Mobile Payments Industry Workgroup (MPIW)
December 3-4, 2014 Meeting Report
Industry Perspectives on Mobile/Digital Wallets and Channel Convergence

Elisa Tavilla
Payment Strategies Industry Specialist
Federal Reserve Bank of Boston

March 2015

The author would like to thank the speakers at the December meeting and the members of the MPIW 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 Boston, the Federal Reserve Bank of Atlanta, or the Federal Reserve System.

I. Introduction

The Federal Reserve Banks of Boston and Atlanta[1] convened a meeting of the Mobile Payments Industry Workgroup (MPIW) on December 3-4, 2014 to discuss (1) different wallet platforms; (2) how card networks and other payment service providers manage risks associated with converging digital and mobile channels; and (3) merchant strategies around building a mobile payment and shopping experience.

Panelists considered how the mobile experience is converging with ecommerce and what new risks are emerging. They discussed how EMV,[2] tokenization,[3] and card-not-present (CNP)[4] will impact mobile/digital wallets and shared their perspectives on how to overcome risk challenges in this environment, whether through tokenization, encryption, or the use of 3D Secure.[5] MPIW members also discussed how various tokenization models can be supported in the digital environment, and the pros and cons of in-app solutions from both a merchant and consumer perspective. With the broad range of technologies available in the marketplace, merchants shared perspectives on how to address the emergence of multiple wallets and the expansion of mobile/digital commerce.

II. POS Wallet Platforms

The first panel included representatives from Paydiant,[6] a white label wallet provider; Softcard,[7] an NFC wallet provider; and USAA Federal Savings Bank (USAA), a financial institution with $125.1 billion in assets.[8] The panelists compared wallet models and approaches to tokenization, consumer experience at the point-of-sale (POS), and prospects for mobile payment adoption and growth.

---

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

[2] 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.

[3] Tokenization is a method for protecting payment card data by substitution of a card's primary account number (PAN) with a unique, randomly generated sequence of numbers, alphanumeric characters or a combination of a truncated PAN and a random alphanumeric sequence, known as a token.

[4] A card-not-present (CNP) transaction is a payment card transaction made where the cardholder does not or cannot physically present the card for a merchant's visual examination at the time that an order is placed and payment effected (e.g., for mail order transactions made via mail, fax, telephone or Internet).

[5] 3D Secure is an XML-based protocol designed to be an additional security layer for online credit and debit card transactions. The basic concept of the protocol is to tie the financial authorization process with an online authentication. This authentication is based on a three-domain model: acquirer domain (the merchant and the bank to which money is being paid); issuer domain (the bank which issued the card being used), and interoperability domain (the infrastructure provided by the card scheme, credit, debit, prepaid or other type of finance card, to support the 3-D Secure protocol).

[6] Paydiant was acquired by PayPal in March 2015.

[7] Softcard was acquired by Google in February 2015.

[8] For more information about the panelists, see Appendix I.

Provisioning and Tokenization across Wallet Models

Paydiant's mobile wallet app integrates with merchant- and bank-branded back-end systems to provide payments, loyalty, offers, and ATM cash access functions. Paydiant's cloud-based platform uses quick response (QR) codes and other mobile technologies, such as near field communication (NFC) and Bluetooth Low Energy (BLE). To enroll, a customer uses his phone to take a picture of his credit card and loads it into the mobile wallet app, or logs into his mobile banking app to add the card.

When Paydiant initially launched its platform, there was no method to tokenize the Primary Account Number (PAN), so it tokenized the transaction. Using Paydiant's mobile wallet and tokenization model, customers scan a Paydiant-generated QR code from the mobile app to pay at the retail POS. The POS system communicates to the Paydiant cloud to request a one-time use, low-value[9] transaction token that represents a unique ID for the purchase. The token includes the merchant name, terminal ID, location, and potentially SKU-level details. Paydiant matches the consumer QR code to the transaction token to capture the real PAN.[10]

Softcard stores payment card credentials in a SIM-based secure element (SE) in the mobile phone for its issuing banks. During enrollment, the Softcard mobile app initiates payment card provisioning but the authentication process is completed through each issuer's respective mobile website.[11] Authentication methods may vary by issuer and are customized and proprietary to each financial institution. Issuers provision real PANs (not tokens), which are stored in the tamper-resistant SE in the mobile phone, but the Card Verification Value (CVV) generated for the transaction is dynamic and similar to a one-time token. One issuer offers a prepaid account through Softcard for which it stores a token in the SE.

