



**Mobile Payments Industry Workgroup (MPIW)
April 9-10, 2015 Meeting Report**

Current Perspectives on the Mobile Wallet Evolution

**Susan Pandy
Director, Payment Strategies
Federal Reserve Bank of Boston**

July 8, 2015

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

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

Mention or display of a trademark, proprietary product or firm in this report does not constitute an endorsement or criticism by the Federal Reserve Bank of Boston or the Federal Reserve System and does not imply approval to the exclusion of other suitable products or firms.

I. Introduction

The Federal Reserve Banks of Boston and Atlanta¹ convened a meeting of the Mobile Payments Industry Workgroup (MPIW) on April 9-10, 2015 to (1) discuss the impact of Apple Pay on the current mobile wallet landscape; (2) gain insights from small and regional financial institutions (FIs) on their mobile wallet experiences; and (3) receive an update from organizations involved in mobile payment standards. All three panels² covered topics such as the evolution of mobile wallets and payments, the transition to digital payments, and enhanced payments security through tokenization. Central to these discussions was the impact of Apple Pay and the revival of near field communication (NFC) technology for point-of-sale (POS) mobile payments.

II. Mobile Wallet Landscape and the Impact of Apple Pay

The first panel represented MasterCard (MC), Total System Services (TSYS), USA Technologies Inc. (USAT), and Walgreens. The last several years have witnessed the emergence of many companies offering mobile wallet solutions, but with little traction. Apple Pay marks a critical point for revisiting the experiences with those mobile solutions. Panelists, whose companies were early mobile wallet adopters, shared their perspectives on the differences between the earlier mobile wallets and the implementation of Apple Pay.

NFC Revival for Mobile Wallets

Panelists likened the revival of NFC for POS mobile payments to it being in a coma during several years of debate until the launch of Apple Pay – which gave NFC a new life. Apple Pay, coupled with the October 2015 EMV³ chip migration and fraud liability shift timetable, should encourage more merchants to accept NFC mobile payments.

The panelists had experience working with NFC prior to Apple Pay. Over the last five years, MC has conducted one-off deployments of NFC in several European countries and is currently focused on the shift to the digital channel, scalability, consumer choice, and security. TSYS previously processed contactless payment cards in the UK and is now focused on being a mobile wallet enabler. As a payment service provider for small, unattended retail businesses (e.g., vending machines), USAT was an early

¹ Federal Reserve Bank of Boston Payment Strategies and Federal Reserve Bank of Atlanta Payments Risk Forum.

² For more information about the panelists, see Appendix I.

³ EMV (Europay, MasterCard and Visa) 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>.

adopter of NFC for payments and initially deployed NFC for vending machines with Softcard⁴ and now with Apple Pay. Walgreens was also an early adopter of mobile wallets and previously accepted Google Wallet and recently launched Apple Pay. It focuses on enhancing convenience by making it easier for the consumer to shop.

MC views Apple Pay as a platform that offers easy onboarding and secure transactions with payment tokenization – a significant driver for achieving scale. It also plans to support LoopPay⁵ as part of the Samsung Pay wallet, as an opportunity to get consumers accustomed to tapping their phones at the POS.

USAT began implementing Apple Pay in early 2015. It is available on 200,000 vending machines, in addition to 100,000 Coca Cola vending machines.⁶ USAT found NFC easy to integrate into its systems and helpful in migrating customers from cash and coin to electronic/mobile payments. Educating the customer is different in the self-service vending market, so USAT invested in a marketing effort to increase familiarity and drive cashless acceptance. High consumer adoption has resulted in 40 percent of all vending sales being cashless on machines accepting credit and debit cards. Overall vending transaction sales have increased by more than 20 percent with the addition of cashless payments with the average cashless purchase being 34 percent greater than the average cash purchase. In machines where USAT implemented NFC for Apple Pay and other contactless payments, the average Apple Pay or NFC transaction was more than 50 percent higher than the average cash purchase. USAT gained a competitive advantage from implementing Apple Pay and is viewed as an innovator in changing the consumer's perception of vending.

