FEDERAL RESERVE BANK OF BOSTON™

Payment Strategies

REPORT

How Mobile Technology is Driving Innovation and Enhancing Payment Security

MPIW January 2017 Meeting Report April 21, 2017

By Susan Pandy, Ph.D. and Marianne Crowe, Payment Strategies, Federal Reserve Bank of Boston

Consumer adoption and merchant acceptance of mobile payments continues to grow, albeit at a slow pace for a variety of reasons. Some of the challenges and opportunities were explored at the Mobile Payments Industry Workgroup (MPIW) meeting[1] convened in January 2017. The discussions focused on next-generation mobile innovation, with insights from other sectors, e.g., transportation, ATM, and the Internet of Things (IoT), and revisited developments with payment tokenization and the future of authentication related to mobile payments and wallets.

I. Mobile Innovation in Transit, ATM, and the Internet of Things

Mobile technology has been a driver for innovation across many sectors of the financial services industry. This topic covered the role of mobile in the transit, ATM, and wearables/IoT sectors.

Mobile in Transit

Many consumers can now use a mobile app or contactless mobile wallet to pay for their daily commutes with regional U.S. transit authorities.[2] A representative from the New York Metropolitan Transportation Authority (MTA)[3] shared the latest business developments and trends in mobile payments for transit related to the (1) importance of transaction speed at the turnstile, offline authentication, and deployment of contactless-only terminals; and (2) differences of adopting open-loop fare payments compared to closed-loop, proprietary fare payment systems.

Transit operators recognize the benefits of expanding payment options to include mobile apps or contactless technology to enable customers to use near-field communication (NFC)[4] "Pay" wallets[5] to pay

[1] 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.

[2] For more information about the transit mobile payments landscape, see Tavilla, E. (2016, May 18). *Commuting Gets a Little Easier with Transit Mobile Payments*. Available at https://www.bostonfed.org/publications/payment-strategies/commuting-gets-a-little-easier-with-transit-mobile-payments.aspx.

[3] The MTA is a unique U.S. public transit organization because of its size: it commands 25 to 30 percent of that market; and operates bus, subway, commuter rail systems, as well as bridges and tunnels.

[4] Near field communication (NFC) is a standards-based wireless communication technology that allows data to be exchanged between devices that are a few centimeters apart. NFC-enabled mobile phones incorporate a smart chip (secure element) that allows the phone to store the payment app and consumer account information securely and use the information as a virtual payment card.

[5] The MPIW refers to Apple Pay, Android Pay, and Samsung Pay as the "Pay" wallets and groups these wallet models together because they leverage NFC and the secure element chip or NFC and host card emulation technology and also use payment

for transit fares, but speed at a transit turnstile is a much higher priority compared to transaction speed at a retail point-of-sale (POS) terminal. Authorizations for such transactions at turnstiles or on board buses need to be processed faster than the time needed to ensure an issuer's online approval. As such, transit agencies seek to rely on offline transaction authentication capabilities of EMV payment devices to maintain turnstile speed while reducing the risk of counterfeit fraud.[6] There are currently numerous transit agencies around the world that have or are seeking to deploy open payment systems. The MTA is working towards the replacement of its current magnetic stripe MetroCard fare payment system, an initiative planned to include the deployment of 10,000 contactless-only payment terminals.

Transit is a merchant where its customers (commuters) by definition often ride twice a day. This affords transit to present an opportunity for customers to develop a habit of paying with mobile and contactless devices. This habituation can in turn lead to greater use of mobile and contactless at other retailers, including those in areas in and around transit locations. The MTA is optimistic that the broader retail payments industry will continue to recognize the cross-industry benefits of contactless and mobile payment usage in transit. Based on anecdotal data and other information cited by the payments industry, the acceptance of contactless on public transit in the UK market has resulted in an uptick in contactless retail purchases (e.g., customer uses contactless to pay for transit contactless also taps to buy coffee or food during his commute).

The MTA, as well as the other transit agencies, are considering how to migrate from closed loop, traditional payment systems to open loop systems in order to offer more customer payment choices and leverage mainstream retail payment technologies. Many transit systems today are not interoperable across regions, prohibiting transit accounts or cards with one system (e.g., Atlanta) to be used in another (e.g., Boston), requiring customers to carry multiple transit cards if they travel across systems. The ability to use a contactless payment card or mobile device enables retail-like interoperability for transit customers.

