



Choosing a Mobile Wallet: The Consumer Perspective

Susan M. Pandy, Ph.D. and Marianne Crowe
Federal Reserve Bank of Boston

March 9, 2017

Susan Pandy is Director and Marianne Crowe is the Vice President in the Payments Strategies Group at the Federal Reserve Bank of Boston. The views expressed in this paper are solely those of the authors and do not reflect official positions of the Federal Reserve Bank of Boston (FRBB) or the Federal Reserve System.

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

The authors would like to thank members of the FRBB mobile wallet team for their engagement and contributions to this report: Christine Capota, Nathaniel Cooper, Leslie Kirschner, Michael Nealand, Emilie O'Malley, and Elisa Tavilla.

Table of Contents

I.	Introduction.....	3
II.	Overview of Wallet Models and User Experience.....	4
	Model 1: Near field communication (NFC) “Pay” Wallets	4
	Model 2: Cloud-based CoF Wallets (Pay with Amazon and PayPal).....	13
	Model 3: Cloud-based CoF Card Network Wallets (Visa Checkout and Masterpass)	16
	Model 4: Merchant/FI QR Code Model: (Chase Pay and Walmart Pay).....	18
III.	Mobile Wallet Model Comparative Analysis	21
IV.	Recommendations.....	22
	Enhance Consumer and Merchant Education on Mobile and Digital Wallets	22
	Increase Targeted Marketing.....	22
	Offer Wallet Loyalty and Rewards Programs	23
V.	Conclusion	23

I. Introduction

The U.S. mobile payments environment is expanding, largely driven by the evolution of mobile and digital wallets. It is difficult to keep pace with the constant change and innovation in this market. Many studies have explored consumer mobile wallet awareness, attitudes, behaviors, and adoption, but few have developed a typology of the models.¹ To better understand the landscape, related market developments, and potential opportunities for best practices and standards, the Federal Reserve Bank of Boston's (FRBB) Payment Strategies group created a cross-functional internal team (wallet team)² to better understand the processes, potential risks, and variations of four wallet models through field testing and industry analysis.

For this paper, a mobile wallet is defined as “a digital container accessed by a mobile device (i.e., smartphone) that stores wallet applications, payment credentials, loyalty cards, and coupons, and is used to make proximity and remote mobile payments.”³ The four wallet models included are:

Model 1: Near field communication (NFC)⁴ “Pay” wallets (Android Pay, Apple Pay, and Samsung Pay)

Model 2: Cloud-based card-on-file (CoF)⁵ wallets (PayPal, Pay with Amazon)

Model 3: Cloud-based CoF card network digital “checkout” wallets (Express Checkout by American Express,⁶ Masterpass, and Visa Checkout)

Model 4: Merchant or financial institution (FI) QR code closed wallets (Chase Pay, Walmart Pay)⁷

The FRBB wallet team field-tested all the wallet models. They tested the NFC Pay wallets with device-specific mobile operating systems (Apple iOS and Android KitKat (4.4 or higher), including the Samsung Galaxy handset). The cloud-based mobile wallets, such as PayPal, Pay with Amazon, Masterpass, Visa Checkout, Chase Pay, and Walmart Pay, are device-agnostic, although some only function in the remote payments environment (Amazon) or the POS environment (Walmart Pay).

Wallet team members collected information about mobile wallet account set-up, enrollment and provisioning of payment credentials, authentication at the time of purchase, and the payment process,

¹ 451 Research (2015); Javelin Strategy & Research (2014); Chadwick Martin Baily (2015); Comscore (2015); Edgar Dunn (2016) *Advanced Payments Report*; Thrive Analytics (2014); as cited in Marous, J. (2015, Sept.) Mobile wallets: The battle for top of mind. *Digital Banking Report*, Issue 238.

² The project team conducted its analysis between June 2015 and May 2016.

³ Wearables and tablets are out of scope for this paper.

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 Card-on-file refers to the authorized storage of a consumer's payment credentials by a merchant or payment service provider that allows the consumer to conveniently make repeat or automatic payments without re-entering payment credentials each time.

⁶ The wallet team did not field test this wallet.

⁷ Another example of this model was CurrentC, developed by the Merchant Customer Exchange (MCX), a merchant-owned mobile commerce network, which was closed in June 2016. For more information, see <http://www.mcx.com/>. Some former MCX merchants have launched proprietary mobile wallets that are similar to the CurrentC model.

including receipt confirmation, returns, and chargebacks. They maintained diaries to track their personal experiences. These field tests provided insight into consumer perspectives by drawing on real user experiences with several merchants.

II. Overview of Wallet Models and User Experience

This section details use cases to describe the four mobile wallet models.

Model 1: NFC “Pay” Wallets

Apple Pay transformed the mobile wallet landscape by combining enhanced security features, including a secure element (SE)⁸ chip to safely store payment credentials, fingerprints for user authentication, and payment tokenization, incorporated into an NFC-enabled⁹ mobile phone.¹⁰

Android Pay and Samsung Pay are similar to Apple Pay, but leverage host card emulation (HCE)¹¹ technology with NFC instead of the SE to pass tokenized payment card credentials to the NFC-enabled POS terminal. Android Pay stores the payment token in a secure area of the mobile phone OS and Samsung Pay stores it in a trusted execution environment (TEE).¹² Samsung Pay also supports magnetic secure transmission (MST)¹³ technology, an alternative to NFC that enables contactless mobile payments at non-NFC POS terminals. Samsung Pay defaults to NFC if the mobile device detects an NFC terminal; otherwise MST is used.

The iOS model uses keys stored on the SE in the mobile device to generate a dynamic cryptogram¹⁴ for each transaction. This cryptogram is passed with the payment token for each transaction to the POS system. Samsung Pay downloads payment tokens and cryptographic keys¹⁵ from a cloud server and stores them on the mobile phone. Similar to Apple Pay, the keys generate a dynamic cryptogram that is passed with the payment token for each transaction. Android Pay stores payment tokens and cryptographic keys in the mobile OS and also passes the payment token and dynamic cryptogram (generated by the keys) to complete a transaction. Because Android relies solely on software architecture,

⁸ GlobalPlatform defines a secure element (SE) as a tamper-resistant chip that securely hosts applications and their confidential and cryptographic data (e.g. key management). In payment applications, the SE controls interactions between trusted sources (bank), trusted applications (mobile payment app) stored on the SE, and third parties (payee).

⁹ 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.

¹⁰ A payment token is a random value that replaces a cardholder’s primary account number (PAN) when initiating a payment transaction.

¹¹ Host card emulation (HCE) works with NFC to route the PAN or token from the mobile phone host processor to the NFC-enabled POS terminal, eliminating the need for an SE in the mobile phone. For more information on HCE, see Crowe, M. and S. Pandey (2016). *Understanding the Role of Host Card Emulation in Mobile Wallets*. Available at <https://www.bostonfed.org/publications/payment-strategies/understanding-the-role-of-host-card-emulation-in-mobile-wallets.aspx>.