When Walgreens first accepted Google Wallet, there was not enough volume to reinforce and sustain staff training. On the other hand, Apple Pay drove a big spike in mobile payment use. Although Apple Pay has received positive feedback via social media, Walgreens believes there is room for Apple Pay to improve, particularly for integrating loyalty.⁷ Consumers do not want to pull out their mobile phone and a separate loyalty card; reinforcing the need for an integrated omni-channel experience. Despite the

⁴ Google acquired Softcard in February 2015 and shut it down on March 31, 2015. For details on the Softcard Mobile Wallet, see Federal Reserve Bank of Boston. (2014, May). *MPIW Security Workgroup Initiative Progress to Date and Current Status*. Available at <http://www.bostonfed.org/bankinfo/payment-strategies/publications/2014/mpiw-security-progress-status.pdf>.

⁵ LoopPay offers a bridge technology called Magnetic Secure Transmission™ (MST) for accepting mobile contactless payments without NFC. For more information on MST technology, see Boden, R. (2015, March 1). MasterCard discusses how Samsung Pay works, *NFC World*. Retrieved from <http://www.nfcworld.com/2015/03/01/334390/mastercard-discusses-how-samsung-pay-works/>.

⁶ Galarza, D. (2015, March 9). Apple Pay is coming to 100,000 Coke machines, *Eater*. Retrieved from <http://www.eater.com/2015/3/9/8176601/apple-pay-100000-coke-machines> and Ha, A. (2015, March 9). Apple Pay now accepted in nearly 700K locations, *Tech Crunch*. Retrieved from <http://techcrunch.com/2015/03/09/apple-pay-stats>.

⁷ Apple announced it will add the Walgreens Balance Rewards program to Passbook Wallet this fall. See <https://www.apple.com/pr/library/2015/06/08Apple-Pay-Giving-Shoppers-Even-More-Ways-to-Pay.html>

current lack of integrated loyalty, Walgreens had the advantage as an early adopter of being able to give its customers their first POS retail experience using Apple Pay.

Potential Challenges to Tokenized Payments

Despite Apple Pay's advantages, there are some operational and set-up challenges, particularly for merchants. For example, if a customer returns a purchase that was made with a token instead of the primary account number (PAN) and does not have the receipt, the return and chargeback processes are not necessarily the same and need to be clarified. Furthermore, because many retailer loyalty programs are not yet integrated with Apple Pay, it is difficult for retailers and processors to use payment tokens to perform marketing and analytics functions. MC explained that the tokenized transaction can be refunded back to the applicable payment card using its network and TSYS agreed that this was possible.

Merchants face another challenge when a consumer makes a return using a different payment card than the one represented by the token stored in the mobile phone and used for the initial purchase. This scenario does not allow the merchant to lookup the original transaction or payment method and requires another way to recover the token associated with the original transaction. The [*EMV Payment Tokenization Specification – Technical Framework v1.0*](#) (EMV specification) includes a mobile device-specific token that maps back to the original PAN. If a consumer taps the phone initially used at the POS, the card network knows exactly which card was used for the original purchase by matching it to the token stored in the phone. (Each card is assigned a different token within the mobile phone.)

In another return scenario, a consumer (husband) purchased the wrong brand of dog food at a pet store. The wife tried to use a different mobile phone to return the dog food but the retailer could not locate the transaction to refund it since the token in the wife's phone for the same payment card⁸ will be different than the token in the husband's phone. Such scenarios concern merchants because they can lead to poor consumer experiences and negative perception of the merchant's ability to resolve problems. While education for merchants and consumers may help, it is not enough. To address these types of merchant issues, the card networks are working with EMVCo⁹ to develop a standard identifier (i.e., Payment Account Reference number or PAR). Details about the PAR are expected to be included in the next version of the EMV specification, to be released in late 2015 or early 2016. The PAR will identify the

⁸ The husband and wife have a joint account but different tokens and different device IDs.