Mobile Functionality at the ATM

The ATM channel differs from other payment channels because it is a self-service function. It also operates in financial institutions (FIs), retail, or other locations and can be owned by FIs or by independent non-bank providers. Examining the use of a mobile device in lieu of a physical card for ATM transactions has been a topic of interest for the past couple of years.

Several large FIs and payment processors are in various stages of developing and implementing cardless mobile ATM strategies and use cases. For cash withdrawal, they typically work by associating the customer's mobile phone with his bank account via a digital wallet or app. Some FIs have implemented NFC functionality that enables a customer to load the debit card linked to his bank account into an NFC wallet (e.g., Apple, Android or Samsung Pay). Similar to making a retail purchase, the customer opens the wallet, authenticates with his fingerprint or code, selects the bank debit card, and taps the phone at the contactless symbol on the ATM. The customer then enters his PIN to perform an ATM cash withdrawal. While convenient, interoperability is an issue because the customer can only use this cardless mobile

tokenization as outlined in the *EMV Payment Tokenization Specification*. For more information on the Pay wallets, see Pandy and Crowe (2017). *Choosing a Mobile Wallet: The Consumer Perspective*.

[6] The transaction is authenticated, but not necessarily authorized.

model at ATMs belonging to the FI where his bank account resides (i.e., for on-us transactions). The card networks are working on a possible solution but it is likely 1-2 years away.

Some FIs are developing a different model where the mobile banking app allows the customer to "pre-order" or "stage" a cash withdrawal. The customer requests a one-time, 7- or 8-digit access code (depending on the FI) generated from the mobile banking app or receives a QR code or other token in lieu of an access code. He enters the access code and a PIN or scans the QR code at the ATM to authenticate and withdraw cash. Other FIs allow the mobile phone to be used to unlock and enter some ATM locations as well.

The Payment Alliance International (PAI)[7] is an independent sales organization and ATM deployer, representing over 70,000 independent ATMs in the U.S., that is working on several cardless ATM functions. One use case enables person-to-person (P2P) transfers between ATMs by texting a one-time token/PIN from the sender's mobile phone to the receiver. In a second example, PAI works with advertisers to enable ATM cardless cash redemption for earned mobile loyalty rewards from participating merchants.

Mobile cardless access greatly decreases the potential ATM fraud skimming because the card is bypassed and lowers operation expenses. Customers are also becoming comfortable using Pay wallets, which are secured with tokenization and biometrics. However, without the physical card it is important for FIs and other ATM providers to have other security controls, including customer alerts and limits on ATM withdrawal amounts.

The Internet of Things (IoT)

Many payment industry stakeholders are seeking new venues for mobile payments. One of these new channels is the Internet of Things (IoT), the concept that "everything is connected." Wearables (e.g., rings, watches) are one application of IoT that has already seen numerous pilots. For example, an Apple Watch paired with Apple Wallet can be used to pay at NFC-enabled merchants. The 2016 Olympics in Rio featured a pilot program with an NFC ring paired with Apple Pay for NFC purchases, which could conceivably store multiple payment applications (e.g., credit, debit, etc.).

Other IoT examples include making payments from cars for parking, gas, or food; or from appliances, such as refrigerators. Mobile wallets are moving to dashboards as automakers partner with card networks and retailers to equip vehicles with in-car payment technology. In 2016, Mastercard partnered with General Motors and IBM to bring mobile payments to OnStar systems in GM car dashboards. Similarly, Visa partnered with Honda for an in-vehicle payments system to pay for gas and parking. Amazon and Google are introducing their voice assistants to cars to allow consumers to make purchases from within their vehicles.[8] Mastercard also partnered with Samsung and online grocery retailers to develop an app that enables consumers to order groceries directly from a range of smart refrigerators.

[7] PAI partners with ATM networks and transaction processors and works with its agents and affiliates to place ATMs in retail locations.

