FEDERAL RESERVE BANK OF BOSTON™

BRIEF

MPIW May 2016 Meeting Brief - July 2016

Impacts of EMV[1] Migration, Wallets,[2] and Innovation on the Future of Mobile Payments

By Marianne Crowe, Susan Pandy, and Elisa Tavilla, Payment Strategies, Federal Reserve Bank of Boston

I. Introduction

The goal of the EMV chip card migration in the U.S. was to increase the security of credit and debit cards at the point-of-sale (POS) by reducing counterfeit card fraud. To do so, new EMV payment cards now have an embedded smart chip that can generate dynamic data to create a unique credential for each payment transaction at the POS. The migration was also necessary to provide global interoperability and enable more secure contact and contactless (e.g., mobile) transactions. There has been clear value in the migration to EMV chip cards with a reduction in counterfeit card fraud, but like any new technology, it has created challenges and complexities for payment industry stakeholders, including merchants, processors, and financial institutions (FIs). Timing has been one complexity; exacerbated by the simultaneous introduction of the near-field communications (NFC)[3] contactless mobile wallet solutions (e.g., Apple Pay, Android Pay, Samsung Pay, collectively the "Pays"). Both developments have had significant impacts to industry stakeholders, particularly POS merchants, as they consider their strategic direction for payments.

These developments and challenges in the retail payments ecosystem were the focus of a Mobile Payments Industry Workgroup (MPIW) meeting[4] convened in May 2016. The meeting focused on: (1) merchant perspectives on the POS EMV chip migration and implementation challenges of a contactless NFC platform for mobile wallets; (2) insights into the evolution of mobile wallets from card issuers, processors, and card networks; and (3) perspectives on payment innovation from FIs, processors, and card networks.

II. Merchant Perspectives on Migration to EMV Chip Technology at the POS

As of January 2016, an estimated 37 percent of U.S. merchant locations were EMV chip-ready, with growth expected to reach 72 percent by December 2016.[5] The retail industry comprises a variety of merchants; which

[1] 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. For more information, see http://www.emvco.com.

[2] A mobile wallet is a digital container accessed by a mobile device that allows a consumer to store applications and credentials being used for proximate and remote mobile financial transactions.

[3] Near-field communications (NFC) is a standards-based wireless communication technology that allows data to be exchanged between devices that are a few centimeters apart.

[4] The MPIW is convened 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.

[5] The Strawhecker Group (2016, Feb.) *EMV in the U.S.: The Whole Story.* Available for purchase at http://www.thestrawgroup.com/services/ereports.

The views expressed in this paper are those of the authors and do not necessarily represent those of the Federal Reserve Bank of Boston or the Federal Reserve System.
Mention or display of a trademark, proprietary product or firm 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

range from very large to very small businesses. They have different business models, product offerings, store environments, marketing strategies, and unique payment system needs. For this reason, EMV chip card deployment has posed some different challenges for the merchant community, despite standard testing and certification processes.[6] Given the complexity of EMV chip technology implementation, most large merchants[7] formed dedicated payments teams – a new focus among merchants driven by a rapidly changing payments environment.

Multi-phased Approach to EMV Enablement

The merchant EMV chip migration at retail locations in the U.S. has occurred in three waves: (1) early adopters migrated prior to the October 2015 liability shift; (2) the second group waited until after the busy 2015 holiday season to minimize customer disruption at check-out and allow more time to train employees on the new system and help customers; and (3) the remaining merchants are in various stages of their EMV chip migration plans, including a "wait and see" position. Once the initial EMV chip implementation is completed, there are ongoing improvements to make. Early adopters (typically larger merchants) prioritized meeting the deadline and some postponed certain requirements (e.g., some user functionality) to accomplish this task.

When implementing EMV chip technology, merchants must consider several factors: (1) cost for new POS terminals; (2) order of payment methods (credit vs. debit, signature vs. PIN); (3) which lines of business (LOBs) to upgrade initially, (4) usability testing, (5) POS certification, (6) understanding the impact on speed of service, and (7) need for staff training and consumer education. Because of the complexity, most merchants opt for a multi-phased approach.

