S. has positively impacted mobile/digital wallet adoption and the expansion of solutions. U.S. smartphone adoption was approximately 20 percent in 2010 and grew to 81 percent at the end of 2016, according to comScore.[16]

U.S. e-commerce sales as a percentage of total retail sales grew from 5.9 percent in 2013 to 8.5 percent in 2017, supported by increased opportunities to use mobile phones to make online purchases. M-commerce as percentage of e-commerce grew from 12 percent in 2011 to 21 percent in 2017. While overall U.S. consumer mobile payment volume is relatively low, it increases each year. According to a 2016 Pew Charitable Trusts survey, 46 percent of U.S. consumers reported making a mobile payment.[17] Consumer security concerns and uncertainty of value using mobile for payments is limiting growth, but as stronger authentication and other security tools are implemented and merchant acceptance expands, consumer comfort levels are expected to follow suit.

Summary of Key Industry Changes: 2010-2017

Over the last eight years, MPIW members have supported key changes that helped shape the evolution of mobile/digital payments, as discussed below.

- ***Increased smartphone adoption***: High adoption of smartphones, coupled with the rise in m-commerce transactions, reflects the increasing comfort level among consumers to use mobile/digital payments and wallets. Purchasing a smartphone is the most common catalyst cited for adoption of mobile payments technology. While millennials and Generation Xers are more likely than older generations to own smartphones, results show that owning a smartphone is approaching ubiquity.

- ***NFC technology platforms***: It is interesting to note that the payments industry has come full circle since 2010-2011 when there was an initial focus on the promise of NFC technology followed by a slowdown with this technology because of its complexity and cost, only to come back to it in 2014 with the launch of the Pay wallets. The emergence of host card emulation (HCE)[18] as an alternative to reliance on the SE in the mobile device also helped to legitimize NFC for mobile payments.

[15] For more information about 3DS 2.0, see Pandy, S. (2017). *Why 3-Domain Secure should be adopted in the U.S*. Available at https://www.bostonfed.org/publications/payment-strategies/why-3-domain-secure-should-be-adopted-in-the-us.aspx.

[16] comScore (2017). *The 2016 U.S. mobile app report*. Retrieved from https://www.comscore.com/Insights/Presentations-and-Whitepapers/2016/The-2016-US-Mobile-App-Report.

[17] The Pew Charitable Trusts. (2017). *Who uses mobile payments? Survey findings on consumer opinions, experiences*. Retrieved from http://www.pewtrusts.org/~/media/assets/2016/05/who_uses_mobile_payments.pdf.

[18] Host card emulation (HCE) allows NFC card emulation without using the secure element (SE) in mobile handsets by enabling NFC card emulation communications to be routed through the mobile phone's host processor versus from the POS terminal through the NFC controller to the SE. For

- ***QR code technology platforms***: QR codes provide an alternative mobile payment option to NFC for merchants and consumers, are less complex and relatively inexpensive to implement, and are more familiar among consumers to adopt. However, the QR code platforms that merchants, financial institutions (FIs) and technology providers are developing tend to be closed-loop.

- ***Enhanced mobile device capabilities***: Smartphone manufacturers continue to expand the key functionalities of the mobile device, e.g., adding fingerprint sensor to enable biometric authentication, camera for barcode scanning, facial or iris recognition for authentication, geolocation, etc.

- ***EMV chip card migration***: The migration to EMV chip cards at the POS has shifted the industry's attention toward securing the CNP environment. Furthermore, it has prompted more acceptance of NFC Pay wallets at the POS for those merchants that have activated the contactless feature on the EMV-enabled terminals.

- ***Enhanced authentication, payment tokenization, and industry security posture***: New and innovative approaches to authentication are addressing consumer concerns about security and also supporting industry stakeholders (e.g., issuers and merchants) in their efforts to mitigate fraud and enhance the consumer transaction experience.