[8] Porche, B. (2017, March 2). In-car payments: A wallet that's truly mobile. *Creditcards.com. Retrieved* from http://www.creditcards.com/credit-card-news/in-car-payments-truly-mobile-wallet.php.

While these innovations are exciting, they face challenges and raise some security concerns. Any IoT payment must be secure, efficient and tokenized, which may be a challenge as the financial technology (fintech) start-up companies introducing these innovations tend to be more focused on speed to market and low cost than on security. Achieving the promise of what connected devices/machines can do also requires access to non-payments data (e.g., personal data, geo-location, inventory, etc.) which must have proper constraints and access controls, as well as standards that support the non-payment and payment data. Using wearables for payments represents a shift away from the card as a form factor to an omni-channel future where the methods to pay will grow exponentially, creating the need for the card networks to address how to integrate with thousands of token requestors.[9] Finally, the limited bandwidth capacity needed to support a multitude of devices on a mobile network will also need to be resolved.

II. Payment Tokenization Revisited

Panelists representing a card network, major bank, payment processor, and The Clearing House (TCH),[10] discussed several tokenization developments, including expansion of tokenization to e-commerce, non-network token service providers (TSPs),[11] the use of a payment account reference (PAR) number,[12] alternate primary account numbers (PANs), and ISO 8583[13] transaction message challenges.

In 2014, motivated by EMVCo[14] and TCH initiatives to replace the PAN with a token in mobile payment wallets, the MPIW conducted an analysis of the payments tokenization landscape.[15] Since then, use of payment tokenization for securing card credentials has expanded and is being considered for other payment models, including e-commerce and Automated Clearing House (ACH) transactions. Payment tokenization enables delivery of a static token and dynamic cryptogram to multiple channels and

[9] A token requestor (TR) is an entity that procures payment tokens from a token service provider (TSP) to be used for completing a purchase. TRs include mobile wallet providers, shopping applications, web browsers, card issuers, merchants, acquirers, acquirer processors, payment gateways, and other payment enablers. A TR must register and comply with a TSP's proprietary requirements, systems, and processes. Once registered, the TR receives a Token Requestor ID and implements the specified Token API. The TR is then able to request tokens from the TSP to provision to customer NFC-enabled mobile devices containing secure elements for token storage.

[10] Established in 1853, TCH is the oldest banking association and payments company in the U.S. and is owned by twenty-four of the world's leading commercial banks for which it provides payment, clearing, and settlement services.

[11] The *EMV Payment Tokenization Specification* defines a token service provider as an entity that provides a token service comprised of the token vault and related processing.

[12] For more information on the payment account reference number, see https://www.emvco.com/best_practices.aspx?id=33.

[13] ISO 8583 - Financial transaction card originated messages — Interchange message specifications. This standard specifies a common interface by which financial transaction card-originated messages can be interchanged between acquirers and card issuers.
It specifies message structure, format and content, data elements and values for data elements. For more information, see https://www.iso.org/obp/ui/#iso:std:iso:8583:-1:ed-1:v1:en.

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

[15] EMVCo (2014, March). *EMV Payment Tokenization Specification – Technical Framework, Version 1.0*. Available at http://www.emvco.com/specifications.aspx?id=263. Version 2.0 available in April 2017. For more information about tokenization and the difference between security (acquirer/processor) and payment tokenization (network/issuer), 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.

environments in addition to POS, such as card-on-file (CoF)[16] and cloud, with the ultimate goal of securing the payment system by replacing all PANs.

Tokenization Helps to Drive Consumer Mobile/Digital Wallet Adoption

All panelists are actively involved in payment tokenization efforts and discussed several improvements and changes that are helping to increase the security, adoption, and use of mobile payments. The early problem with the identification and verification (ID&V)[17] process for token provisioning that surfaced when the NFC Pay wallets were launched over two years ago, was quickly addressed and implementation of tokens for POS payments works smoothly. The card networks are now applying the same tokenization controls to mobile in-app and online digital transactions and some have reciprocal agreements to tokenize digital wallet transactions that are processed through each other's digital checkout wallet solutions to support interoperability. Today, not only are consumers more aware of where Pay mobile wallets are accepted at POS and online, they are also informed by their FIs or merchants that the token in their mobile wallet or on a receipt is a secure replacement for their PAN.