Merchants had to make several decisions when planning their EMV implementation strategy, which initially including an assessment of the overall cost to deploy new EMV-enabled terminals. Merchants then had to decide whether to implement credit or debit card first, and whether to include signature and PIN simultaneously or separately, with most implementing signature first and PIN later. Merchants with multiple LOBs (e.g., full- and off-price, online and physical stores, smaller brands), had to decide which LOBs to upgrade to EMV first. Most merchants started with their primary retail locations, with rollout to other LOBs in subsequent phases. Usability testing had to be conducted prior to implementation. Some national retailers worked with issuers to test the in-store user experience; while others enabled EMV chip technology in select locations before rolling it out to all stores. The certification process for EMV-enabled POS terminals was challenging. With only two qualified POS hardware vendors, there were implementation delays.

Merchants strive to provide both a convenient and secure checkout experience for their customers. Merchants, particularly quick-service restaurants (QSR), had to assess the impact of the EMV process on transaction speed. Prior to EMV migration, many QSRs took advantage of network operating rules to suppress signatures for transactions under $50 to speed up the checkout process, but since migrating to EMV have had to disable the

[6] The EMVCo certification process for terminals and software requires level 1 or 2 certification, including security and compatibility tests (each card brand is different). Small merchants with relatively simple setups only have to certify the hardware and software. Large custom setups require level 3 certification with business involvement because it is an end-to-end process that tests every conceivable transaction type (potentially several hundred tests) before approval. For more information about EMV testing and certification, see EMV Migration Forum (2016, April) *EMV Testing and Certification White Paper: Current Global Payment Network Requirements for the U.S. Acquiring Community*. Version 2. Retrieved from http://www.emv-connection.com/downloads/2016/04/EMV_Testing Certification_WP_FINAL_April2016.pdf.

[7] The Payment Card Industry Security Standards Council (PCI SSC) defines Tier 1 merchants as those that process over 6 million transactions per year. For purposes of this whitepaper, we consider these to be "large" merchants.

feature until other software changes can be made. Despite consumer perception and media accounts of slower chip transaction times relative to magnetic stripe cards, most merchant panelists[8] do not think EMV has significantly increased transaction processing time. However, card networks recently announced solutions to improve EMV chip transaction times and facilitate the EMV transition.[9] To address the new EMV card process, which is not uniform across card networks or merchants, staff needed training on how to process an EMV chip transaction, and how to explain the change to customers.

Merchant EMV Implementation Challenges

Merchants in all retail segments (e.g., QSRs, big box retailers) experienced several challenges with EMV implementation: (1) certification issues, (2) franchisee dynamics, (3) POS integration, (4) chargebacks, and (5) fraud.

Certification Issues

As noted above, the limited number of POS hardware vendors created implementation delays for many merchants. Merchants requiring software modifications to EMV terminals worked with their hardware vendors to develop the code, which needed to be tested and certified, adding to delays. Furthermore, merchant panelists asserted that the certification process does not test the actual code; instead it certifies to the "perfect" basic process and does not address special features code. Consequently, a certified terminal does not guarantee that it is ready for actual use. Because some merchants installed their EMV-enabled terminals prior to certification, they could not process EMV chip transactions, leaving them liable for fraud and resulting in chargebacks. The card networks responded to these issues by streamlining testing requirements and simplifying the EMV terminal certification process.[10]

Franchisee Dynamics

Franchisee merchants faced significant resource challenges, needing investment from both corporate and independent small business owners to achieve a cost-effective EMV terminal deployment in all stores. EMV-enabled terminals are expensive and include not only the hardware cost (from $500 to $1,000 per terminal),[11] but additional costs for installation and to modify the terminal for tokenization and encryption. For example, a QSR with 9,000 stores reported having only 7,000 EMV terminals installed to date, noting that at least four terminals are needed per store. This QSR is also looking for ways to implement EMV terminals for its drive-through service, which is available at over 70 percent of its stores.

[8] This does not reflect the views of all merchants in the industry, as some have reported dissatisfaction with the transaction time.

