FEDERAL RESERVE
BANK OF BOSTON™

REPORT

Multi-faceted Evolution of Mobile Payment Strategy, Authentication, and Technology

MPIW August 2017 Meeting — Summary of Key Findings
October 30, 2017

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

The Mobile Payments Industry Workgroup (MPIW)[1] is comprised of payment stakeholders focused on eliminating barriers to successful adoption of mobile and digital retail payments in the U.S. Consumer adoption and merchant acceptance of mobile payments continue to grow, albeit at a slow pace for several reasons. Some of the challenges and opportunities were explored at the MPIW meeting convened in August 2017, including: (1) consumer mobile wallet adoption trends; (2) mobile payment strategic development; (3) emerging authentication technology; and (4) new technology applications, such as the Internet of Things (IoT) and wearables.[2]

I. Consumer Adoption Trends for Mobile / Digital Wallets

The first panel[3] presented data on mobile/digital wallet consumer adoption trends from two studies. The first was the Federal Reserve Board's *2016 Consumers and Mobile Financial Services Study*.[4] In 2015, 28 percent of smartphone users reported making a mobile payment in the previous 12 months. Among these smartphone users who reported making a mobile payment, the most common payment activities conducted via a mobile browser or mobile app were (ranked in order): paying a bill, purchasing merchandise or digital content, or paying for goods in a store. Of those mobile payment users with smartphones who made in-store payments, 73 percent had done so in the preceding month. Respondents who made mobile payments were asked about their primary reason for adopting the technology. Most common responses included convenience (45 percent), purchase of a smartphone (20 percent), availability and ability to make a mobile payment (14 percent), and comfort with the security of a mobile payment (7 percent).

The Federal Reserve Board study further showed that demographically, younger consumers and minorities[5] were more likely to make mobile payments. Income was not a determinative factor. Some respondents also indicated their interest in using smartphones to receive offers and promotions based on location, receive

[1] The MPIW is convened by the Federal Reserve Banks of Boston and Atlanta. For more information, see http://www.bostonfed.org/bankinfo/payment-strategies/index.htm.

[2] Wearables are smart electronic devices (electronic device with microcontrollers) that can be worn on the body, either as an accessory, e.g., fitness bands, smartwatches, or as part of material used in clothing. One of the major features of wearable technology is its ability to connect to the Internet, enabling data to be exchanged between a network and the device.

[3] Alejandra Lopez-Fernandini, Federal Reserve Board and Jaclyn Holmes, Auriemma Consulting.

[4] U.S. Board of Governors of the Federal Reserve System (2016, March). *2016 Consumers and Mobile Financial Services*. Retrieved from https://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201603.pdf. This survey had been conducted for five consecutive years (2011-2015). For the 2015 survey, the data was collected from November 4-23, 2015 with 2,510 respondents. All data is self-reported from the respondents.

[5] Minority adoption rates have been higher than white, non-Hispanic consumers over time for both mobile banking and mobile payments.

The views expressed in this paper are those of the author 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

and manage discount offers and coupons, and compare prices while shopping. When asked about their willingness to provide information about their smartphones, 40 percent indicated they would share their location to receive location-based offers and 74 percent were willing to answer security questions or provide additional information to enhance transaction security.

Respondents who did not use mobile payments found it easier to use a payment card, had concerns about security, or did not see any benefit to using mobile payments. The primary security concerns included having a phone hacked, interception of data, or a lost or stolen mobile phone.

The second study was Auriemma's Mobile Pay Tracker.[6] It tracks consumers who own eligible near field communication (NFC)[7] mobile devices for the "Pay" wallets (Apple Pay, Android Pay, and Samsung Pay).[8] According to the study, adoption of Apple Pay was 42 percent among eligible respondents when launched in 2015, but has leveled off to approximately 35 percent. Samsung Pay and Android Pay also experienced high adoption with their initial launches,[9] but growth has also slowed over the last 18 months.[10]

Eligible population groups tend to skew toward younger consumers, but are starting to level off as more consumers age 55 and over are purchasing eligible mobile devices. Most respondents are homeowners with incomes of $50K or more, and/or credit card revolvers; a consistent finding throughout the Auriemma study. Users tend to skew towards the affluent, while the Federal Reserve Board study found that income was not a determinative factor. One possible reason for the variation may be that the Federal Reserve Board study does not identify specific types of wallets, while the Mobile Pay Tracker does so for the Pay wallets.