¹² The trusted execution environment (TEE) 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.

¹³ Magnetic secure transmission (MST) technology emulates the magnetic stripe on a credit card wirelessly when a user holds the mobile phone over the POS magstripe reader.

¹⁴ A cryptogram is a layer of security dynamically created for each transaction using the EMV payment token and additional transaction data to create a transaction-unique value. The calculation and format may vary by use case.

¹⁵ Visa supports limited use keys (LUKs) and Mastercard supports single-use keys (SUKs) that are derived from a master domain key shared by the issuer and the cloud card management vendor (e.g., Samsung). Replenishment of the keys is driven by thresholds, such as time to live and number of transactions, set in the mobile application platform.

strong software-based protections and tools, such as sandboxing¹⁶ and white-box cryptography,¹⁷ are needed to secure the storage of payment tokens and keys.

The NFC Pay wallets uniquely combine a set of characteristics that differentiate them from other wallet models:

- 1) They are considered open wallets because they accept any eligible credit or debit card from a participating FI for funding and can be used at any NFC-enabled merchants.¹⁸ *However, they cannot function across mobile operating systems* (e.g., Apple Pay only works on eligible Apple iPhones and devices, and Android and Samsung pay only work with eligible Android and Samsung mobile devices);
- 2) They follow the *EMV Payment Tokenization Specification* (EMV spec)¹⁹ which supports using a payment token in lieu of the primary account number (PAN)²⁰ and a dynamic cryptogram from the beginning to the end of the transaction;
- 3) They perform issuer identification and verification (ID&V)²¹ before a payment token is provisioned to a wallet during consumer enrollment;
- 4) They leverage NFC technology to make proximity payments at POS by holding the mobile phone over the NFC-enabled terminal; and
- 5) They accept e-commerce “in-app” and browser-based tokenized mobile payments through participating merchants’ native mobile apps or mobile browsers, unlike purchases made directly from merchant native mobile apps which accept other payment methods. These mobile “in-app” purchases use payment tokenization and allow a consumer to authenticate and authorize a payment with his fingerprint or passcode.

The following section describes the key components of the Pay wallet process: 1) account set-up, 2) enrollment and payment token provisioning, 3) transaction flow, 4) user authentication experience at the time of purchase, and 5) user security experience.

¹⁶ Sandboxing improves application security by isolating an application to prevent outside malware, intruders, system resources or other applications from interacting with the protected app.

¹⁷ For more information about white-box cryptography, see <http://blog.bellid.com/what-is-white-box-cryptography>.

¹⁸ For Apple Pay’s current list of participating financial institutions, see <https://support.apple.com/en-us/HT204916>. For Android Pay, see <https://www.android.com/pay/>. For Samsung Pay, see <http://www.samsung.com/us/samsung-pay/>. Apple Pay also accepts private-label credit cards (e.g., Kohl’s, BJ’s, Ulta, Meijer, and J.C. Penney).

¹⁹ EMVCo (2014, March). *EMV Payment Tokenization Specification – Technical Framework*. Available at <http://www.emvco.com/specifications.aspx?id=263>. For more information about tokenization and the difference between security (acquirer/processor) and payment tokenization (network/issuer), see Crowe, 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>.

²⁰ A primary account number is a variable length, 13 to 19-digits, set of ISO 7812-compliant numeric characters generated with ranges associated with a BIN by a card issuer.

²¹ The *EMV Payment Tokenization Specification* describes ID&V as a set of functionalities and services that allow for a trusted association of the payment token to the PAN from an authorized cardholder. EMV ID&V allows for the validation of 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; PAN-based risk score assessment; and one-time password by the card issuer or its agent to verify the cardholder.

User Account Set-up Experience

Consumers are prompted to enroll in the pre-installed wallet when purchasing and activating a new phone, but they can do it at any time. The FRBB wallet team loaded the respective wallets to their mobile phones based on the type of handset.²² Five members tested Apple Pay and Samsung Pay, and four members tested Android Pay.

Account set-up experiences varied based on the type of wallet and payment card. Before enrolling payment credentials in a Pay wallet, the wallet team members had to create either an Apple ID/iCloud account, a Samsung account,²³ or link a g-mail account to Android Pay, which they found time-consuming. Unlike the other Pay wallets, Android Pay also requires the consumer to enable NFC using the “settings” feature on the mobile device.

For payment authentication the team members either set up a fingerprint (Touch ID for Apple Pay), or a passcode/PIN in lieu of a fingerprint. Android Pay and Samsung Pay require consumers to configure their mobile phones to use a PIN or pattern to lock/unlock the phone for added security.

User Enrollment Experience

Before making the first mobile payment, the consumer enrolls his payment credentials in a Pay wallet. This registration process is consistent for all Pay wallets. The consumer manually enters the PAN, expiration date, and card verification code (CVC),²⁴ or uses the mobile phone’s camera to scan an image of the payment card and then enters the CVC manually. The consumer enters his name as it appears on the card and the billing address. For Apple Pay, consumers can opt to enroll their default payment card (card-on-file) for their iTunes account. Similarly, consumers can enroll the payment credentials they previously had on file for Google Wallet into Android Pay, which also accepts PayPal²⁵ as a funding source.

The process for adding payment cards varied slightly across wallet team members. For instance, if they enrolled in Apple Pay by scanning the card with the camera on the phone, sometimes the camera did not capture all the information from the physical payment card, including the card art. In that case, the user had to manually enter the card information.

Similarities between Pay wallets included how the card was verified (by email or text message);²⁶ display of wallet and issuer terms and conditions; and notification of completed enrollment (via pop-up window, email, and/or letter from the issuer). The only enrollment challenge wallet team members experienced pertained to instances when a card could not be enrolled because the related card issuer did not participate

²² Compatible handset models: Apple Pay - iPhone 6, 6 Plus or higher, Samsung Pay – Galaxy 6, 6 Edge or higher, and Android Pay - 4.4 or higher (KitKat and Lollipop versions).

²³ During the testing period team members had to first install the Samsung Pay wallet app on their phones, although this may no longer be a requirement. However the process was very time-consuming compared to the other wallets.

²⁴ Card networks vary in their definitions for the card verification code whether it refers to the static magstripe data, static data on the back of a credit/debit card, or the dynamic code generated by an EMV chip. This study generically refers to this as a card verification code (CVC).

²⁵ A consumer links PayPal to the Android Pay account using his PayPal login credentials.

²⁶ This will also vary by issuer. For example, some issuers may require the user to contact a call center for additional verification and other issuers may require voice authentication.

in the wallet. In this case, the user received the message, “issuer not supported.” Team members reported positive experiences during the card enrollment process with the messages displayed in the wallet app, such as “contacting the issuer,” “card successfully added to wallet,” or “card activated.”