To further promote consumer adoption, Android Pay and Samsung Pay have added rewards and loyalty programs to their solutions; while the card networks are marketing new ways to use mobile payments in everyday use cases, e.g., for food delivery or parking.

Payment Tokenization Expansion to Other Use Cases and Channels

The card networks are developing pilots with large merchants to tokenize card-on-file (CoF) e-commerce transactions, with plans to launch commercially in late 2017. Merchants (or their acquirers) will use application programming interfaces (APIs) provided by the card networks to directly connect to the networks and request payment tokens. Processors and payment gateways will be able to integrate with the networks to introduce a one-to-many process for token distribution. Card networks are also working to include more data with the token in the transaction record to help issuers and CoF merchants improve the customer experience.

TCH supports the need for tokens to apply to multiple payment rails, including cards, ACH, and real-time payments. ACH and real-time processes use the same deposit account credential, and TCH wants them to share the same payment token. TCH has to determine how a token that passes through ACH will be converted back to the DDA number to enable the issuer to post the payment. In 2016, TCH shared this project with NACHA as a framework to fit into its rulemaking process. TCH is currently piloting ACH tokenization and reconciling how tokenization will operate across the two ACH operators' (TCH and Federal Reserve Bank) networks so that they can tokenize any transaction that comes over the TCH network.

[16] Card-on-file refers to the authorized storage of a consumer's payment credentials by a merchant, a payment service provider, or a wallet service provider, that allows the consumer to conveniently make repeat or automatic purchases without the need to re-enter payment credentials each time.

[17] Identification and verification is a method through which an entity can validate the cardholder and the cardholder's account (PAN) to establish a confidence level for the payment token to PAN/cardholder binding. Examples of ID&V methods include: account verification message; risk score based on assessment of the PAN; use of one-time password by the card issuer or its agent to verify the cardholder.

Inclusion of Non-Network Token Service Providers (TSPs)

The bar is high to become a non-network TSP because of the responsibility and level of security required. Building the engine for a token vault is very complicated and requires a tightly controlled security environment. Organizations other than card networks may apply to become TSPs and generate tokens if they meet specific requirements described in the *EMV Payment Tokenization Specification* (EMV spec): (1) become certified and register (and pay) with EMVCo; (2) outline what the non-network TSP would be used for (e.g., if cards, need to connect with card networks; (3) integrate with each wallet provider (however, wallet providers are unlikely to be willing to work with a massive number of TSPs because it requires a separate connection be established to each TSP). Card network TSPs ensure security via encryption and dedicated communication lines between parties (no information is transmitted over the internet). Furthermore, access to the token vault (maintained by the card network) is limited and protected by considerable security components.

The key issue is not who creates the tokens, but that tokens created by non-networks must mirror tokens created by the card networks to ensure integrity and consistency in the ecosystem. Merchants must see the exact same format of data, regardless of who generates the token. Because the card networks must tokenize the PANs for all of their issuers, there may be an opportunity for non-networks to partner in the effort to tokenize PANs for other channels, e.g., merchant CoF, digital wallets, e-commerce platforms, etc. TCH plans to launch a TSP service later in 2017 as a non-network based alternative tokenization solution.

Payment Account Reference (PAR) Number

The current payment token structure is one-account-to-many-tokens. This structure disconnects merchants from their customers because they only see the token for a transaction and not the last four digits of the PAN, which they use for customer lookups and other backend processes. Further complicating the token structure are customer purchases made in a different channel, e.g., e-commerce, where a different token may be assigned. Some merchants cannot distinguish between a payment token and a security (acquirer) token, although the acquirer can differentiate because the card networks designate token BIN ranges that include a Token Requestor ID, token assurance value, and extra data elements.

To address the one-to-many token structure, EMVCo introduced the Payment Account Reference (PAR) number.[18] PAR is a unique 29-character non-financial transactional field associated with a specific cardholder PAN. The PAR is static and can be used in place of sensitive consumer identification fields; and transmitted with the transaction message to facilitate consumer identification.