Eighty percent of in-store point-of-sale (POS) users reported using their respective Pay wallet in the previous month. Slightly fewer in-app users (72 percent) reported previous month usage.

Results from the Mobile Pay Tracker showed that incentives are driving more frequent mobile payment usage. However, incentives tend to be more impactful for creating habitual use than encouraging first-time trials. Over half of respondents (56 percent) say they often forget to use their Pay wallet until after they have paid – offering incentives may be an effective way to keep mobile payments top of mind at the POS.

Within the Pay wallet user population, security is not the top barrier. Rather, Pay wallet users report that there are not enough merchant locations that accept Pay wallets. Other deterrents to consistent usage

[6] Mobile Pay Tracker was launched in 2015 and is conducted quarterly. The study examines consumer behaviors and trends impacting mobile payments, specifically, Apple Pay, Android Pay, and Samsung Pay. It surveys 500 Apple Pay eligible participants and 1000 Android Pay eligible participants quarterly, repeating a majority of the metrics for tracking purposes. Samsung Pay is also examined, allowing for a full view of the major players in mobile payments. For more information, see http://www.acg.net/services/payment-insights/mobile-payments-report/.

[7] 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.

[8] 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 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*.

[9] Adoption was 19 percent and 23 percent for Android Pay and Samsung Pay, respectively, and has grown to approximately 26 percent for each.

[10] The survey asks respondents to indicate their wallet preference between Samsung and Android, since Samsung phone owners can use both wallets.

include perceptions that cashiers are unfamiliar with how to process Pay wallets, or seeing a long line at the register. Pay wallet users in the Auriemma study indicated they would use their mobile wallet more if there was greater merchant adoption and if more consumers began to use them.

II. Evolution in Mobile Payment Strategy

According to a 2016 Ovum study, 81 percent of merchants now consider payments a fundamental part of their business strategy, with 92 percent expecting to maintain or increase their investments over the next 12-18 months.[11] The second panel[12] discussed how payments are a fundamental part of their overall business strategies and the evolutionary path they have taken to develop their mobile payment and wallet strategies. They also shared insights into some of the merchant and consumer challenges and the potential for opportunities to collaborate. They noted that payment industry stakeholders are modifying their mobile platforms and offerings to create an omni-channel experience that enables customers to cross from one channel to another (i.e., online, in-store, in-app).

Dunkin' Brands

Dunkin' Brands is a franchise-based quick-service restaurant (QSR) business in which speed of service is an important goal. Payments did not become a strategic business until the launch of the Dunkin' Donuts mobile app in 2012, with the Dunkin' gift card (i.e., stored value) as the funding source. Dunkin' began accepting contactless payments when they deployed EMV chip terminals in 2016.

While the initial mobile app realized successful consumer adoption, the integration of Dunkin's loyalty program in 2014 drove greater adoption, incentivizing customers to use the app more often.[13] For franchisees, loyalty added value and increased efficiency for their business. In 2016, Dunkin' added the *mobile order ahead* feature as a key component of its mobile platform. *Mobile order ahead* users can customize their orders and save their favorite drinks to their mobile apps, making it more convenient to place orders before pick up in the store. The Dunkin' mobile app is designed to get its customers "in and out" of the store quickly.

Walmart and Sam's Club

Walmart has payments strategies for each of its three divisions: the U.S. market, Sam's Club, and international market (operating in twenty-seven countries).[14] Walmart believes mobile payments are still in a nascent stage in the U.S.

In the U.S., Walmart offers an in-store mobile wallet, Walmart Pay, as a feature within its Walmart mobile app. Walmart Pay is designed to drive customer self-checkout using QR-code based payments at the POS. The checkout register generates a QR code that the customer can scan at any time during the checkout

[11] Ovum (2016). *2016 global payments insight survey: Merchants and retailers changing the merchant experience*. Retrieved from https://www.aciworldwide.com/-/media/files/collateral/other/2016-global-payments-insight-survey-merchants-and-retailers.pdf.

[12] Panelists included Dunkin' Brands, Walmart, and Bank of America.