[9] American Express, Discover, MasterCard, and Visa have all released specifications (specs) for "Quick Chip" to increase the speed of EMV chip card transactions by a few seconds. The new specs permit an EMV card to be dipped and withdrawn from a terminal before the transaction is finalized.

[10] Woodward, K. (2016, June 27). Swifter EMV certification will aid chip card transition–and terminal makers. *DigitalTransactions*. Retrieved from http://www.digitaltransactions.net/news/story/Swifter-EMV-Certification-Will-Aid-Chip-Card-Transition_And-Terminal-Maker.

[11] Guldenstern, E. (2016, June 9). How card companies hope to get more merchants on the EMV train, *Credit Union Journal.* Retrieved from http://www.cujournal.com/news/payments/how-card-companies-hope-to-get-more-merchants-on-the-emv-train-1026147-1.html.

POS Integration

Implementing EMV chip terminals is not a simple "out of box" effort, but requires a lot of integration at POS with processors. The process is even more complicated for smaller merchants[12] who may need more POS support to integrate payment methods for special programs such as Supplemental Nutrition Assistance Program (SNAP), Special Supplemental Nutrition Program for Women, Infants and Children (WIC), and other Electronic Benefits Transfer (EBT) cards.

EMV terminals are shipped with default settings, some of which caused problems for merchants. The default display screen on some terminals prompts the consumer to select *Visa Debit* (meaning the transaction would be processed on the Visa network), or *U.S. Debit*, for which the transaction would use the common account identifier (AID)[13] and be routed to one of the U.S. debit networks if it required a PIN. In either case, the terminal first had to determine whether the transaction required a PIN or signature ID. Merchants had three choices: 1) use the existing, default display screen; 2) program the POS terminal to prompt the consumer to choose either credit (signature) or debit (PIN) as their verification method and therefore, override the merchant's application selection on EMV; or 3) program their POS terminal to recognize and route through the common AID, resulting in a prompt for the consumer to enter a PIN. Most merchants worked with their terminal providers and acquirers to make user-friendly changes. However, the changes are not uniform across merchants and the card network rules and specifications are not clear about the screen prompt deployment.

Overall, large and small merchants consider the EMV terminal display default setting as a constraint on merchant choice, driving merchants to make adjustments that better suit their own retail environment and customer needs.

Chargebacks

Many merchants received a high number of chargebacks on their first post-EMV chargeback statements, many of which appeared to be unrelated to EMV and the October 2015 liability shift. Some chargebacks may be caused by system error or friendly fraud.[14] Others may stem from a lack of understanding by the FIs, but it is difficult for the merchants to determine the cause. While all merchants have been impacted, more chargebacks affected those who had not converted from mag-stripe technology to EMV chip cards.

Because of changes to bank operating procedures to reflect the liability shift back to issuers, there has been some confusion in how to handle chargebacks. If FIs reviewing the chargebacks cannot determine the cause (e.g., a counterfeit card (EMV), or a lost or stolen card), they have been charging them back to merchants, even those that are EMV compliant.[15] Merchants that have the time and staff to research their chargeback statements and challenge those they believe are incorrect, have been able to get some of them reversed. Unfortunately, most merchants do not have the time nor detailed knowledge needed to do the

[12] Below $5 million in annual processing.

[13] The Common Debit AIDs allow merchants to select any of the global debit payment networks and U.S. debit payment networks that are enabled on an EMV chip card.

[14] Friendly fraud is when a consumer uses a credit card to make a purchase and then disputes the charge with their credit card company once the item(s) are received.

[15] Heun, D. (2016, March 14). Chargebacks are angering merchants on many fronts. *PaymentsSource*. Retrieved from http://www.paymentssource.com/news/retail-acquiring/emv-chargebacks-are-angering-merchants-on-many-fronts-3023697-1.html.

research. Consequently, even though it appears EMV is reducing POS counterfeit card fraud, it appears that chargebacks have not decreased.