- ***Increased e-commerce and m-commerce transaction volume***. Payments are no longer solely focused on the POS environment. Research shows that consumers are using their smartphones more to pay for m-commerce purchases via mobile app or mobile browser than they are for POS purchases. The introduction of wallets that can be used at POS, in-app, and online have made this possible.

- ***Omni-channel consumer experience:*** Consumers have come to expect an omni-channel experience – to shop in one channel and place an order in another, or to order merchandise online and to pick it up in the store.

- ***Engagement with regulators***. The MPIW meets every two years with financial institution and other relevant regulatory agencies to exchange ideas and share information about developments in the mobile payments industry. These meetings between industry stakeholders and regulators provides a unique opportunity for MPIW members to inform and educate regulators on key industry trends, security considerations, technology platforms, and solutions.

2018 and Beyond

Roles in the emerging payments ecosystem are changing. Traditional industry stakeholders (e.g., financial institutions) have realized that success in the mobile/digital payments environment requires collaboration and partnerships with non-banks, including card networks, processors, merchants and fintechs. The MNOs that played a significant role in the development of NFC mobile wallets several years ago are no longer active, but the technology giants have in some cases filled the gap. Amazon, PayPal, Google, and Apple are established technology companies that have begun to compete in the payments industry by offering

more information on HCE, see Crowe, M. and Pandy, S. (2016). *Understanding the role of host card emulation in mobile wallets*. Available at https://www.bostonfed.org/publications/payment-strategies/understanding-the-role-of-host-card-emulation-in-mobile-wallets.aspx.

their own solutions and collaborating with card networks, merchants, and FIs to provide better and more secure consumer experiences.

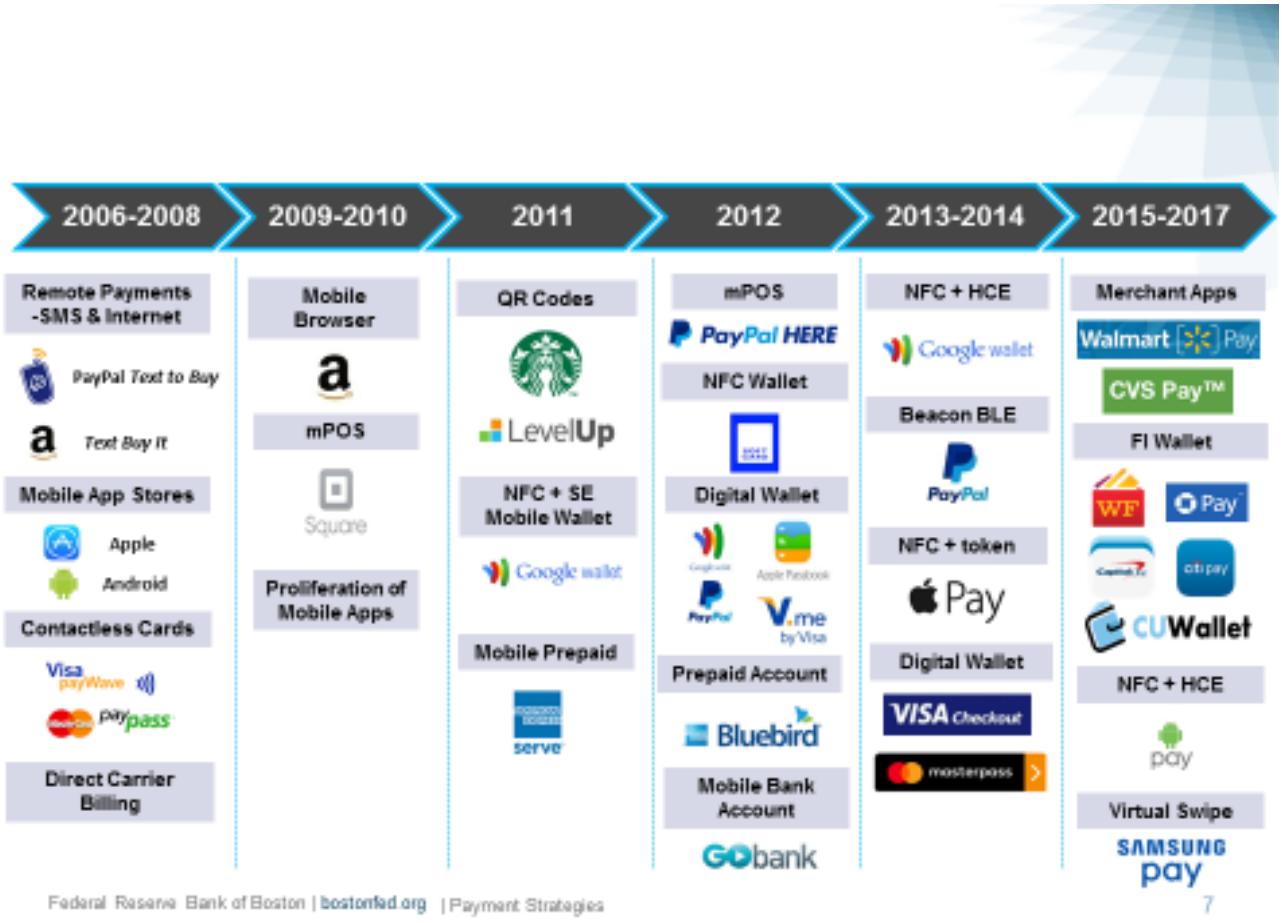
Stakeholders are eager to enhance the consumer experience and to support stronger engagement while reducing friction in the payments process. They need to work together to address the challenges related to making mobile payments a habitual behavior among consumers for daily activities, (e.g., transportation, parking, coffee, lunch, etc.). These challenges include market confusion with many solutions, solutions that are non-standardized, and limited merchant acceptance.