⁹ EMVCo LLC is a consortium that manages the EMV standard for chip and payment tokenization specifications. It is jointly owned by American Express, Discover, Visa, MasterCard, JCB, and Union Pay.

PAN across Token Requestors,¹⁰ which will allow merchants and acquirers to know the reference to the original PAN.

Fraud and Security Considerations

Panelists also discussed the recent fraud related to Apple Pay with provisioning the payment token associated with the PAN. During the provisioning, the card issuer performs the customer identification and verification (ID&V) process and reviews information such as device data, geo-location, IP address, and address verification prior to loading the token associated with a consumer's card into the mobile phone. Each card issuer has a customized and proprietary approach to ID&V. While there were early problems with ID&V, the card issuers have addressed many of these issues by deploying more controls and to date, there have been no further reports of provisioning fraud.¹¹

A major challenge will be how to support the card-on-file/ecommerce environment with the expected shift in fraud from POS to ecommerce as EMV chip technology is implemented. Tokenizing the mobile and digital data, applying token assurance levels, and working with ecommerce merchants will help to improve legitimate acceptance rates. Token assurance levels, outlined in the EMV specification, assign risk scores to identify the level of risk associated with the token.

Over the next several months, other mobile/digital initiatives are planned. New wallets will launch, including Google Android Pay, Merchant Customer Exchange (MCX)/CurrentC,¹² Samsung Pay, and more in-app payment solutions, particularly in the dining industry for paying at the table with tablets and mobile phones. More POS terminals will be enabled to accept EMV chip cards (and potentially NFC), and more fraud solutions for the online environment will be available.

All these changes enforce the need for better consumer education. For example, tokenization is an abstract concept and should be referred to as “enhanced security.” It will take some time before the mobile and digital solutions are ubiquitous, and in the meantime, consumers will be swiping magnetic strip cards, dipping EMV cards, and tapping contactless cards and mobile phones for payments, making

¹⁰ Under the *EMV Payment Tokenization Specification*, a Token Requestor (TR) is defined as an entity that procures payment tokens from the Token Service Provider (TSP) for completing an actual purchase or payment, and includes the mobile wallet providers, shopping applications, web browsers, card issuers, merchants, acquirers, acquirer processors, payment gateways, and other payment enablers. A TR must register with a TSP and comply with their proprietary requirements, systems, and processes. Once registered, the TR is assigned a TR ID and can then implement the specified Token API. When the process is completed, the TR can request tokens from the TSP to provision to customer mobile devices that contain secure element chips.

¹¹ For more information about Apple Pay and the underlying provisioning and ID&V process, see Federal Reserve Banks of Boston and Atlanta (2015, June). *Is payments 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 For more information about MCX/CurrentC, see <http://www.mcx.com/>.

the potential for confusion a real issue. What is the consumer's appetite and capacity to grasp all the different mobile payment models? How many wallets does a consumer need and how many should a merchant offer? What are the different value propositions offered by the various solutions? These are questions for the industry to consider.

Some MPIW members noted the need for the industry to be more proactive and to collaborate to mitigate fraud through education and information sharing. While the industry is moving in the right direction in terms of enhanced security for payments, no system is perfect and there will always be attempts to break it.

III. Insights from Small and Regional Financial Institutions on Mobile Payments

The second panel included representatives from the Pennsylvania State Employees Credit Union (PSECU), Jack Henry & Associates (JHA), SunTrust Bank (SunTrust), and Georgia United Credit Union (GUCU). They provided the FI perspective on the barriers and benefits of mobile wallet platforms. Panelists shared their participation decisions and experiences with Apple Pay – whether implementation was relatively easy or challenging, any risks, and customer adoption. They also discussed the business model and return on investment (ROI), adoption rates, EMV migration, regional acceptance, and brand impact and the desire to be top of wallet.