As a temporary solution to this problem, Visa and American Express plan to ease EMV chargeback liability for merchants. Beginning in late summer, they will not allow chargebacks for counterfeit card fraud on transactions under $25; instead issuers will absorb these losses. In addition, starting in October 2016, issuers will be limited to ten fraudulent counterfeit card transactions per card. These liability shift changes will be in effect until April 2018 and are expected to eliminate 40 percent of counterfeit fraud chargebacks and 15 percent of counterfeit fraud losses on Visa cards for merchants nationwide.[16] MasterCard has taken a different approach by updating its network operating rules and making adjustments that will more accurately detect chargebacks that do not meet the network's criteria for merchant liability and minimize the cost to merchants who are not yet EMV compliant.[17]

Fraud

Fraud decreased among EMV-compliant merchants, and increased for merchants that have not yet implemented EMV. Merchants that missed the October 2015 deadline believe that non-compliance made them natural targets for fraud because their goods are sellable (e.g., high-value clothing, home goods, and jewelry). One card network reported an increase in fraud between the October and December 2015 holiday season. However, merchants believe some of this fraud may be attributable to issuers who did not immediately re-issue all of their credit cards after a recent breach.

III. Merchant Perspectives on Contactless EMV, NFC, and Mobile Wallets

Merchants are currently focused on completing their EMV implementations. Enabling NFC mobile payment acceptance at POS is not a high priority for many merchants, even though EMV terminals generally include NFC contactless capability. Some merchant panelists stated that they previously accepted contactless payments but have chosen not to enable NFC in their new EMV POS systems in the absence of a strong business case (i.e., low contactless transaction volume and consumer demand. Also, EMV POS terminals require further modifications to support NFC and consequently, additional testing and certification.

Some merchants are concerned that NFC mobile wallets could pose business challenges to POS integration, access to customer data, and choice of which digital wallets and payment methods to accept. For example, merchants who offer co-branded and private-label cards find it difficult to integrate these payment products and promotional offers (e.g., special financing offers, promotional APR) into the wallets. Merchants may not have visibility into valuable customer transaction data processed through a Pay wallet. Finally, the various mobile wallet solutions offer a range of payment technology methods; however, if merchants accept one NFC wallet, they are required by the card networks to accept all wallets using that same technology.

[16] Visa (2016, June 16). *Visa to Help Accelerate EMV Chip Migration and Support Merchants*. [Press Release]. Retrieved from http://pressreleases.visa.com/phoenix.zhtml?c=215693&p=irol-newsarticlePR&ID=2177933.

[17] For example, MasterCard can stop a chargeback from going back to the merchant for counterfeit contactless chip cards processed on a contactless terminal made for mag-stripe cards if the issuer authorizes the transaction, even though the terminal is not an EMV-capable deviceStewart, J. (2016, June 20). MasterCard joins Visa in easing EMV testing and chargebacks for merchants. *DigitalTransactions*. Retrieved from http://www.digitaltransactions.net/news/story/MasterCard-Joins-Visa-in-Easing-EMV-Testing-And-Chargebacks-for-Merchants.

Although NFC mobile wallets may not be a current priority at POS for some merchants, mobile commerce via mobile web and mobile app is an increasingly important area of focus. Many merchants recognize that fraud will shift to the online card not present (CNP) channel, which requires a more holistic, omnichannel mobile strategy that responds to customer needs and prioritizes online security and fraud prevention. To create an omnichannel experience and address the convergence of in-store, mobile, and online shopping channels, some merchants offer features such as "order online and pick-up in store" or "order ahead and pick-up in store."

Smaller merchants and QSRs have a stronger interest in mobile wallet payments at the POS as well as their drive-through traffic. However, they face challenges in implementing mobile contactless Pay wallets at the drive-through because of terminal placement. Panelists noted that many smaller merchants have modeled their own mobile apps on the Starbucks example, which is based on a prepaid account, rewards, and order-ahead features.