The PAR can support payment tokenization by being included in the transaction message sent to the POS terminal. The POS terminal recognizes the PAR and transmits it to the merchant and acquirer. This allows merchants and acquirers to track and manage accounts across multiple changing tokens without relying on a PAN because the tokens associated with the PAN are all linked to the same PAR.

[18] See EMVCo Special Bulletin 167 – Payment Account Reference, available for download at https://www.emvco.com/specifications.aspx?id=23.

EMVCo has posted an FAQ about PAR on its website[19] and the card networks are working on plans to support PAR, but the ecosystem is still developing the capacity to carry this data field in the transaction message and integrate with card networks. Therefore, PAR implementation remains several years away.

ISO 8583 vs. API Use with Wallet Payments

There was some discussion on the benefits of using APIs versus ISO 8583 to address carrying additional data in the transaction messages for wallet solutions. APIs provide opportunities to break away from the constraints of ISO 8583 in various situations, but there are limitations. The ecosystem for transaction messaging is very complex. There are numerous "handoffs" in the sequential ISO 8583 transaction process. For example, if only one party in the value chain (acquirer, PIN network, card network) upgrades its systems, the message must be translated back to the lowest common denominator, which is the ISO 8583 format.[20] However, stakeholders in the value chain vary in how they populate the fields in the 8583 message. As a result, some data elements are dropped or omitted from the ISO 8583 message and the issuer or merchant receives less information. For example, data for different fraud controls (e.g., wallet service provider ID) may be dropped or the token may be listed in a different field. Complying with the existing EMV spec and using APIs to carry the additional data and improve transaction speed could resolve this problem.

The provisioning process for the Pay wallets already uses APIs and some MPIW members believe that this presents an opportunity to institute more APIs to provide relief from the constraints of ISO 8583.

III. The Future of Authentication

The panelists focused on a few key themes related to authentication: eliminating static authentication data and employing biometrics, risk-based authentication (3DS 2.0), and the role of the mobile network operator (MNO)/mobile device in authentication.

Biometrics

The payments industry has long recognized the need to eliminate static passwords for consumer authentication. The evolution of mobile wallets has reduced reliance on usernames and passwords because most mobile phones are now equipped with fingerprint sensors which enable biometrics to accept fingerprint authentication, as well as a microphone for voice authentication, and a camera for eye vein or facial recognition. Biometrics provides a dynamic, explicit login at the time of authentication. While this is a valuable development in securing mobile transactions, care must be taken to protect consumer privacy and prevent the ability to hack biometric data.

Risk-based Authentication

[19] https://www.emvco.com/faq.aspx?id=310.

[20] There are several versions of ISO-8583 in use in the market: ISO-8583:1987, ISO-8583:1993, and ISO-8583:2003. ISO-8583:1987 is the most widely used version; therefore, even if part of the network has implemented ISO-8583:2003, the transaction message may pass through a node that uses the 1987 version, reducing the entire message to the 1987 version.

Risk-based authentication (RBA) tools leverage valuable customer data to make approval decisions without interrupting most transactions for additional consumer authentication. This reduces customer friction and shopping cart abandonment, making these tools more attractive to merchants and issuers. Also, by allowing more data to be shared for fraud prevention, RBA tools can provide a holistic view that can help identify fraud trends with strong fraud detection rates and low false positives which tend to be a very expensive problem for merchants. Panelists noted that RBA has been shown to reduce call center fraud by over 85 percent.

EMVCo's 3-Domain Secure (3DS)[21] version 2.0 is a risk-based tool used to authenticate the cardholder during the online and mobile transaction process. The panelists had positive feedback on 3DS 2.0. Because it is risk-based, about 95 percent (or more) of a merchant's transactions should pass without a challenge or interruption to the consumer checkout experience, depending on the e-commerce merchant's confidence level (the merchant determines when to invoke 3DS). This allows merchants to focus their fraud management budget on monitoring the 5 percent or less of potentially fraudulent transactions. The key is not only to block the fraudsters but also to improve the online and mobile transaction process for valid customers.

Role of MNO/Mobile Device as Authenticator

The volume of payment transactions originating from mobile devices (via mobile app and mobile browser) is growing. For mobile wallets in particular, the authentication process begins with consumer enrollment of a payment account. This is where the mobile device is bound to the legitimate customer using extensive verification methods. For instance, collecting the device ID is an important part of this process, as well as other information such as email, phone number, and location data (if the consumer opts-in).