Status of Apple Pay Financial Institution Implementations

SunTrust¹³ is responsible for the eastern market from Maryland to Florida and Mississippi with 1,500 branches and three primary lines of business – wholesale, mortgage, and consumer bank. An early adopter, SunTrust was involved within 60 days of learning about Apple Pay. They decided to participate because they saw Apple Pay as an opportunity to test a digital wallet with minimal cost. Since its November 2014 implementation of Apple Pay, SunTrust customer adoption and transaction volumes have been strong – increasing month over month, and customer feedback has been very positive.

Jack Henry & Associates (JHA)¹⁴ is a core payment processor of credit and debit card and ATM transactions. Similar to TSYS, JHA sees its company as an enabler for Apple Pay and other mobile solutions. Issuer clients of JHA have shown a lot of interest in Apple Pay. Currently 16 issuers are live, and over 100 are in the queue. JHA is working with its debit card issuers to address concerns about debit routing options.

¹³ Nathan Meyer is Vice President, Emerging Payments and Apple Pay at SunTrust.

¹⁴ John Postle is General Manager, JHA Payment Processing Solutions at Jack Henry.

Pennsylvania State Employees Credit Union (PSECU)¹⁵ has decided not to deploy Apple Pay at this time but is performing due diligence while watching the market evolve. Because PSECU is a remote delivery operation and has only two branches, its call centers are a big part of its delivery strategy; therefore, management must fully understand the provisioning process and requirements for Apple Pay.

Georgia United Credit Union (GUCU)¹⁶ plans for Apple Pay are similar to those of regional institutions. Since 2009, GUCU has had a mobile platform for account management. GUCU has initiated its plan to offer Apple Pay to its members within the Atlanta area later in 2015 and is currently researching Google Wallet in response to member interest. However, provisioning is a key issue for GUCU to evaluate.

Evaluating Apple Pay

GUCU did not consider ROI when evaluating Apple Pay because they believed the mobile wallet would pay for itself and saw it as a service that would distinguish them from other FIs. Because GUCU has only 17 branches with members spread across the state, Apple Pay provides a new delivery channel; and since the average age of GUCU's current customer base is 49 years old, GUCU wants to use Apple Pay to appeal to a younger demographic. It also believes that its members should decide what FI is top of wallet, based on pricing, rewards, etc. While 38 percent of GUCU members use iOS, the majority use Android; hence, Apple Pay cannot be the only mobile wallet it offers.

Similarly, SunTrust's decision to launch Apple Pay was not based on ROI, which would have been difficult to measure. For SunTrust, the value of Apple Pay was its novelty, the opportunity to be a first adopter in a regional bank market, and to provide additional benefit to its customers. Using MC's turnkey token service, MasterCard Digital Enablement System or MDES,¹⁷ simplified SunTrust's launch of Apple Pay in November 2014. While the provisioning component was a learning process, SunTrust has not received any negative customer feedback. SunTrust added a few extra steps for ID&V to support the Yellow Path¹⁸ authentication process and emphasized that FIs can put controls in place to prevent fraud during the provisioning process (e.g., added controls in call centers, requiring visits to branch, etc.).

¹⁵ Tom Ruback is Chief Operating Officer at PSECU and responsible for transaction services, ACH, call center, ATM, debit and credit at PSECU. Headquartered in Harrisburg, Pennsylvania, PSECU serves over 400,000 members and has over \$4 billion in assets.

¹⁶ Mark Bartholomew is the Chief Information Officer at GUCU.

¹⁷ MDES is currently used for Apple Pay and was launched in September 2014.

¹⁸ When a new card is added to Apple Pay, the card issuer must verify that the individual loading the card is the actual cardholder to prevent an unauthorized user from adding someone's card to another phone. When this verification process requires additional investigation by the card issuer it is called *Yellow Path Authentication* (conversely, when a card is automatically accepted, it is considered "Green Path" and when it is rejected it is "Red Path"). *Yellow Path* authentication was optional for Apple Pay card issuers until a month before the official launch when it became mandated and many card issuers had to quickly assemble support for card-user authentication, which resulted in different levels of *Yellow Path* authentication.