IV. Issuer, Processor, and Card Network Insights into the Mobile Wallet Evolution

Over the last year, several mobile and digital wallet models and solutions have emerged. Wallet providers included technology companies, merchants, and issuers (bank-branded). This landscape has presented challenges and fragmentation in the payments ecosystem. Issuers must re-assess their payment strategies, treating mobile as a new channel with new payment opportunities. They have to evaluate their customer base and which Pay wallets to implement, as well as their organizational needs, costs, and customer demand. Some small banks[18] and credit unions are taking a "wait and see approach" because of limited resources and the need to prioritize EMV chip card issuance to their customers. Medium and larger issuers[19] have more resources to focus on both EMV and mobile wallets, but still struggle with deciding how many Pay solutions to implement.

In building a mobile wallet business case, issuers have to consider customer demand (adoption and actual use) and merchant acceptance. If few merchants accept any of the Pay wallets, then consumers cannot use them. This is a typical chicken and egg problem that could benefit from merchant and issuer efforts to increase customer awareness through consistent signage and messaging, and education about the value and security components of the wallet, as it was noted that the education actually created some customer (consumer and issuer) confusion.

Issuers must also decide whether to make all their cards eligible immediately or selectively offer cards through their wallets, and whether to include loyalty cards and other rewards. The good news is that issuers supporting Apple Pay report a gradual increase in enrollment and usage, as well as positive customer reviews and feedback. Furthermore, there is general consensus among stakeholders that adoption grows as more mobile wallets enter the market.

Payment processors play an instrumental role in supporting their FI clients' business needs and opportunities, in addition to their primary processor role. For issuers with limited resources, payment processors have helped them with mobile wallet and payment tokenization certification, implementation, and education.[20] They have

[18] Less than $500 million in assets.

[19] Greater than $500 million in assets.

[20] 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. For more information about tokenization and the difference between security (acquirer/processor) and payment tokenization (network/issuer), see Crowe,

provided consulting, guidance, and education to help FIs prepare for EMV chip deployment. The card networks also worked through the processors to enable FI mobile wallets. As a result, the processors have found it challenging to manage multiple payment initiatives for their clients and would have preferred to take a staggered approach to implementing EMV chip, mobile wallets, and payment tokenization.

Because the Pay wallets primarily only support mobile payments, issuers have to discover how to drive more interaction with their customers. Issuers are realizing that the digital channel is the first way to communicate with a customer; and therefore, are aligning their digital channels with the Pay wallets. From a consumer adoption perspective, the card networks report increases in overall volume and wallet loyalty, and they see more repeat transactions from users. This behavior is supported by monthly increases in the growth of U.S. consumer mobile wallet use, which makes these customers valuable to card networks, processors, and issuers.

Regardless of the current state of mobile wallet adoption, some panelists expect more wallets to enter the market into the future – from FIs, merchants, and other technology providers (e.g., a grocery chain-branded wallet). Other panelists believe that current mobile wallet adoption is organic because as more consumers discover non-FI based wallets, they will begin using them. In this scenario, consumers will most likely try different wallets as they pick and choose between solutions until they find the combination of wallets that meet their needs. Until there are more ubiquitous wallet solution(s) and broader merchant acceptance, the mobile wallet space will be fragmented. However, some panelists view this as a period of opportunity where FIs can focus on the development of mobile solutions, beyond payments, that will enhance consumer account relationships and ultimately translate into stronger financial returns.

V. Issuer, Processor, and Card Network Perspectives on Payment Innovation

Panelists shared their views on "fintech" companies that use technology to make financial services more efficient. Fintechs have been touted as dis-intermediators by the payments industry, but most stakeholders agree that innovation is at fintech's core and cannot be ignored. Fintech is a means for the payments industry to embrace marketplace disruption and leverage the gains from innovative technology.

Smaller FIs look to the card networks to leverage innovation rather than create it themselves; whereas larger FIs consider innovation a competitive advantage and use their own innovation labs to incubate technology, such as biometrics. Many fintechs work directly with FIs, which must determine what is important and prioritize their opportunities, as well as ensure that the fintech aligns with the FI's mission. Typically, FIs look to consumers to tell them what is important as innovation is becoming a big differentiator.