USAA implemented Apple Pay in November 2014 and reported strong enrollment. To sign up for Apple Pay, a customer adds his credit or debit card via iTunes or Passbook either manually or by taking a photo of his card with the phone camera. Apple Pay then sends the customer's name, PAN, expiration date, and CVV to the Token Service Provider (TSP),[12] who issues a token in exchange for the PAN.[13] The PAN is stored in the token vault, managed by the TSP, and not in the mobile phone.

---

[9] Per the Payment Card Industry Security Standards Council (PCI SSC) August 2011, *Information Supplement: PCI DSS Tokenization Guidelines*, a "low-value token" is a security token and a "high-value token" exists when "the token itself can be used in lieu of cardholder data to perform a transaction." PCI SSC considers high-value tokens to be payment instruments.

[10] The real PAN is used for backend processing, but eliminated from the transaction flow.

[11] Participating issuers in Softcard include American Express, Chase, and Wells Fargo.

[12] A **Token Service Provider** (TSP) performs several functions: generating, issuing, provisioning, maintaining, and mapping tokens; setting assurance levels; and de-tokenization. Under the current EMVCo, token spec card networks serve as TSPs.

[13] For more information, refer to *EMV Payment Tokenization Specification – Technical Framework* http://www.emvco.com/specifications.aspx?id=263

Consumer Experience and Usability

The panelists considered how offline and online mobile wallet capabilities impact consumer experience and usability. A consumer does not need internet connectivity to use an NFC wallet (e.g. Softcard), which can also operate in battery-off mode. However, the consumer cannot select a payment method or perform authentication if the phone is turned off. Softcard uses a default card to enable payment in battery-off mode, but the issuer decides whether to allow this capability since it assumes the liability. While cloud-based wallets require connectivity and adequate bandwidth, many retailers and other venues have addressed these issues. For example, some sports stadiums, such as the Barclay Center in New York, are equipped with free high-density WiFi and internet access points to ensure an optimized digital experience for fans who want to pay with their mobile wallets.

Creating habituation is critical to fostering broader consumer adoption of mobile payments. However, the panelists agreed that efforts must go beyond payments to give consumers a compelling reason to use their mobile phones for commerce. Consumers are more likely to adopt when they are offered incentives and the brand promotes the payment experience. For example, the Starbucks mobile app shows stars going into a cup to track a customer's progress towards earning rewards. On the other hand, Subway has experienced tremendous growth for its app despite little marketing beyond word-of-mouth. As consumers increasingly use mobile phones throughout their shopping experience (e.g., to receive offers, look up product information, compare prices, and communicate with other consumers), wallet providers can leverage mobile marketing and incentives to encourage retailer app usage.

Mobile Payments Adoption and Growth

It is still too early in the mobile payment evolution for wallet providers to determine the impact of POS or in-app mobile transactions. Based on USAA's observations of Apple Pay, mobile is primarily being used as a cash replacement today, with a relatively small average ticket size. This may be due to the types of merchants and limited number of locations that are currently NFC-enabled. As they measure growth, issuers will need to track not only initial adopters, but also repeat users of Apple Pay.

Quick service restaurants (QSRs) are a rapid growth market for different wallet platforms. Using in-app solutions to order-ahead (e.g., for retail purchases or meals) is expanding. One of the key challenges with mobile ordering/order-ahead is timing, which can be addressed with other mobile technologies. Paydiant uses geo-fencing technology to notify a QSR of a customer's arrival. Some merchants use Bluetooth beacon solutions at drive-thru restaurants. Regardless of the technology and venue, it is important to

ensure a positive customer experience through consumer education and clear messaging on how to use different wallets.