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

[14] Walmart generates approximately $500 billion in sales across these three divisions.

process with the Walmart Pay mobile app. The app is linked to the customer's online account profile where a default payment method is stored on file. While Walmart Pay does not offer a customer loyalty program, customers can activate "Savings Catcher"[15] to realize cash savings when using the app.

Sam's Club has a different business model, and is piloting the "scan and go" mobile app feature in approximately 600 stores across the U.S. Sam's Club customers use their mobile phones to scan products as they load them into their shopping carts in the store. When done shopping, customers use their mobile phones to check-out, receive an electronic receipt, and skip the checkout line. The customer's receipt and purchased goods are still checked by the store employee at the exit as a loss prevention tactic.

Bank of America

Bank of America's (BofA) mobile strategy allows customers to choose from a variety of wallets based on their preferences. The issuer does not offer a proprietary wallet solution but enables its payment cards to be loaded into other wallets such as Apple Pay, Android Pay, Samsung Pay, Microsoft Wallet, as well as the card network digital checkout wallets for online purchases. BofA is also developing a more seamless integration of its cards into the PayPal digital wallet. For its merchant clients, BofA facilitates creation of mobile payment solutions based on using stored value or incorporating loyalty. This strategy helps to ensure that BofA cards are present in the consumer's mobile wallet.

Consumer and Merchant Challenges to Mobile Payment Adoption

Several factors may impact greater consumer adoption of wallets: an overcrowded market and multiple, non-standardized solutions; merchant legacy systems and technology; and limited NFC-enabled POS terminals.

The number of competing mobile payment options at checkout can create consumer confusion. When selecting a payment method, some consumers may consider which method offers the greatest discount, reward, points, or convenience. Other consumers may choose the method that best protects them against fraud.

Some merchants accept multiple wallet solutions (e.g., Pay wallet, PayPal, and/or a proprietary wallet), which impacts both the consumer and merchant experience. Merchants need to determine which other wallet/payment methods, in addition to their proprietary solution, will be the best combination to attract the most customers. To make this determination, they need to consider the trade-offs related to cost, brand, and experience; and consider that as consumers attempt to increase their use of mobile wallets, their expectations may be that the wallets are also accepted at more locations.

Many large merchants are also challenged by decades-old underlying software that supports the merchant's payments and customer management infrastructure. This makes it difficult for merchants to respond quickly to newer technology. Each merchant has unique integration requirements, which causes wide

[15] Savings Catcher compares prices of eligible items purchased at Walmart to the advertised prices in the weekly print advertisements of major local retail stores. If Savings Catcher finds an advertised price that is lower than what was paid for the same exact item at Walmart within a limited time, the customer receives a credit for the difference that can be applied to an e-gift card.

variation in the time needed to update systems. Despite this challenge, merchants recognize the importance of keeping pace with innovation to meet customer demands and evolving business models.

Another merchant challenge relates to the way NFC works with Pay wallets. Merchants must actively turn on the NFC contactless capability for their POS terminals; however, once it is turned on, it works with all NFC contactless wallets and network cards contained within the wallets. The current design prevents merchants from being able to choose which NFC wallets and payment cards to accept because of the *Honor All Devices* rule[16] which requires merchants to accept all cards carrying the card network's logo.

Even without the *Honor All Devices* rule, merchants have limited ability to accept digital wallets selectively because they cannot identify a particular digital wallet or even if a digital wallet is being used at all by the consumer using an NFC-enabled mobile phone. There is an existing data field in the transaction message to provide the device/wallet ID, but is not utilized in practice. Knowing this information could help merchants identify and prevent wallets or devices they consider higher risk (e.g., certain wearables) from sending NFC payments. Also, because merchants do not know what each wallet does with the customer data, they risk losing control of their POS and the ability to prevent their customer data from being shared with competitors.

Collaboration Opportunities for Authentication and Mobile Wallet Adoption

Industry stakeholders agree that there are many opportunities for collaboration to increase adoption and enhance security, particularly for customer authentication practices in the card-not-present and card-on-file environments. Some companies offer collaboration-based technology that enables card issuers and e-commerce merchants to increase payment card acceptance and reduce fraud and chargebacks. Many payment industry stakeholders are collaborating to bring the new 3-Domain Secure 2.0 (3DS 2.0)[17] capability into the market to enhance e-commerce and m-commerce authentication.