Some merchants and wallet providers offer mobile rewards programs. Consumers can enroll multiple loyalty cards in the Apple Wallet²⁷ to receive and automatically redeem rewards: Walgreens *Balance Rewards* card, My Coke Rewards card, Kohl’s *Yes2You Rewards* card, and MyPanera. Android Pay accepts the Walgreens *Balance Rewards* card and My Coke Rewards card. Both Android Pay and Samsung Pay accept gift cards.²⁸ Samsung Pay also accepts most loyalty cards that use bar codes and offers a Samsung Rewards card, which allows users to earn points for every purchase, and redeem for rewards (e.g., gift cards). The wallet team used Apple Pay and Android Pay to test several rewards programs, including Sodexo, Walgreens, Kohl’s, and Panera and experienced no problems with the process. One team member attempted to enroll her WageWorks²⁹ transit card into a wallet to learn that the card was not supported.

The provisioning process requires the issuer to perform EMV identification and verification (ID&V) to ensure that the consumer is the legitimate owner of the payment credentials before the payment token is created and provisioned to a Pay wallet. The ID&V process examines the risk assurance score³⁰ and any additional data to decide whether or not to provision a payment token to a mobile wallet. Apple Pay also reviews certain data elements (e.g., age of iTunes account, device ID, history of phone activity, phone model, geolocation, etc.) and generates a risk score that is shared with the issuer to aid in the risk assessment. If the risk assessment determines that the account is low risk, the issuer can automatically accept it and provision the token to the mobile device.³¹

If the account is considered risky or raises other flags, issuers may perform stepped-up authentication to verify the cardholder and PAN using the following methods: (1) call center (consumer is directed to call a 1-800 number); (2) one time password (OTP) that the consumer receives via email or mobile phone number on file with issuer; or (3) customer login to his mobile banking app. Figure 1 illustrates the Pay wallet payment token provisioning process in Step 1, and the transaction flow in Step 2.

For example, one team member tried to enroll her husband’s credit card in her Apple Pay wallet, which was flagged by the issuer. She was directed to contact an issuer call center representative who told her that she could not enroll the card in her wallet because she was not the primary cardholder.

²⁷ Apple Wallet is an application in Apple’s iOS (previously known as Passbook) that allows users to store coupons, boarding passes, event tickets, store cards and, starting with iOS 8.1, credit cards, loyalty cards, and debit cards via Apple Pay.

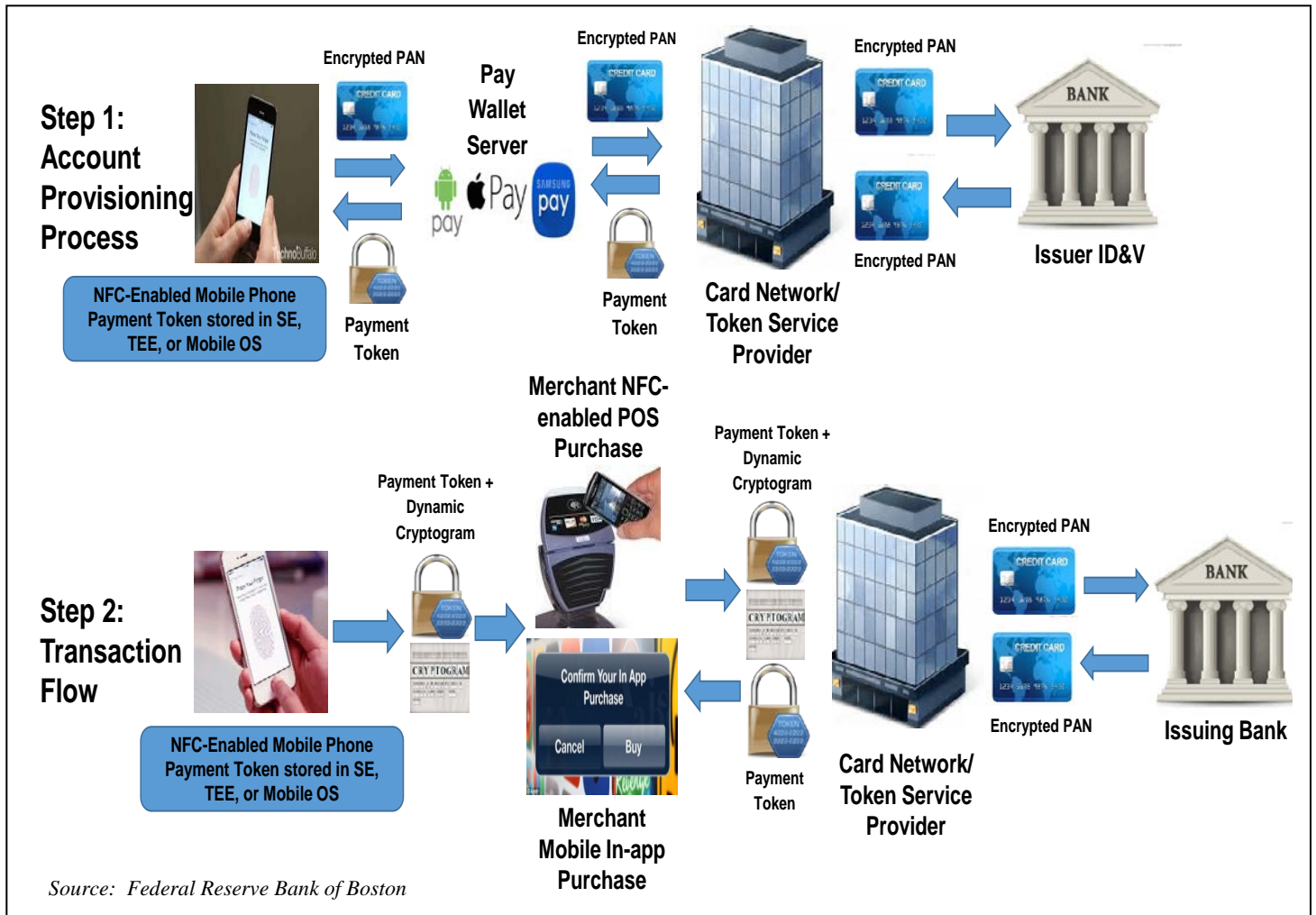
²⁸ Samsung Pay supports gift cards from 50 merchants, with no limit to the number of gift cards that can be added to Samsung Pay. The list of retailer gift cards supported is available at <http://www.samsung.com/us/support/answer/ANS00047403/>. To use membership or loyalty cards, users launch the Samsung Pay app, select the card, and hold their Samsung mobile phone displaying the card’s barcode to the merchant’s scanner at the register.

²⁹ WageWorks is an employer benefits service that provides tax-advantaged programs (prepaid accounts) for consumer-directed health (e.g., flexible spending or health savings accounts), commuter (transit and parking), and other employee spending account benefits.

³⁰ Under the *EMV Payment Tokenization Specification*, token service providers (TSPs) assign risk scores or token assurance levels to tokens at provisioning. The token assurance level is a mechanism to identify the level of risk associated with a token, and is based on (1) the type and outcome of the ID&V process when the token is provisioned; (2) the entity that performed the ID&V; (3) the domain in which the payment token is to be used; and (4) supporting token assurance data.