The industry and the MPIW will continue to examine how different technologies (e.g., NFC or QR codes) will drive consumer mobile wallet adoption. QR codes have been particularly successful and pervasive in developing countries, such as China, India, and South Africa. However, QR codes cannot be used in a multi-channel environment and do not offer the same security afforded by NFC. It is equally important to monitor innovative technology solutions that can be used to make payments, making what constitutes "mobile" even broader (e.g., the Internet of Things (IoT), connected devices, and wearables).

As a collaborative forum, the MPIW will continue to play an important role in identifying and understanding the changes in the emerging payments technology environment and share information and ideas about how to make the ecosystem more efficient, secure, and interoperable. At the same time, the MPIW will continue to provide industry education through whitepapers, presentations, and raising important issues with stakeholders. However, it would be helpful to expand the reach of our presentations to other forums and to engage more MPIW members to partner with us in these educational efforts.

The MPIW has proven that its value with early identification of industry pain points and issues that are important to its members. Input from MPIW members allows us to drive an agenda for the group and support its future direction. In doing so, we are able to adapt to the needs of the mobile payments industry by relying on the expertise of our members.

Appendix A: Mobile/Digital Payment Evolution 2006 - 2017



Appendix B: 2011 MPIW Principles v. 2016 MPIW Principles

	2011 MPIW Principles	2016 MPIW Principles
1	The proposed environment is best defined by the concept of an "open mobile wallet."	Open wallet concept includes both mobile and digital mobile wallets.
2	The mobile infrastructure would likely be based on NFC contactless technology resident in a smart phone and merchant terminals.	Convergence of multiple technology platforms for mobile payments.
3	Ubiquitous platforms for mobile should leverage existing rails, including ACH for non-card payments, and support new payment types that meet emerging needs.	Establish ubiquitous platform for existing and new clearing and settlement rails.
4	Some form of dynamic data authentication would be at the heart of a layered mobile payments security and fraud mitigation program.	Dynamic data authentication provides long-term integrity and security for transactions across all channels.
5	Standards would be designed, adopted, and complied with through an industry certification program to ensure both domestic/global interoperability, including a standard to ensure that devices used to facilitate mobile payments do not create any electronic interference problems.	Develop and adopt a global interoperable platform in the U.S. for mobile payment standards and certification of payment methods.
6	A better understanding of a regulatory oversight model should be developed in concert with bank and non-bank regulators early in the effort to clarify compliance responsibilities.	Ongoing dialogue with U.S. regulatory agencies to inform them about current developments, potential issues and future trends in the mobile payments industry.
7	Trusted Service Managers should oversee the provision of interoperable and shared security elements used in the mobile phone.	Neutral TSMs and TSPs to oversee provision of shared secure elements or tokens used in the mobile phone.
8		Understanding the role of nonbanks in the mobile payments ecosystem.