In terms of mobile wallet adoption, several collaborative endeavors have also emerged. Chase Pay has partnered with LevelUp[18] to allow Chase Pay users to order ahead at participating restaurants using the LevelUp mobile app. Chase Pay has also partnered with Best Buy, Starbucks, and Walmart. PayPal has also announced several partnerships. PayPal users will be able to use their Chase payment cards to make in-store purchases within their PayPal accounts or alternatively, Chase Pay can be used at online retailers that accept PayPal. PayPal has also integrated with Android Pay and Samsung Pay so that PayPal can be selected as a payment method within those mobile wallets.

[16] Levitin, Adam J. (2016, Aug.8) Pandora's digital box: Digital wallets and the Honor All Devices rule. Retrieved from https://ssrn.com/abstract=2819146. Similar to the "Honor All Cards" rule, the "Honor All Devices" rule requires merchants to accept all devices set up to transact through the card network, to the extent that the merchant accepts payments using the communications technology employed by the device (e.g., magstripe, NFC, and Internet) and tie acceptance of a card network's payments via digital wallets to the acceptance of traditional plastic cards that use the same communications technologies.

[17] 3-Domain Secure (3DS) is a secure communication protocol used to enable real-time cardholder authentication directly from the card issuer to improve online transaction security and support the growth of e-commerce payments. 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.

[18] Level Up is a Boston-based mobile payment network, connecting consumers and merchants for mobile payments using QR codes generated from a consumer mobile app. For more information, see https://www.thelevelup.com.

III. Emerging Authentication Landscape

The third panel[19] discussed how mobile/digital wallets are driving changes for authentication strategies and tools in the payments ecosystem, such as EMVCo's[20] 3DS 2.0 protocol and the Payment Services Directive II (PSD2)[21] regulatory requirement in Europe. These new authentication solutions are shifting away from reliance on static data elements such as vulnerable passwords to other technologies, such as biometrics (e.g., fingerprints), behavioral analytics, and other strong customer authentication. The industry is also contemplating how technical standards may affect the future management of authentication (e.g., transaction data flows using 3DS 2.0 and Consumer Device Cardholder Verification Methods (CDCVM), and authenticator certification programs expected from the collaboration between FIDO (Fast IDentity Online) Alliance and EMVCo. This shift is being driven by the need to enhance security while providing a more optimal customer experience. Panelists discussed the following topics: (1) traditional authentication technologies; (2) emerging authentication technologies; and (3) authentication during customer registration and at point of transaction.

Traditional Authentication Technologies

Traditional authentications methods, such as password, PIN, SMS, one-time password (OTP),[22] and knowledge-based authentication (KBA)[23] continue to be used; however, because all of these methods involve a "shared secret" that is provided to the service provider, they are vulnerable to fraud.[24] Therefore, applying traditional methods for multifactor authentication is still relevant for mobile payments, where the mobile device brings these multifactor components together as something you have (i.e., device or token in user's possession), something you are (e.g., biometric such as fingerprint whether stored on the user's device or in the cloud), and something you know (e.g., password, PIN).[25]

Most issuers still use SMS or OTP for step-up authentication[26] because customers are familiar with those methods. However, they are not the best approaches for authentication and should only be maintained as

[19] Panelists included inAuth, RSA Security, FIDO Alliance, American Express, and Giesecke & Devrient.

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

[21] PSD2 is a data and technology-driven directive that aims to drive increased competition, innovation, and transparency across the European payments market, while also enhancing the security of Internet payments and account access. At the core of PSD2 is the requirement for banks to grant third-party providers access to a customer's online account/payment services in a regulated and secure way. This access to account rule mandates banks or other account-holding payment service providers to facilitate secure access via application programming interfaces.

[22] A one-time password (OTP) is valid for only one login session or transaction, on a computer or other digital device. An OTP is typically sent via SMS to a mobile phone, and frequently used as part of two-factor authentication.

[23] Knowledge-based authentication requires a user to answer secret questions that cannot easily be found in a physical wallet or online (e.g., mortgage amount, prior residences, high school mascot, favorite book, etc.).