Mobile network operators (MNOs) have access to rich data about the mobile device which can be used to enhance the consumer authentication process because it has deep security and authentication controls. MNOs know if the customer is using a different phone or has changed the phone number or name on the account. They can also track and manage this information across mobile devices registered with the MNO. The MNOs also work with third party providers to detect mobile phone spoofing. Once a spoofed phone has been detected, it can be directed to a fraud specialist that can use knowledge-based authentication to question the fraudster.

Building a New Authentication Framework

If a fraudster obtains consumer enrollment data, he can use his own biometric data and the stolen payment credentials to register the account. Therefore, verifying the identity of the consumer is the first point of

[21] 3-Domain Secure (3DS) is a secure communication protocol used to enable real-time cardholder authentication directly from the card issuer during an online transaction to improve online transaction security and support the growth of e-commerce payments. The new 3DS 2.0 specification updates the risk management approach by incorporating risk-based elements and delivering expanded capabilities in terms of technology, security (e.g., tokenization), performance, user experience, and flexibility. Unlike the original version, 3DS 2.0 automatically registers all customers with participating issuers, so consumers do not need to enroll to use the service.

vulnerability. Unless the person has been verified as the legitimate owner of the account, it will not matter what other security methods are applied during the process because the fraudster will have control of the account.

There is no silver bullet to improving authentication. If a company focuses too much on one vulnerability or solution, this only benefits fraudsters as they will seek to exploit other elements. Moreover, it begins with a company's approach to risk management, data analysis, and the ability to leverage multiple layers of security, including the use of tokenization. Some industry experts refer to this as the three pillar approach: authentication, tokenization, and risk management – coupled with the collection of massive customer data. Merchants benefit from operating or having access to robust risk management systems that can learn from the customer transactional data. This means being able to associate customer purchases to a legitimate device or mailing address.

Authentication processes are changing but there are challenges to adopting next-generation authentication tools more broadly. Despite improvements in authentication, there are still concerns related to customer experience, privacy, and the ability for stakeholders to share information to enhance authentication. Regardless of the technological solutions available in the market, the need remains for more collaboration and feedback between merchants and issuers. Currently, this type of feedback loop is not mandated in the industry. However, many experts advocate a need for merchants, processors, and issuers to be able to better communicate about problems with fraud.

IV. Key Findings

1. Tokenization is helping the payments industry to shift away from its reliance on a payment credential to focus more on digital identity. It has value beyond mobile payment use cases and should be expanded to secure payment credentials and other data for applications and verticals such as ATM, ACH, transit, wearables and IoT. Education continues to be needed to help the industry understand how tokenization works, how payment tokenization is different from security tokenization, and how the two approaches can be reconciled.

2. Authentication tools and practices exist to strengthen the security of mobile and digital payments but are not used consistently across industry segments. The general consensus is that authentication needs to start with the enrollment process and there is a need to gather as much information as possible to employ Know Your Customer (KYC)[22] tools at different levels. The definition of KYC is changing in the IoT world with the availability of connected devices that now transact on behalf of the customer. The payment industry should also consider how to better leverage data available from the MNOs, particularly as the mobile device is recognized as an important authentication factor. To effectively use the authentication data and minimize fraud, a formalized feedback loop between the stakeholders in the transaction process – merchant, issuer, and processor – is needed.

[22] Know your customer (KYC) refers to the 2014 requirements proposed by the US Financial Crimes Enforcement Network (FinCEN) to increase the focus on anti-money laundering and terrorism financing (AML). FinCEN's KYC are part of a broader regulation setting out the core elements of a customer due diligence program to help financial institutions avoid illicit transactions by improving their view of their clients' identities and business relationships.

3. Recognize that IoT is closer than we think. While it may seem like this is a slow-motion shift in the industry, it is important for stakeholders to monitor IoT developments and be prepared to handle payments for new form factors as they move to the omni-channel and engage within the open banking API economy. It will also be important to track adoption and understand the security concerns and challenges in a world that expands beyond mobile phones. New innovation partnerships are forming that should be monitored.