JHA viewed Apple Pay as an opportunity to be innovative and remain relevant in the market. To prepare its client issuers for implementation, JHA obtained certifications from Apple for each client, and facilitated onboarding and enrollment. In the future, JHA plans to make changes to support online maintenance messages so that card issuers can more easily maintain tokens. To prepare its clients to handle their provisioning/authentication responsibilities (e.g., Yellow Path – for validating requests), JHA suggested that its FIs review how they handled customer validation (e.g., to make sure they were not just asking for the last four digits of an SSN). To date, feedback on Apple Pay has been positive.

PSECU took a different approach to evaluating the business case for Apple Pay. For any business case, PSECU evaluates financial and member impacts, as well as the impacts to internal processes and resources, including information technology and marketing components. There are two primary reasons that PSECU has not implemented Apple Pay: (1) it is in the middle of converting its 350,000 card portfolio to EMV; and (2) not enough members have the iPhone 6/6 Plus to support Apple Pay, nor are they asking for it. (Almost one-third of its members use mobile banking, and of those, 60 percent used an Apple iPhone 5 or older model prior to December 2014.) However, the number of members using iPhone 6/6 Plus grew to 35,000 after the holiday season.

Apple Pay Mobile Wallet

As a processor, JHA is trying to work concurrently on Apple Pay and EMV, depending on its clients' needs. Some clients are further ahead with EMV and want to implement it before Apple Pay, while others prefer to launch Apple Pay first. Within FIs, there is a dichotomy between the marketing departments that want to deploy Apple Pay now and the operations/fraud departments that want to deploy EMV first.

Top of wallet was a concern for the FIs. PSECU evaluated the risk of losing top of wallet and not meeting members' expectations of it being a technology company, but concluded top of wallet was not a driver to early adopt Apple Pay, since the top ten largest FIs had already implemented Apple Pay and because they do not compete for credit card transactions. PSECU does not offer credit cards with rewards so they did not expect their credit card to be the default card in the wallet. If it is not going to be the default card, then there is no need to rush to implement Apple Pay.

Like JHA, SunTrust is also working to implement both Apple Pay and EMV. SunTrust is positioning itself in anticipation of more customers using mobile wallets. It expects that the EMV migration will have some impact on mobile wallet growth with increased merchant acceptance of NFC terminals and consumer awareness. After only five months, a significant percentage (30%) of its mobile users have

iPhone 6 mobile devices. SunTrust believes its customers expect the bank to create a good experience for them and that they will make more mobile payments eventually; therefore, it wants to ensure that the SunTrust card is top of wallet.

Most card issuers believe that it is important to be top of wallet because it leads to incremental spend on that card. From the card network perspective, when a card is top of wallet, there is a continued preference by the customer to use that payment method. Some merchants disagree that a mobile wallet leads to higher spending, or that it only applies to low value items. Others see value in the potential for the mobile wallet to displace cash. One quick service restaurant has seen higher spend with mobile transactions because some customers add a food item to their regular coffee purchase.

IV. Update from Organizations Involved in Mobile Payment Standards

The purpose of the third panel was to focus on several standards organizations involved in mobile payments. Panelists representing Groupe Speciale Mobile Association (GSMA), GlobalPlatform (GP) and NFC Forum shared their perspectives on standards developments, particularly for mobile payments. They also explained their various areas of expertise, membership composition, and how the organizations related to one another.