³¹ Consumer must accept the issuer terms and conditions to complete token provisioning process.

Figure 1. Pay Wallet - Payment Token Provisioning Process and Transaction Flow



User Authentication Experience at Time of Purchase

To make a Pay wallet purchase at a retail POS, the consumer holds the phone over the NFC-enabled terminal to automatically wake up the wallet (Apple Pay or Android Pay) and initiate the payment process. He then authenticates using a fingerprint or PIN/passcode which allows the payment information to be sent from the phone to the POS terminal. The consumer swipes-up from the home button to wake-up the Samsung app on the mobile phone, or selects the Samsung Pay app icon from his home screen and uses his fingerprint or PIN to authenticate. Whether the consumer selects the Pay wallet from within a merchant native mobile app (in-app) or directly from his mobile phone, the payment process is the same.

The team tested the Pay wallets for both POS and mobile in-app purchases at several small and large retailers.³²

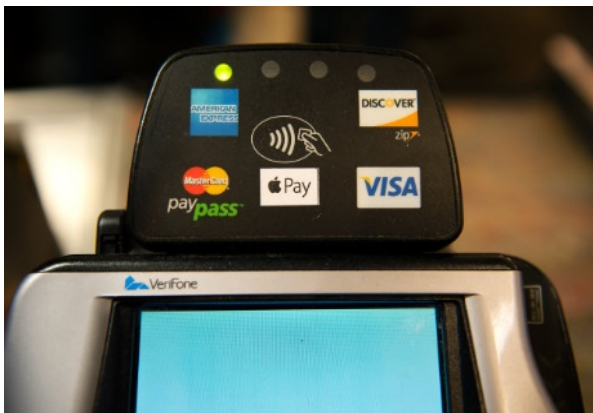
³² Team members made POS purchases at the following retailers: Anthropologie, BJ’s, DSW, H-Mart, Kohl’s, Macy’s, McDonald’s, Park n’ Shop, Petco, Roche Brothers, Star Market/Shaws, Trader Joe’s, Walgreens, Wegman’s, Whole Foods, Wine

POS Transactions: Completing a Pay wallet transaction varied by wallet type and merchant, and team members observed several challenges during the transaction testing process.

First, team members had to determine if the retailer accepted NFC Pay wallet payments since very few are NFC-enabled yet. Some retailers still have old POS terminals that are neither EMV-chip compliant or NFC-enabled. Some have migrated to EMV chip, but have not activated the NFC functionality. A few merchants had accepted NFC contactless transactions prior to the EMV migration but then disabled the functionality.

How acceptance of contactless NFC Pay wallets is communicated or displayed at merchant locations was inconsistent. Some merchants displayed the wallet acceptance logo on the doors to their store entrances and/or on the POS terminal itself. Typically, the POS terminal will at least have the NFC logo on it to indicate that it is NFC-enabled. But many merchants have now started to include the Pay wallet logo on the terminal as well. The appearance of the logo and location of its display on the terminal depends on the hardware manufacturer. Since newer terminals come from the manufacturer with the contactless symbol displayed on the reader, this adds to the confusion if the NFC feature is not yet activated, as noted above.

Figure 2. Pay Wallet Signage (Displayed on or near POS terminal or at store entrances)



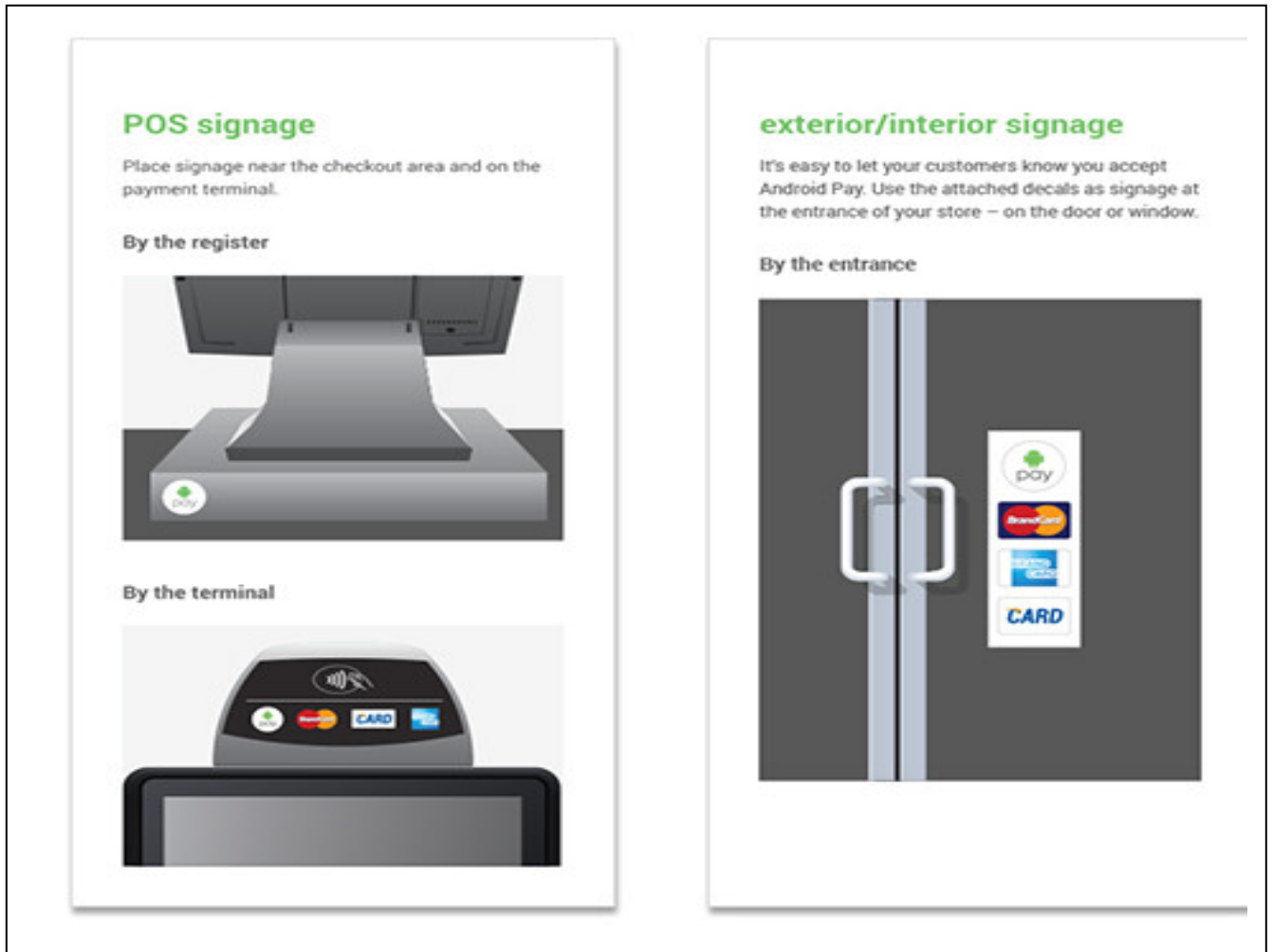
NFC and Apple Pay logos on POS terminal



Samsung Pay signage on retailer door

Emporium, and with taxi services in Boston and New York City. Mobile in-app purchases were made at Dunkin' Donuts and Starbucks to reload prepaid accounts, iTunes, and for merchandise purchases at Sephora and Target.