Appendix C: Payment Strategies/MPIW Publications

Date	Publication
Oct 2017	Multi-faceted Evolution of Mobile Payment Strategy, Authentication, and Technology
June 2017	Adapting to Mobile Wallets: The Consumer Experience
May 2017	What's New with Regulation in the Mobile Payment and Fintech Space?
Apr 2017	How Mobile Technology is Driving Innovation and Enhancing Payment Security
Apr 2017	Rewarding Loyal Customers to Increase Mobile Payments Adoption
Mar 2017	Boston Fed Team Puts Mobile Payments to the Test
Mar 2017	2016 Mobile Banking and Payment Survey of New England Financial Institutions
Jan 2017	Why 3-Domain Secure should be adopted in the U.S.
Nov 2016	Getting Ahead of the Curve: Assessing Card-Not-Present Fraud in the Mobile Payments Environment
Jul 2016	Impacts of EMV Migration, Wallets, and Innovation on the Future of Mobile Payments
May 2016	Understanding the Role of Host Card Emulation in Mobile Wallets
May 2016	Commuting Gets a Little Easier with Transit Mobile Payments
Feb 2016	Mitigating Fraud Risk in the Card Not Present Environment
Feb 2016	Mobilizing Consumers to Shop
Oct 2015	A Case Study in Mobile: Paving the Way for Mobile Payments in Thailand
Aug 2015	Mobile Banking and Mobile Payment Practices of U.S. Financial Institutions: Results from 2014 Survey of FIs in Five Federal Reserve Districts
Jul 2015	Current Perspectives on the Mobile Wallet Evolution
Jun 2015	Is Payment Tokenization Ready for Primetime?
May 2015	Mobile Banking in New England is Mainstream: 2014 Mobile Banking and Payments Survey of Financial Institutions in the First District – Summary of Results
Mar 2015	Industry Perspectives on Mobile/Digital Wallets and Channel Convergence
Feb 2015	Transit Mobile Payments: Driving Consumer Experience and Adoption
Nov 2014	2014 Payments Fraud Survey: First District Summary of Results
Nov 2014	Tapping and Zapping Our Way through Boston
Sep 2014	Summary of Mobile Payments Industry Workgroup (MPIW) Meeting Discussion on the U.S. Tokenization Landscape - June 2-3, 2014
Aug 2014	Update on the U.S. Regulatory Landscape for Mobile Payments
May 2014	MPIW Security Workgroup Initiative Progress to Date and Current Status
Jan 2014	Meeting the Needs of Non-Traditional Consumers and Achieving Scale with Mobile Contactless Payments in the U.S.
Nov 2013	Technology and Security Considerations for Mobile Contactless Payments at the Point-of-Sale in the U.S.
Oct 2013	The Future of Mobile Security: Understanding the Risk Environment for Mobile Payments
June 2013	Summary of Mobile Payments Industry Workgroup (MPIW) Meeting with Merchants and Mobile Payment Start-ups, September 25, 2012
May 2013	U.S. Mobile Payments Landscape – Two Years Later
July 2012	The U.S. Regulatory Landscape for Mobile Payments
March 2011	Mobile Payments in the United States: Mapping Out the Road Ahead
Jan 2010	Mobile Payments Industry Roundtable Summary