[24] The user provides the credential to the service provider that must securely store the secret for future reference. These shared secrets are vulnerable to phishing or socially engineering attacks that coerce a user to share their secret credential with a fraudulent third party who can then use the credential to commit fraud.

[25] Given the shifting threat landscape, "something you know" authentication factors are considered the most vulnerable to attack; and therefore, present the highest risk of fraud. It is worth noting that OTP over SMS is theoretically an example of "something you have" but modern man-in-the-middle attacks have demonstrated it is nearly as easy to phish an OTP and use it to attack a service in real-time as it has been to phish a password, thus leading standards organizations like the U.S. National Institute of Standards and Technology (NIST) to issue updated guidance in 2017 calling for OTP via SMS to be "restricted" while only recommending proof-of-possession public key cryptography for the highest level of authentication assurance.

[26] Step-up authentication can be used when a transaction is considered suspicious, such as a consumer logging into an account from an unknown device. In this instance, a merchant or issuer can decide to request additional authentication from the customer using out-of-band authentication (OOBA) by sending a passcode via SMS text or email to the customer for verification.

fallback options. Panelists agreed that the best authentication experience for a consumer is one performed with limited involvement by the consumer, such as simply touching a fingerprint sensor or looking at a smartphone (using the camera), secured with a strong cryptography protocol between the device and the payment service without involving the consumer directly.

Consumer and stakeholder opinions about the effectiveness of different methods also vary. Stakeholders need to balance the authentication solutions that are most effective for their business and acceptable risk level with the customer's appetite for using those solutions. Depending on the type of transaction, dollar amount, etc., a customer may prefer more security over less friction, but not in all cases. For instance, an issuer might introduce step-up authentication (even if using OTP via SMS) because the customer is traveling and transacting out of the country.

Emerging Authentication Technologies

The panel discussed several developments in authentication methods and related proprietary standards: 3DS 2.0, biometric authentication methods, EMVCo's CDCVM requirements, and the FIDO Alliance authentication technical specifications.

3-Domain Secure (3DS) 2.0

3DS 2.0 is a risk-based system used to pass cardholder authentication context data to an issuer when a merchant or payment service is attempting to authorize a cardholder transaction during the online and mobile transaction process. The original version of 3DS (1.0) was not widely adopted by merchants or issuers in the U.S. because it required all customers to be redirected to the issuer's website to enroll during the purchase process, thereby interrupting the shopping experience and leading to high shopping cart abandonment. Unlike 1.0, 3DS 2.0 automatically pre-registers all customers with participating issuers, and incorporates risk-based elements. The new protocol supports mobile app purchases and other non-browser driven payments (e.g., smart devices, gaming consoles, etc.). It also allows merchants to control the look and feel of the interface compared to 3DS 1.0 where issuers created that content. Finally, it expands the scope to include risk assessment of card-centric activities that are not payment transactions, such as when a consumer adds a new card to a digital wallet.

3DS 2.0 allows merchants to pass additional data elements to the issuer through the access control server[27] that provide more intelligence about the transaction and the customer. Since 3DS 2.0 is risk-based, the shopping experience is not interrupted unless the issuer considers the transaction a higher risk and asks the merchant if it can perform step-up authentication with the customer for additional verification. 3DS 2.0 eliminates the use of passwords when a transaction is challenged by an issuer; the issuer recommends a method of step-up authentication, and the merchant can move forward with the recommendation or remediate in some other manner of their choosing. As with the existing protocol, 3DS 2.0 will shift the fraud liability to issuers when both the issuer and the merchant are participating and the merchant follows the issuer's recommendation.

[27] The 3DS 2.0 protocol requires an Access Control Server (ACS) on the issuer side, which verifies whether a 3DS authentication is available for a particular primary account number (PAN), and manages cardholder authentication for a specific transaction. Most financial institutions outsource the ACS to third party providers.

When asked about the prospects for 3DS 2.0 to reduce attempted fraud, one panelist described a similar solution that has been in the market for several years and has stopped 95 percent of attempted fraudulent transactions with very low false positives, with only five percent of transactions challenged. Data on how much fraud will be reduced with 3DS 2.0 will not be available until it is widely adopted in the industry.