GSMA

GSMA is a trade association that represents the mobile carriers and related companies. It is not a standards organization, but develops public policy for the mobile industry and its customers and works with standards bodies, including GP and NFC Forum. Originally, GSMA focused on roaming agreements for using mobile phones in foreign countries. It now develops requirements and guidelines for digital commerce and identity, and specifications for mobile carriers. GSMA is owned by over 800 members, who must be GSM (SIM card) mobile operators, although it has an associate member classification for the broader mobile ecosystem, with approximately 100 members representing companies such as handset manufacturers, smart card vendors, and industry partners, e.g., EMVCo. GSMA organizes and hosts the Mobile World Congress each year.¹⁹

GlobalPlatform (GP)

GlobalPlatform (GP) is a cross industry, non-profit association with 130 members worldwide. Its goal is to identify, develop, and publish specifications that promote the secure and interoperable deployment and management of multiple applications on secure chip technology. GP operates and standardizes at a

¹⁹ For more information on Mobile World Congress, see <http://www.mobileworldcongress.com/>.

platform level, with a standardized methodology that supports the platform to ensure that it will work with any application that is developed. This allows developers of the platform (e.g., wallet apps) to have assurances that the platform will function as it should. GP did this by creating Application Programming Interfaces (APIs) to be developed in a standard manner.

The GP organization model is an administrative model (i.e., load, manage, compartmentalize). It uses a methodology for specification development similar to the NFC Forum that includes a committee review, member review, and a public review via its website as the final step. It does not move forward with technology until the public review period has ended and all public comments have been addressed by the technical committees and approved by its board of directors. Almost every implementation of GP has a unique service provider layer built on top (e.g., U.S. Department of Defense (DoD) uses GP for its common access card – the DoD built a customized application to meet its needs based on the core GP specification).

GP has deep technical relationships with GSMA and EMVCo, and all of EMVCo's members are members of GP. While GP has no authority to impose a standard on the industry, it has become a *de facto* standards body for smart chip. Unlike GP, EMVCo can mandate and enforce changes related to the use of the networks that the card brands/EMVCo own.

NFC Forum

The NFC Forum is a global standards organization with 175 members. It was formed to advance the use of NFC technology by developing specifications, ensuring interoperability among devices and services, and educating the market about NFC technology. The NFC Forum membership maintains all aspects of the NFC Forum technical specifications. For example, it has released about 15 specifications that address reader-writer mode and other NFC features. With chip manufacturers, it has developed a certification program and other efforts globally to authorize test labs to certify devices for NFC.

NFC Forum has special interest business-centric groups for payments, retail, and transport to evaluate the NFC market requirements. NFC Forum follows a model that is common in the industry with multiple membership tiers where upper tiers gain more rights and obligations. It releases specifications using a formal process with rules of procedure. The common denominator is that each company has the opportunity to influence the outcome based on their investment – through volunteering and time commitment.

The Standards Process

Standards work is often counterintuitive as it involves bringing competitors together to collaborate on technology; however, it is through this process that companies are able to recognize common problems and reach consensus on interoperable solutions. Companies join standards groups to represent their interests and as a standard matures, momentum builds.

EMVCo, NFC Forum, GP, GSMA, and others have written agreements covering how they can exchange documents across their organizations in order to understand something (i.e., technology) ahead of time. The goal is to reduce overlap, contradictions, gaps, and redundancies. This is a great example of how associations work together to identify the core business requirements and then develop the appropriate specifications.

The work done to implement contactless card technology in mobile phones is one example of how working together on specifications and business requirements can reduce complexity and bring NFC-enabled contactless payments to market. Several organizations collaborated to review over 1000 pages of specifications from EMVCo, GSMA, and GP and to reduce the core information to 48 pages. As a result, companies only have to answer three business-oriented questions for how to go to market with a mobile contactless payment application. This type of effort enables developers to cut through the complexity and shorten the development process and time to market from 12-18 months down to 6 months or less. EMVCo and GP often utilize the same test labs where EMVCo performs the security evaluation and GP tests the functionality and performance of the underlying platform.

Collaboration and resource management are critical to the standards process. It is important to understand everyone's expertise and to see what they can focus on to avoid duplication and prevent user organizations from having to test separate specifications. The NFC Forum is looking to collaborate in two areas: (1) end-to-end testing (looking at the full experience), which it is already working on with GSMA and has a certification program (conformance with the specification); and (2) particular industry interoperability challenges. Interoperability is an issue because it affects the consumer experience at a retail location where a consistent experience is needed.