III. Convergence of Mobile and Ecommerce Channels

Panelists from Visa, MasterCard, and Giesecke & Devrient (G&D) discussed how the mobile experience is converging with ecommerce; and the emergence of new threats and risks as these channels become more integrated. The panelists also considered how the migration of cards to the EMV chip may increase CNP fraud in mobile and digital environments, as well as how tokenization, encryption, and 3D Secure tools can help mitigate this risk.

Risk of Data Exposure through Mobile Apps

One key security concern is how to prevent exposing data on the backend of POS systems. Payment solution providers are allowing third parties, some with limited payments experience, to access their technology via application programming interfaces (APIs). It is important to compartmentalize the backend and to control which apps can access the system. Fraudulent apps present the greatest risk, and the platform providers (i.e., app stores) should enforce more stringent app vetting processes. Security for in-app solutions has yet to be fully addressed.

Access and Use of Payment Data

Convergence and growth of mobile and ecommerce creates access to more data, which presents benefits and risks. While more data can help strengthen security, merchants worry that the information may be used for purposes beyond fraud prevention. The policies vary by wallet solution. For example, the card networks do not see individual consumer data about their Apple Pay purchases. They can identify the merchant, and issuers can distinguish between in-app and in-store POS mobile transactions. The card networks only see trends and patterns, such as how many Visa or MasterCard tokens were used at a particular merchant. Issuers have contractual agreements with wallet providers, such as Softcard, specifying the type of data shared and restrictions on its use. Similarly, merchants have agreements with Apple regarding the use of in-app data for Apple Pay.

Ecommerce and Card-Not-Present Fraud

Many ecommerce merchants have developed expertise and proprietary tokenization solutions to manage CNP fraud. The merchants are concerned that newer solutions (e.g., Apple Pay) may change or diminish

the effectiveness of their proprietary tokenization schemes and would like to understand how their schemes will function with other tokenization systems.

In-App Mobile Payments

Panelists discussed in-app mobile payment opportunities introduced by Apple Pay. Many stakeholders believe that in-app solutions will be a big area of growth in the next year. Apple Pay's in-app solution provides more information about the consumer (e.g., the mobile device, merchant location, etc.) than a typical ecommerce transaction and uses the fingerprint to strengthen authentication. For example, using an in-app mobile payment solution at a gas station to activate the pump lowers risk because it can prevent skimming and reduce fraud. Open for discussion is whether the additional information is enough to treat these mobile transactions as card present, which are typically lower risk than CNP.

IV. Merchant Perspectives

MPIW members representing Cumberland Farms and Walmart shared their views on the expansion of mobile and digital commerce and multiple wallets.

In 2012, Cumberland Farms partnered with PayPal to launch a mobile app proof of concept, which generated little volume. When they added ACH with *SmartPay,*[14] an in-app and POS solution using QR codes, adoption accelerated. Implementation required few hardware changes at the pump and POS. The app offers customers a $0.10 per gallon discount and loyalty coupons for in-store purchases with about a 50 percent redemption rate. SmartPay's success was also driven by an aggressive media campaign resulting in over 100,000 customer enrollments in the first 45 days.

SmartPay transactions are authenticated by a payment gateway that communicates with the POS system and the mobile phone. When a customer logs in to his SmartPay account, the transaction goes to the ACH network to verify whether the customer is in good standing. The ACH network then sends a message to activate the pump. The transaction is processed as an offline ACH debit. The $0.10 discount is included in a loyalty field in the confirmation message and adjusted at the pump.

Although the mobile app can geo-locate the customer at a Cumberland Farms location, it cannot identify the pump number, so the customer enters it manually in the app. When the transaction is completed the customer receives an in-app receipt and an email notification. Staff training was not critical because the app is primarily centered on self-pay. SmartPay enables Cumberland Farms to collect and glean

[14] 600 Cumberland Farms gas stations in the northeast now accept SmartPay. For more information on the Cumberland Farms SmartPay mobile app, see http://www.cumberlandfarms.com/SmartPay/Landing.aspx.

information about its customers. The loyalty program is also being used to drive foot traffic into its stores and increase retail revenue.