Biometrics

Given the availability of fingerprint sensors, cameras, and microphones on most smartphones, implementation of biometrics has the potential to restructure the authentication market. Biometrics can replace traditional methods and also be used to perform behavioral analysis. Biometrics provides the tools and leverages the sensors present in the mobile device to monitor a user's screen navigation, typing style, and other information sources to create a trust metric that can complement the physical biometric.

One concern with biometrics is how to protect the storage location from compromise. In the Pay wallets the biometric data managed by the embedded sensor (also known as an authenticator) is encrypted and stored as a template in a secure enclave within the mobile device. The FIDO Alliance promotes the importance of keeping all biometric data within the device that captured it.[28]

Another concern stems from mobile apps that store the biometric data in the cloud. In addition to biometric sensors embedded in the device by the manufacturer, many mobile apps rely on third party service providers to embed other biometric solutions (e.g., face, voice, behavioral) in their apps. This may create an inconsistent consumer experience across apps and discourage consumer acceptance. The panel discussed the various modalities of biometrics and the rapid pace of innovation, noting that knowledge of the modality being used does not necessarily explain how the template is stored or protected.

Consumer Device Cardholder Verification Method (CDCVM)

CDCVM is a set of cardholder verification requirements established by the card networks to assess transactions originating from mobile devices. CDCVM defines the evaluation criteria for assessing whether the person presenting the payment instrument is the legitimate owner of the instrument. For example, Apple Pay in-store transactions use Touch ID or the device passcode as the CDCVM, instead of traditional PIN or signature. CDCVM is performed and verified entirely on the iOS device or Apple Watch and no additional customer verification action (such as entering PIN or signing receipt) is required at POS.

Merchants with high foot traffic desire fast throughput at POS, including fast, efficient cardholder verification for mobile in-app payments, while simultaneously requiring strong proof that customer verification has been accomplished with a high degree of trust to reduce the risk of fraud. CDCVM is becoming an important verification tool as more payment credentials are provisioned to mobile devices.

FIDO Alliance and Authentication Platform

FIDO Alliance (FIDO) defines technical standards for fast, strong, on-device "authenticators" built into all internet-connected devices. To support this focus, FIDO released two sets of specifications in December

[28] FIDO Alliance specifications do not displace biometric proprietary solutions but these solutions can exist on top of the FIDO platform.

2014, Universal Authentication Framework (UAF) and 2nd Factor Authentication (U2F).[29] The specifications support a wide range of authentication modalities including biometrics, PINs, etc. A FIDO-enabling authenticator (e.g., fingerprint sensor) entails building support for the public key cryptography, device attestation, and public registry of device metadata that meet FIDO specifications. All FIDO authenticators create a public-private key pair and store the private key on the device while the public key is stored on the server. This removes the risk of credential compromise via a data breach or phishing attack since the private key cannot be shared off-device. Any user verification modality can be used to "unlock" the private key to sign authentication challenges from the online service (e.g., embedded biometric sensor or PIN number). FIDO's certification program objectively evaluates the conformance and interoperability of the technical implementation of FIDO authentication specifications. FIDO expects to add security certification testing in the near future to help ensure the on-device credentials are protected from malware and advanced physical attacks.[30]

FIDO replaces the password with a local on-device store of authentication credentials (e.g., the private keys defined in the FIDO protocol). The payment credentials still follow the traditional clearing and settlement process, and FIDO credentials are only used when the payment instrument is a wallet service that uses FIDO authentication for account authentication.[31] FIDO's strategy is tied to the device, not only for distributing the secure storage of credentials to these edge devices, but also for a common user experience across all the apps a consumer is likely to use.[32, 33]

According to FIDO, the device-centric ecosystem allows the industry to collectively move away from its dependency on passwords and other shared secrets vulnerable to social engineering attacks. Credentials in the FIDO model are bound to the device in which they were created. These credentials can be protected by hardening the mobile device against malware attacks by using a trusted execution environment (TEE),[34] a restricted execution environment, or secure enclave. This technology exists on almost every smartphone and is important to understand because data stored in these areas is protected from malware attacks.

Authentication during Customer Registration and at Point of Transaction

Securing the mobile wallet experience requires issuers and mobile wallet providers to have a comprehensive authentication strategy. This includes validating the cardholder and the device during wallet registration and at the point of transaction, and determining if the payment was initiated by an authorized device. Securing the end-to-end payment experience relies on this combination of identity and device confidence, in addition to strong provisioning methods to validate payment card information added to the mobile wallet. Successful solutions will minimize risk by securing the customer registration process.