For example, the NFC Forum noted that moving from card to mobile payments represents a big change in terms of operating system platforms. This has created interoperability challenges caused by the rate of innovation and the industry's inability to keep pace (i.e., replacing the mobile phone more frequently and certifying applications to run on multiple handsets). In the past, the certification process for a new mobile device could take up to one year, which was too long given the speed of technology innovation. GP is

introducing a security evaluation process that will shorten the evaluation period to no more than 90 days. GP emphasized that standards organizations do not try to dictate industry winners and losers, but try to deliver agnostic specifications to the market.

V. Conclusion

Several key points emerged from the panel discussions: (1) the entrance of Apple Pay into the mobile wallet market has had a significant, positive impact on the payments landscape; (2) the timing of Apple Pay close to the deadline for EMV migration will further help to drive NFC adoption; (3) the evolution of mobile/digital wallets and payments means different things to various stakeholders – card networks, FIs, merchants, and payment processors; and (4) interoperable standards that support a rapid pace of technological innovation are critical to advancing the industry.

For card networks, Apple Pay and EMV chip and tokenization represent platforms to enable more secure transactions. However, many stakeholders also acknowledge that EMV migration may cause a shift in fraud from POS to ecommerce.

Some merchants see Apple Pay as an opportunity to (1) gain competitive advantage; (2) distinguish themselves as technologically-savvy and innovative to their customers; and (3) migrate customers from cash to electronic or mobile payments. However, merchants recognize that Apple Pay is in its infancy and would benefit from integrating loyalty, which it has plans to do in the near future. Other challenges remain in terms of resolving issues with the return and chargeback processes. It is understood that EMVCo and industry stakeholders are working to resolve some of these issues for merchants.

Small and regional FIs have varying perspectives on the implementation of Apple Pay and future considerations for mobile wallet adoption. The FI panelists generally agreed that Apple Pay (1) presents an opportunity for them to be top of wallet for their customers; (2) is a means to distinguish themselves from other FIs – as early adopters; (3) provides a new delivery channel; and (4) offers an opportunity to appeal to younger customers. Many FIs have wanted to test the use of mobile wallets and Apple Pay provided an opportunity with little risk. Other FIs are trying to juggle both their EMV and mobile/Apple Pay projects. Regardless of whether small

and regional FIs are implementing Apple Pay, many agree that more customers will be using mobile wallets in the future.

Payment processors see Apple Pay as an opportunity to distinguish themselves as innovators and to gain competitive advantage. Most processors want to enable mobile wallets for their FI and merchant clients and – to date – their experiences with Apple Pay have been positive.

Amidst all of this rapid technology change and innovation in the mobile payments industry, open standards organizations play an important role in creating a level playing field for the industry. Through their members, standards organizations fulfill a distinct need in the market by evaluating the business requirements for various technologies. This is done through collaboration and building consensus among industry stakeholders. Standards bodies produce requirements or technical specifications that provide industry stakeholders with a baseline for developing their own customized solutions, reduce complexity, support interoperability, and enable speed to market.

Appendix I – Panelist Organizations

Georgia United Credit Union <https://georgiaunitedcu.org/>

Global Platform <http://www.globalplatform.org/>

Groupe Speciale Mobile Association (GSMA) <http://www.gsma.com/>

Jack Henry & Associates <https://www.jackhenry.com>

MasterCard Worldwide <http://www.mastercard.com/us/company/en/>

NFC Forum <http://nfc-forum.org/>

PSECU <https://www.psecu.com/>

SunTrust <https://www.SunTrust.com/>

Total System Services (TSYS) <http://www.tsys.com/>

USA Technologies, Inc. <https://www.usatech.com/>

Walgreens <http://www.walgreens.com/>