Processors also have innovation labs where they focus on new technology to support differentiation. Processors strive to solve for existing or future problems through use of innovation. They may also seek technology assets that connect to their existing systems and help to drive value and revenue (e.g., through acquisitions).

Card networks treat innovation somewhat differently from other industry stakeholders. While card networks have innovation labs and engage with non-bank strategic partners, they also have developer centers (e.g., to develop application programming interfaces (APIs)). Fintechs represent a generational shift to the card

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.

networks who have responded by hiring more employees with technology backgrounds and a "Silicon Valley" mindset.

Innovation and Security

Panelists consider Apple a good example of fintech as it was particularly innovative in how it leveraged technology and security (i.e., NFC, payment tokenization, issuer identification and verification (ID&V),[21] and fingerprint authentication) to develop Apple Pay.

Initial Apple Pay rollouts experienced fraudulent payment credentials being provisioned to consumer mobile wallets as a result of weak issuer ID&V used in call centers. Issuers remedied the problem with enhanced token provisioning strategies and stepped-up authentication through the use of one-time passwords (OTPs) or logging in to the issuer's mobile banking app. Lessons learned from the early implementations include: (1) the more information collected about a customer, the stronger the ID&V will be. Processors emphasize the importance of collecting the customer's mobile phone number, which the issuer can use to send an email or text alert to the customer's mobile phone if fraud occurs; and (2) use of dynamic rather than static questions to authenticate the customer during the call center ID&V process. However, the preferred methods of ID&V are moving towards OTP and app-to-app authentication versus the call center.

Issuers have applied innovative ways to authenticate their mobile wallet customers by linking to their mobile banking app, which provides know your customer (KYC)[22] information and history. The issuer can gather additional information through the mobile app to help with verification and risk scoring, such as the age of the mobile phone and the mobile phone number. Some issuers also prefer to provision payment cards to a customer's mobile wallet through the mobile banking app, i.e., push provisioning, although not all issuers have implemented this approach.

Issuers are also exploring the use of third-party databases to support ID&V. For example, some databases contain mobile network operator (MNO) information about the owner of the mobile phone. This data can be used by issuers to provide good customer assurances during the token provisioning process.

VI. Takeaways

- EMV chip migration continues to pose challenges to industry stakeholders but it is gradually moving forward.
- Stakeholders must also focus on strategies to address the anticipated shift in fraud to the online channel, including mobile.
- Many larger merchants are prioritizing their mobile commerce strategy (mobile app and mobile browser) over mobile POS.
- Smaller merchants see more value in mobile wallet adoption at the POS versus EMV chip implementation.

[21] A process through which an entity may successfully validate the cardholder and the cardholder's account in order to establish a confidence level for linking a payment token to the cardholder's PAN. See *EMV Payment Tokenization Specification* http://media.scmagazine.com/documents/95/emvco_payment_tokenisation_spe_23619.pdf.

[22] Know Your Customer (KYC) was mandated by the Bank Secrecy Act and the USA PATRIOT Act of 2003. It requires banks and non-banks to conduct a thorough review of a potential customer before accepting that customer as a new client.

- FIs are evaluating existing and new mobile wallet solutions to determine what is needed to engage the customer, e.g., through loyalty, rewards, and other bank services.
- Some FIs want to wait for the market to mature before they implement mobile wallets.
- The card networks view implementing the Pay wallets as a way for issuers to future-proof their digital strategies.
- Innovation is critical with the pace of technological change and stakeholders must adapt or be dis-intermediated.
- Technology is evolving to secure the mobile channel and address the anticipated increase in online fraud with the introduction of payment tokenization and a new 3-Domain Secure (3DS) specification (2.0)[23] which uses a risk-based authentication model.
- More information-sharing between stakeholders (merchants, issuers, and the mobile wallet solution providers) is needed to improve the ID&V process. Stakeholders are optimistic that agreements can be reached to leverage some of this information in the future to better combat fraud.

[23] 3-D Secure is an XML protocol designed to provide an additional layer of authentication to CNP online transactions, supported by Visa Verified by Visa, MasterCard SecureCode and American Express SafeKey.