[29] For more details, see https://fidoalliance.org/.

[30] FIDO Alliance offers its technical standards free of any licensing fees or restrictions. The certification testing program is open to anyone to participate in, with no requirement to join the Alliance.

[31] Samsung and PayPal were first to publicly deploy FIDO authentication in 2014.

[32] When a device establishes a preferred locking method such as a fingerprint, it can also make that authenticator available to app developers through a common API resulting in a common authentication experience across all apps, including payment apps on that device. FIDO is an open standard that device manufactures add support for in these APIs.

[33]FIDO is also working with the World Wide Web Consortium (W3C) to standardize FIDO authentication in APIs for web app developers.

[34] The trusted execution environment is a secure area of the main processor of a mobile phone (or other connected device). It guarantees code and data loaded inside (e.g., payment tokens) to be protected with respect to confidentiality and integrity.

A secure enrollment process also relies on data availability, use, and expert support. Wallet providers and stakeholders (such as issuers) need to collect and analyze more information – from the device, from customer behavior, or from the transaction, etc. Device data can prevent a fraudster from using a man-in-the-browser attack[35] to overtake a customer's mobile device. Passive data (e.g., all data to and from a customer's server) should also be collected and passed through a risk analysis engine. Artificial intelligence and machine learning can be used to analyze device, customer, and transaction data risks. 3DS 2.0 also supports payment card enrollment for wallets and card-on-file environments.

Collecting data to strengthen consumer authentication allows stakeholders to make better decisions. However, they must maintain a balance between the amount of personally identifiable information (PII) they collect and what consumers are willing to share. In general, not all consumers have the same level of understanding related to security of digital payments or comfort using some of the tools (e.g., biometrics). For example, some consumers trust using a fingerprint to authenticate, while others worry about how that information is stored because the consequences are high if a biometric template is stolen.

According to an American Express study that surveyed 5,000 consumers and 400 merchants in the digital payments industry, 37 percent of consumers have terminated a shopping experience before checkout because of security concerns. This underscores the need to deploy the appropriate combination of security in a way that makes the value clear to the consumer and does not hinder the consumer experience.

III. Securing Payments for Internet of Things (IoT) and Wearables

The last panel[36] discussed the future of IoT and wearables and the implications for payments. Payment devices have evolved from laptops, smartphones and tablets, to IoT and wearables. Hence, what constitutes "mobile" is becoming broader. However, the potential of IoT and wearables expands beyond the payments process and across all aspects of the retail model.

Using tokenization and cryptograms creates a framework to secure IoT payments. The tokenization model should remain the same since the foundation already exists. Some environments may be able to connect directly to a card network but with the number of potential IoT devices, it would not be feasible for a card network to manage all of them directly. Working through an *on behalf of* token requestor[37] or aggregator model is one way to connect an IoT to a card network and obtain tokens. Because card networks do not have the resources to address the potential need for thousands of tokens they may work with other companies that offer *on behalf of* token services.

[35] A Man-in-the-browser (MiTB) attack is an internet threat similar to a man-in-the-middle (MiTM) attack that uses a proxy Trojan horse to infect a web/mobile browser by taking advantage of vulnerabilities in browser security to modify web pages or transaction content.

[36] Panelists included Gemalto, Mastercard, and a consultant.

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

A token service provider (TSP)[38] provides issuance and support of a payment token rather than a primary account number (PAN). Companies that perform trusted service manager (TSM)[39] or TSP functions can connect to a card network token service to obtain tokens and keys and provision them to an original equipment manufacturer (OEM) (e.g., Apple, Android) or other companies. Some TSPs also aggregate payment tokens across card networks that allow companies using the TSP to make only one connection for payment tokens from multiple card networks (rather than four separate connections).

Token requestors may be OEMs, merchants, issuers, and even card networks (e.g., Mastercard can be a TR of Visa tokens and vice versa). This model is evolving; however there is a need for consistent vernacular by the card networks to describe these types of services.