Figure 3. Android Pay POS signage and exterior/interior signage



Once team members determined that a retailer accepted Pay wallets, they could begin the transaction, which varied depending on the wallet. Those using Android Pay had to first unlock their phones to start the purchase process, which increased the transaction time. However, because the Apple Pay and Samsung Pay wallets automatically wake up when the mobile phone is held over a POS terminal, those users did not need to unlock the phone.

Users held the mobile phone over the contactless terminal and authenticated with either a fingerprint or passcode. Authentication must be completed before the payment credentials can be transmitted from the mobile phone to the NFC terminal to initiate the transaction. Where the user actually held the phone over the terminal to find the signal to receive the communication varied depending on the type of terminal; sometimes the user had to wave the phone around to find the correct spot.

Some merchants allowed customers to tap ahead before the transaction was completed (e.g., in grocery stores while items are rung up by the cashier),³³ but in other venues, notably in taxis, consumers had to wait for the process to complete and the taxi driver to initiate the payment screen where the customer selected the payment method. Depending on retailer's rules, team members were also prompted to provide a signature for transactions that exceeded a certain dollar amount (e.g., \$50 or \$100).

There were slight nuances in how users were notified of a successful transaction. For example, Apple Pay users received a notification displayed on the mobile phone screen: a check mark and "done," and in some cases the phone also vibrated.³⁴ Android Pay users received a green check mark and the mobile phone vibrated to indicate the transaction was complete, and a push notification was sent to the phone. Samsung Pay users saw a check mark and "done" to indicate a completed transaction. All three Pay wallets provided paper or email receipts for POS transactions on request (which users can designate when setting up the wallet). Users could also view their mobile wallet transaction history within the Pay wallet app.

Wallet team members found that the time to complete a POS transaction was comparable to using a plastic credit or debit card. If the terminal functioned properly the transaction process was smooth and convenient. When the terminal could not read the NFC signal from the phone, team members had to use another payment method.

From a support perspective, team members observed that retail staff had varying levels of familiarity and knowledge of the Pay wallets, although they noted that familiarity gradually increased over the duration of the project. Employees were least familiar with and often more confused by Samsung Pay, which launched later than the other Pay wallets and introduced a new component, MST technology, which allowed users to make contactless payments at any POS terminal.³⁵

When testing Samsung Pay using MST, one wallet user noted that it was unclear if the MST signal had been successfully transmitted from the phone to the POS terminal to complete the transaction until the paper receipt began printing, as there was no indication of the transaction status on the POS terminal or the mobile phone.

The Pay wallet experiences for wallet team members were generally positive, but they had more knowledge of how the mobile payment solutions worked. Novice users who try to pay with a Pay wallet at a merchant location may experience confusion and frustration. While lack of merchant acceptance is a major barrier to consumer adoption, some of the merchants that accept the Pay wallets still have inconsistent processes and staff training issues, which they need to address. These issues prevent some consumers from trying to use a Pay wallet even if they want to, and a bad experience may discourage them from trying to use the wallet at other venues that do accept it.

³³ Star Market requires Apple Pay customers to show the device account number located in the settings for the wallet on the mobile device if the transaction exceeds a certain amount (e.g., \$100). Staff is provided with detailed instructions for accepting Apple Pay, including how to help the customer locate the device account number.

³⁴ This process does not apply to Samsung MST transactions, which mimics the magnetic stripe card swipe transaction process.

³⁵ Only a limited number of Samsung Pay MST transactions were tested. Wallet members found that cashier familiarity with MST was inconsistent.

In-App Transactions: Online merchant acceptance of Pay wallets for mobile in-app purchases is also small but growing. The wallet team experienced positive results when they made mobile in-app purchases. To make a purchase, the user shopped with a participating retailer via its mobile app or mobile browser and selected the Pay wallet at checkout. The user authenticated with a fingerprint or password to complete the transaction and saw a check mark and “done” on the mobile phone screen to indicate that the purchase was successful. The user also received an email confirmation from the merchant and was able to see the purchase in his transaction history for the Pay wallet. Wallet team members reported a significantly faster and more convenient checkout experience because they did not have to enter their payment credentials or shipping information (although they had to verify the shipping address on file with the merchant), and only needed to authorize the transaction with a fingerprint or passcode. Some merchants that accept Apple Pay and Android Pay for mobile in-app purchases include Groupon, Sephora, and Target.

Returns: Team members also tested the Pay wallet return process with varying results.³⁶ Some merchants automatically processed returns and credited the card used to make the purchase, and some asked users to show the physical credit card or to swipe it on the POS terminal. Other merchants asked users to tap the mobile phone they used to make the purchase over the POS terminal to initiate the return and re-credit the payment card account. Team members agreed that this last method was the most convenient and should be the standard method used to process NFC wallet returns.

User Security Experience

The Pay wallets provide several controls to secure the mobile payment: (1) during enrollment the payment credentials are encrypted and transmitted to the card network and issuer. Then they are tokenized and provisioned to the mobile device; (2) payment tokenization³⁷ ensures that the PAN is never stored on the mobile phone, on a cloud server, or with a merchant; and (3) fingerprint, PIN, or passcode is created for authentication, providing another layer of security. The wallet team members were satisfied with how these controls worked.

They also found that security methods used during the Pay wallet account set-up process were effective. These included: disabling the ability to take screenshots during the account set-up process; using an email address for verification; and notifying the customer when the account set-up was completed.

Overall, they reported positive experiences with the security of the Pay wallets.

³⁶ All returns were made with accompanying original receipts.

³⁷ When a consumer authorizes and authenticates a purchase, a payment token that maps back to the PAN stored in the token service provider’s (TSPs) token vault and cryptogram are sent to a merchant to obtain authorization to complete the transaction. A token service provider (TSP) is an entity that provides the generation, issuance, maintenance, and other processing support for payment tokens and operation of the token vault. Currently, only the card networks can serve as TSPs for EMV payment tokens.

Model 2: Cloud-based CoF Wallets (Pay with Amazon and PayPal)

Pay with Amazon and PayPal were included in this study because of their maturity and scale of adoption in the market. Pay with Amazon launched in 2013 and as of February 2017 has been used by 33 million customers.³⁸ Pay with Amazon only processes e-commerce payments (including mobile). PayPal began in 1996 and currently has 192 million active accounts.³⁹ Both are considered “open” wallets because they are mobile device-agnostic and can be used at any participating merchant via mobile browser or mobile app. PayPal can be used at POS and online via the mobile and digital channels and plans to add NFC capability in the future. Both accept several payment methods as funding sources (e.g., credit, debit, prepaid and gift cards, ACH, loyalty, private-label store cards, etc.). Merchants use application programming interfaces (APIs) to add Amazon and PayPal wallets to their mobile apps or mobile websites.