The SmartPay app has been very successful. While it would be more expensive to implement Apple Pay than the ACH model, Cumberland Farms is considering offering it to customers as a payment choice at the pump given the ease of implementation.

Walmart is focused on providing its customers with a seamless, omni-channel shopping experience, of which mobile is a component. The big box retailer wants a highly secure system that is not dependent on sensitive customer data. It prefers to have any sensitive customer data removed, not only from its system, but from merchant systems in general. Walmart has built features into its mobile app which engage with customers throughout their shopping experience via the mobile channel (e.g., product research, build shopping lists, etc.). The app also provides in-store functionalities, such as product location and description. The retailer wants to keep its customers continuously engaged, so they do not have to switch apps to pay at the POS. Walmart's goal is a solution that is fast, reliable, and scalable, has low-cost transparent fee structures, and does not share customer transaction data. It also seeks a mobile solution that includes Walmart-branded and preferred tender types (e.g., private label cards), allows the merchant to route transactions to preferred networks, and poses minimal impacts to its existing POS system.

While customer interest in mobile payments is still nascent, Walmart wants to be prepared with a solution for future demand. Currently Walmart's staff training is primarily focused on the migration to EMV chip cards. For Walmart, the U.S. EMV POS implementation is complex, particularly with the integration of PIN-debit and government benefits. For example, Electronic Benefit Transfer (EBT) cards, tax codes and tax holidays vary by state.

Both panelists agreed that the top mobile commerce value propositions to consumers are convenience and value. Mobile enhances the shopping experience and helps consumers save time and money. The added security afforded by mobile is also a key benefit.

Conclusion

Three key trends emerged from the panel discussions: (1) the need to accommodate the convergence of payment channels (mobile, physical, and ecommerce); (2) a strong desire among industry stakeholders to provide convenience and value in the mobile/digital payment experience through value-added features beyond payment that will drive adoption by leveraging coupons, loyalty, and rewards; and (3) the need to

reduce payment fraud by removing sensitive payment credentials/account numbers from the payment transaction flow.

Merchants see the potential to increase the appeal and use of consumer mobile payments when offered with a strong value proposition. Financial institutions and merchants can leverage existing customer relationships to foster more seamless, customized experiences as mobile and online channels converge. Greater perceived value by consumers could increase use and strengthen loyalty. More merchants are offering mobile apps and equipping retail venues with the necessary technology to create mobile experiences for their customers.

Industry stakeholders agree that there will continue to be multiple wallet solutions. However, changes to POS systems can be expensive and slow to implement, making it difficult to add new mobile wallets as payment choices. Many also view Apple Pay as a positive development for NFC mobile payments at POS and in-app. They are optimistic about Apple's ability to stimulate the market, to provide enhanced security, and to engage many financial institutions in mobile payments. One merchant noted that its Apple Pay POS implementation seemed to require minimal work, but CNP pricing for in-app solutions remains an issue.

Tokenization can help improve security in ecommerce and mobile transactions (e.g., by removing the real PAN). As multiple tokenization schemes evolve, standardization can help foster compatibility and interoperability. Collaboration across all stakeholders and broad industry education and awareness are critical to success. Additional mobile technologies, such as geo-location, biometrics and BLE, can also be leveraged to provide richer consumer data and reduce risk in the payments system.

Next Steps

The Federal Reserve Banks of Boston and Atlanta will publish a whitepaper on the U.S. tokenization landscape in 2Q 2015. The whitepaper will document and assess the perspectives of mobile payments industry stakeholders regarding challenges and opportunities surrounding payments tokenization initiatives and the role of tokenization in securing the mobile payments ecosystem. It will also identify gaps that need to be resolved and provide recommendations to the industry.

Appendix I – Panelist Organizations

Cumberland Farms www.cumberlandfarms.com

Giesecke & Devrient (G&D) www.gi-de.com

MasterCard www.mastercard.com

Paydiant www.paydiant.com

Softcard www.gosoftcard.com

USAA Federal Savings Bank www.usaa.com

Visa www.visa.com

Walmart www.walmart.com