Securing payment credentials in an IoT and wearables environment is just as important as it is with traditional card/mobile/digital payments. Some concerns were raised about the ability for consumers to control the connection of their payment cards to multiple connected devices with the increased use of discrete tokens for each IoT device. Consumers may not understand how tokens are bound to their various devices and need to know where their credentials are stored. Issuers should be able to provide some controls for the consumer to manage those tokens. One card network is developing application programming interfaces (APIs) that will enable issuers to access the card network when a new token is provisioned on any device and provides information on where customer tokens reside in the mobile banking app and allow them to toggle the tokens on and off. The mobile banking app will display the last four digits of the token so the customer can recognize it on a receipt. An issuer can also make features available to allow the customer to see the token on a wearable and to set dollar limits.

Panelists discussed concerns about Bank Identification Numbers (BINs) and the issuance of tokens for IoT and wearables. Card networks manage token BINs by account range. Mastercard, for example, expanded its BIN range to eight digits and licensed a new set of BINs.[40] This change should allow for more BINs to support new payment products (e.g., smartwatch, selfie, etc.). Visa is expected to implement eight digit BINs in April 2022.

The industry is about to embark upon the next stage of the evolution of the connected consumer, where technology influences much of what the consumer does, and sometimes in opaque ways. Retailers should recognize that retail is no longer only about physical sales and e-commerce. Future technology developments will envelope IoT and wearables, together with voice commerce (e.g., Amazon’s Alexa) and payments using social media. For example, both Alipay[41] and WeChat Pay[42] have become embedded with the merchant and customer experience in Asia. Whether this market progression will impact the behavior and choices of U.S. consumers remains to be seen. With IoT, any connected device will have the ability to

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

[39] Trusted service manager (TSM) is a role in a near field communication ecosystem. It acts as a neutral broker that sets up business agreements and technical connections with mobile network operators, phone manufacturers, or other entities controlling the secure element on mobile phones.

[40] As supply of new primary account numbers (PANs) has become limited, MasterCard announced in 2014 that they would be utilizing a new BIN (Bank Identification Number) range for MasterCard-issued credit cards starting in 2017. Historically, all Mastercard PANs began with a “5,” but new cards will be issued that begin with a “2.” These cards will work the same as cards starting with a “5,” though CNP merchants should verify that their systems and processes are ready for this change.

[41] Alipay is a QR-code based mobile app, owned by Chinese company Alibaba Group.

[42] WeChat Pay is a Chinese social media mobile app developed by Tencent.

order goods and services, which raises more security considerations as there are more access points to consumer account information. Consumer expectations will be shaped by the many devices that impact their lives, and by the ways their payments providers respond to the new opportunities that will proliferate as quickly as those devices.

IV. Key Findings

1. **The user experience is beginning to converge as more mobile/digital wallets are developed on common platforms and offer similar features, which will help build consistency in how consumers interact with mobile wallet apps**. Most mobile wallets are developed on NFC or QR code/cloud platforms and may offer a variety of features: receipts, loyalty programs, ability to track rewards, and order ahead with many of the quick-service restaurants (QSRs).

2. **Increasing customer adoption and merchant acceptance of mobile/digital wallets continues to be a challenge**. The industry must focus on increasing adoption and usage – both by consumers and merchants, particularly smaller, lower-tiered merchants. More incentives must also be considered to increase habitual use. Additionally, smaller merchants need to be educated on the benefits and risks of mobile payments to their businesses.

3. **The customer mobile experience is now omni-channel**. Merchants need to support an omni-channel customer solution and focus on the appropriate mix of payment choices to present in each channel. Each business needs to identify the ideal user experience by evaluating what mobile wallet features and functions consumers most prefer.

4. **Progress is being made on enhanced authentication**. The general consensus of industry stakeholders is that authentication must begin with the customer enrollment process, and that more data is needed for analysis to better manage risk. Stakeholders also agree that there is an opportunity to collaborate to enhance security for the card-not-present and card-on-file environments.

5. **While IoT and wearables are becoming a reality, they raise some security concerns**. Extending payment tokenization to IoT and wearables can address some security gaps, but may create business complexities with the expansion in the number of token requestors and new providers that are offering certain components of (but not all) TSP services that need to be resolved. The industry needs to perform more thoughtful analysis on the implications of IoT being integrated into the payment system.