User Account Set-up and Enrollment Experience⁴⁰

The consumer account set-up processes are relatively similar, whether using a mobile app or mobile browser. Amazon automatically enrolls existing online customers in Pay with Amazon, which is activated the first time a customer uses it via mobile browser or mobile app. To create an Amazon account, a customer enters his name, email address, and (self-created) password. Amazon may require the customer to verify the email address by selecting a link within an email message and entering a confirmation code. The customer will then have access to any of his existing payment methods on file with Amazon.

PayPal customers enter their name, email address, and phone number, and create a username and password to set up an account. They answer security questions to be used if they forget their login credentials or when additional verification is needed. PayPal customers can also opt to create a PIN as a second factor of authentication for purchases. Like Amazon, PayPal also sends a link via email for the customer to confirm his email address. The customer clicks on the link and enters his login credentials or one-time code, depending on the verification process that the wallet has in place, to complete the account set-up process.

After the account is set up, Amazon and PayPal customers can enroll one or more payment credentials to their accounts to be stored on file. They can also designate a default payment method for future purchases. Amazon and PayPal perform proprietary risk management and verification processes and validate payment credentials with the issuing bank. Pay with Amazon and PayPal customers enter the PAN, name on the card, expiration date, and billing address via a mobile browser or mobile app, as well as CVC for PayPal, to enroll credit or debit cards. Customers can enroll a bank account (ACH) or gift cards to fund their online Amazon accounts, but cannot use these methods for mobile purchases through

³⁸ Finextra (2017, Feb. 7) *Pay with Amazon payment volume nearly doubled in 2016*. Retrieved from <https://www.finextra.com/pressarticle/67937/pay-with-amazon-payment-volume-nearly-doubled-in-2016>. Amazon has ~294 million customer accounts worldwide.

³⁹ Per website <https://www.paypal.com/us/webapps/mpp/express-checkout>.

⁴⁰ Accounts can also be set up using a desktop PC or tablet browser and consumers can then initiate transactions from a mobile device.

Pay with Amazon. PayPal customers can link bank accounts (ACH), debit and credit cards to a PayPal account.

The wallet team reported that the account set-up and enrollment processes for both Pay with Amazon and PayPal were easy and convenient.

User Authentication Experience at Time of Purchase

Both wallets use multifactor authentication to verify identity by requiring the customer to log in to his wallet account to authenticate. Amazon customers must enter an email address or mobile phone number and password. Customers may also opt to stay signed in to their account on the mobile browser for up to two weeks. When using Pay with Amazon for the first time with an online merchant, the customer is prompted to agree to share his name, email address, and shipping address with that merchant. On the backend, Amazon performs additional authentication of the customer based on data it collects such as device ID, IP address, geolocation, login behavior, session browser habits, and other behavioral analytics.

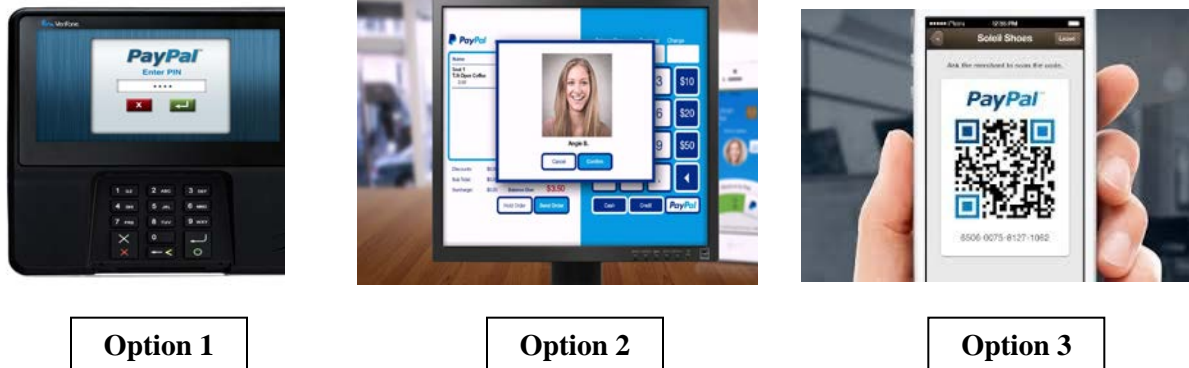
When a customer uses a mobile browser or mobile app to make a purchase at a participating merchant and selects PayPal as the payment method, he is directed to PayPal to enter his account credentials. However, if the user has enabled PayPal One Touch he can authenticate using a fingerprint that he has registered with the account. PayPal also performs additional authentication of the customer on the backend, collecting data similar to what Amazon collects.

*PayPal POS Transactions:*⁴¹ PayPal provides several “handsfree” options for consumers to authenticate and authorize POS purchases at participating merchants.⁴² Option one allows the customer to select the “PayPal” icon on the POS reader at checkout, and enter his mobile phone number and a PIN on the POS PIN pad. He does not need to use his mobile phone or mobile app. Wallet team members who tested this option reported a seamless experience. Option two allows consumers to share their geolocation with participating merchants. The merchant recognizes the customer when he enters the store. When he makes a purchase his photo displays on the terminal and he states his name to authorize a purchase. Option three requires the customer to display a QR code generated from the PayPal mobile app on his phone and scan it at the POS terminal. These options are illustrated in Figure 4.

⁴¹ Only applies to PayPal. The customer must obtain a PIN from PayPal to use this service.

⁴² Customer authentication methods may vary by merchant. FRBB wallet team members only tested the handsfree mobile phone number and PIN combination at Home Depot and Nine West.

Figure 4. PayPal POS “Handsfree” Options



Mobile Remote Transactions: Both Pay with Amazon and PayPal wallets are easy to use whether from a mobile browser or a merchant mobile app. Because the consumer’s payment credentials are stored on file, he does not need to enter them. He only needs to provide a shipping address if it differs from his original address on file. The PayPal remote mobile payment process offers great convenience by eliminating the need to enter login credentials if the customer chooses to use PayPal One Touch to authenticate and authorize a purchase.

Users can find participating online merchants for Amazon on its website, although this is not available for PayPal.⁴³ However, PayPal does list current offers (i.e., discounts) by participating merchants.⁴⁴ The wallet team members used Pay with Amazon at several online merchants, including L’Occitane, Midwest Sports, and Homeclick. They had the opportunity to review their shopping cart before confirming the purchase and received an on-screen confirmation number when the order was completed, followed by an email confirmation from both the merchant and from Amazon. Some of the PayPal merchants that the wallet team purchased from included: 1-800-flowers.com, 1-800-PetMeds, Beauty.com, Bed Bath & Beyond, and eBay.

User Security Experience

Both Amazon and PayPal wallets encrypt consumer data in transit and create security tokens to replace PANs, so that only tokenized values are shared with merchants for purchases.⁴⁵ They also have sophisticated risk management programs with proprietary risk models and advanced technology to detect, and often predict, suspicious activity to help prevent identity theft. These risk engines analyze data, building on successive customer interactions in the CNP environment to develop an internal risk score that determines the level of risk and whether to allow, challenge, or decline a transaction. Amazon and PayPal can track a broad range of proprietary and transaction data, such as what a typical transaction for that customer looks like, average shopping cart size/items, historical purchase data, and login behavior. If

⁴³ For a current list of participating merchants, see <https://payments.amazon.com/featuredmerchants>.

⁴⁴ See <https://www.paypal.com/deals/stores>.

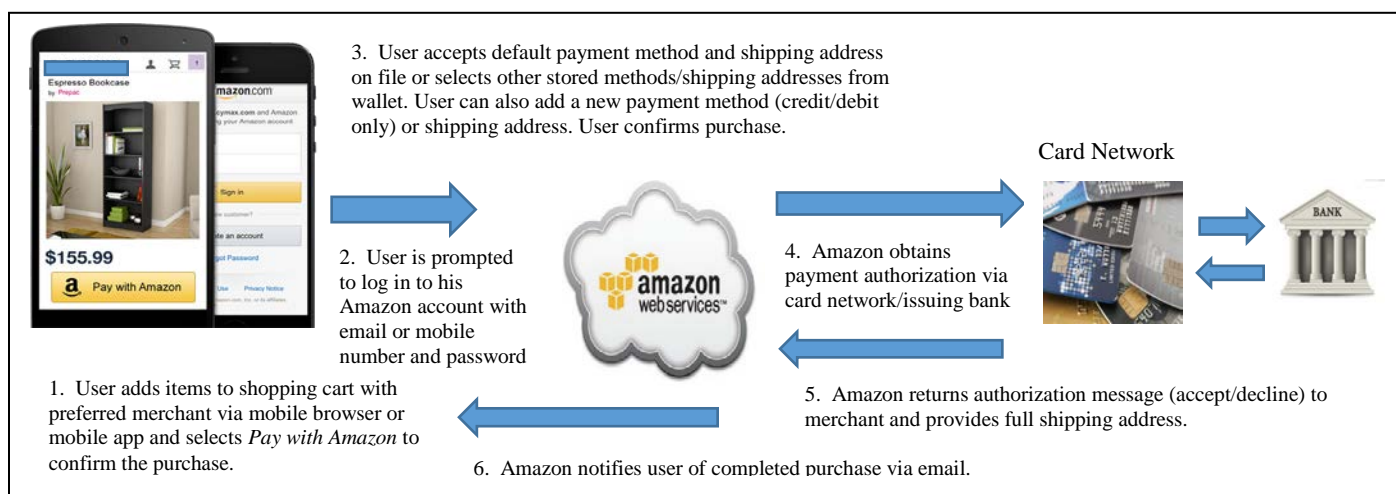
⁴⁵ Like payment tokens, security tokens also replace the sensitive payment account information with a non-sensitive token value. However, security tokens are generated on the back-end or post-authorization, and are also used to protect for data at rest.

the transaction is identified as high risk, Amazon and PayPal can present a security challenge question to the customer, or use historical transaction data or other authentication methods (e.g., 3-Domain Secure),⁴⁶ to verify the cardholder. They use email alerts to notify customers of any changes to their accounts and to confirm purchases.

Both companies also have strong vetting processes to validate participating merchants and mitigate fraud. Because PayPal and Amazon process on behalf of participating merchants that accept their wallets, the customer’s PAN is never shared with the merchant.

The wallet team reported no challenges or concerns related to security.

Figure 5. Pay with Amazon Transaction Flow on a Merchant Mobile Browser or Mobile App



Model 3: Cloud-based CoF Card Network Wallets (Visa Checkout and Masterpass)

Visa and Mastercard⁴⁷ developed digital “checkout” wallets, initially for online purchases, although Masterpass is developing a POS version. Visa Checkout launched in July 2014, and as of May 2016, had 12 million customer accounts worldwide.⁴⁸ Masterpass launched in 2013 and has over 40 million users worldwide.⁴⁹ Merchants work directly with the card networks to integrate the digital wallets into their mobile browser or mobile app checkout carts. Using digital checkout wallets eliminates the need for merchants to collect or store consumer payment credentials.

⁴⁶ For more information about 3-Domain Secure, see Pandey, S. (2017). *Why 3-Domain Secure should be adopted in the U.S.* Available at <https://www.bostonfed.org/publications/payment-strategies/why-3-domain-secure-should-be-adopted-in-the-us.aspx>.

⁴⁷ AmEx also offers a checkout wallet “Express Checkout,” but the FRBB wallet team did not test it.

⁴⁸ Statistica (2017). *Number of registered Visa Checkout users as of May 2016 (in millions)*. Retrieved from <https://www.statista.com/statistics/578460/visa-checkout-total-registered-accounts/>

⁴⁹ LetsTalkPayments (2016, Jan. 13) *A Comparison of 3 Biggest Digital Wallets Globally for 1-Click Checkout*. Retrieved from <https://letstalkpayments.com/a-comparison-of-3-biggest-digital-wallets-globally-for-1-click-checkout-2/>.

User Account Set-up, Enrollment, and Authentication Experience

To set-up a check-out account the consumer first selects the wallet from the merchant mobile website or downloads the mobile app. Next he enters his name, email address or mobile phone number, and creates a password to login and enroll. (Other options include enrolling through the issuer's online/mobile banking platform if offered; or being directed by a merchant, issuer, or partner service provider to the wallet during the checkout process.)

The consumer adds other personal information and payment credentials to the account, either manually or by using the mobile device camera to scan the payment card (if scanning, the CVC must be entered manually). Because Visa and Masterpass wallets are card brand-agnostic, consumers can add any eligible card-branded credit or debit cards. The consumer may also need to answer security questions for future authentication or to reset forgotten passwords. When enrollment is complete the customer receives email confirmation.

Wallet team members found the account set-up, enrollment, and authentication processes fairly straightforward with some exceptions. Scrolling through multiple screens on a mobile phone to enter a lot of data was tedious, so some members preferred to set up and enroll in the wallet using a traditional desktop PC.

Like the other wallets, finding merchants that accept Masterpass or Visa Checkout is difficult, which limits adoption. However, some merchants market directly to consumers and offer discounts as incentives to use the checkout wallets. Consumers can find a list of participating merchants on each wallet's website or look for the wallet logo on preferred merchant websites.

User Security Experience

After the consumer has added payment credentials, the digital wallet provider performs a risk management process, which verifies the email and billing addresses and collects information about the mobile device, including device ID and IP data checks.⁵⁰ It may also perform velocity checks, issuer CVC verification, account monitoring, review of consumer enrollment attributes or transaction history, and proprietary fraud tests.

Similar to Pay wallets, Masterpass and Visa Checkout both work through the card issuers to provision payment tokens to the wallets, used in lieu of PANs for these wallet purchases. Both networks also have robust risk management systems to monitor cardholder and account behavior for anomalies to prevent fraud. The wallet team reported no concerns while testing security of the checkout wallets.

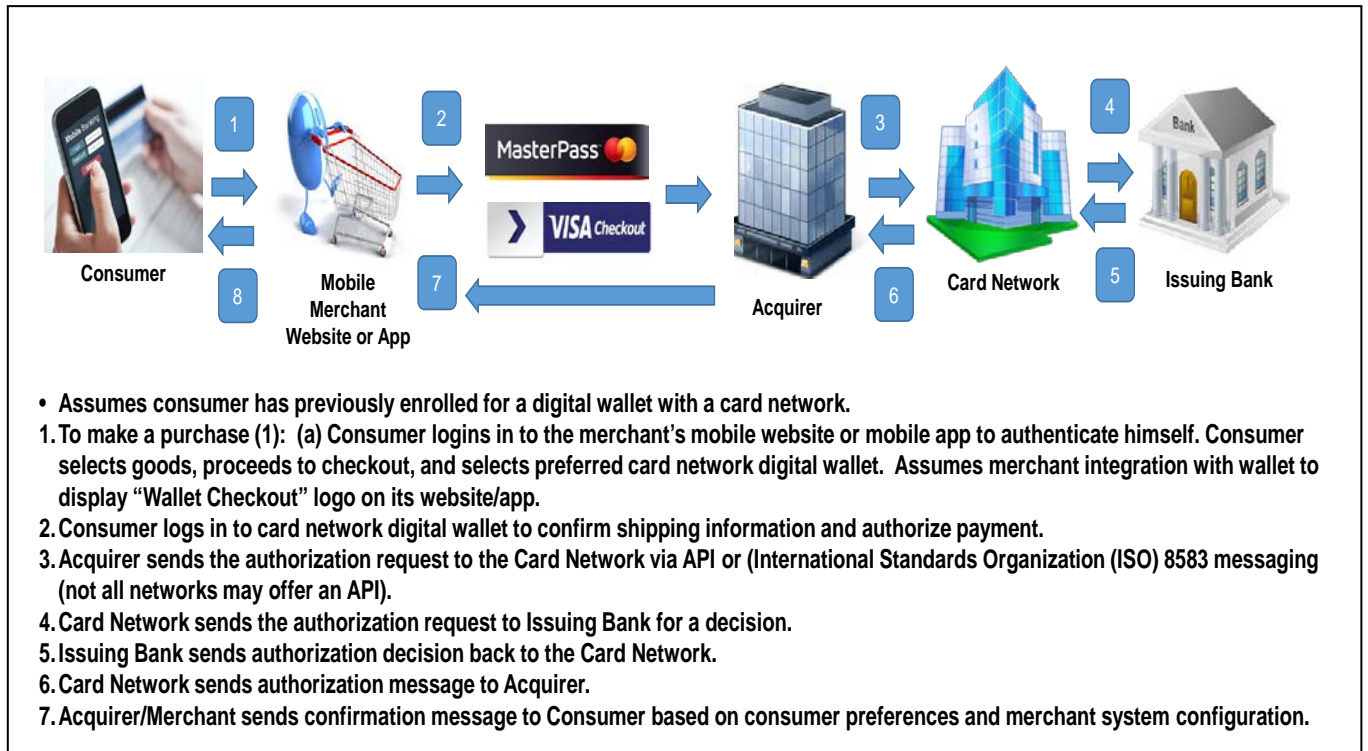
User Purchase Experience

The wallet team used Visa Checkout or Masterpass to pay for several digital purchases, including airline luggage fees and parking. They preferred using the digital wallets at less frequented or less familiar merchants because they did not need to create a new customer profile or share their payment credentials

⁵⁰ Internet Protocol (IP) data checks identify an Internet user's geographical information, including: country, region, city, latitude and longitude, zip code, internet service provider, and domain name.

with the merchant. After completing a purchase, the customer received an email confirmation from the merchant. While not tested, the return process is the same as with a plastic credit card.

Figure 6. Card Network Digital Wallet Transaction Flow



Model 4: Merchant/FI QR Code Model: (Chase Pay and Walmart Pay)

These wallets share some similarities with the Model 2 wallets (cloud-based and device-agnostic), but are classified in a different model because they use QR codes to complete POS purchases, are merchant or FI-branded, and closed-looped.

Chase Pay

Chase Pay is a digital wallet that can be used for POS, in-app, and online purchases with a mobile browser or mobile app. Chase Pay is relatively new, launched in November 2016. It is considered closed-looped because it is only available to its card customers⁵¹ and only used at participating merchants.

User Account Set-up, Enrollment, and Payment Experience

Chase.com customers with eligible cards (Chase Visa consumer credit, debit, and Chase Liquid (prepaid) cards) are automatically enrolled in Chase Pay, simplifying the provisioning process. A customer must accept the Chase Pay terms and conditions before using the wallet for the first time.

⁵¹ Chase had 94 million credit, debit, and prepaid customers when it was launched. Currently, Chase Pay does not accept Visa business credit or debit cards, or any Mastercard branded cards.

User Authentication at the Time of Purchase

Customers can pay for purchases through the Chase Pay mobile app or select Chase Pay as a payment option with participating online/mobile merchants.⁵²

To make a POS purchase, the consumer unlocks his phone (if locked), and logs in to his Chase Pay mobile app to authenticate. He opens the app to display the QR code for the cashier to scan, which is an extra step that is not needed for NFC Pay wallets.

To make an online purchase the customer selects Chase Pay as his payment method on the merchant website and is prompted to enter his Chase.com login credentials (username and password) to authenticate if he does not have a Chase bank account. If he forgets his Chase Pay password, he has to reset it, which makes the transaction process longer. One wallet team member experienced this situation because she uses her Chase credit card infrequently and had forgotten her login credentials. Once the authentication is complete, Chase verifies the customer's payment and shipping information on the backend and approves or declines the transaction.

User Security Experience

Chase generates a unique payment token for each payment card in the Chase Pay mobile wallet, which is used in lieu of the PAN when making a purchase. Chase Pay does not share the PAN with the merchant and only shares information that a customer typically provides when making an online purchase: payment token, email address, phone number, and billing/shipping address. For added security, the Chase Pay wallet can automatically update a PAN if a replacement card was issued because the original card was lost, stolen, or expired.

Walmart Pay

Walmart Pay launched in July 2016. It currently averages 22 million users per month, with an estimated 90 percent of transactions completed by customers who use the service three to four times a month.⁵³ Because the Walmart Pay wallet uses a QR code, consumers can download the app to any mobile phone, but can only use it to make in-store POS Walmart purchases. The app offers other features including check-in to pick up a purchase ordered online at a Walmart store, ordering prescription refills, and finding a Walmart location that has a particular item. Walmart recently began accepting Chase Pay for purchases on Walmart.com and at POS, which are routed through the Walmart mobile app.

⁵² For a current list of participating merchants, see <https://www.chase.com/digital/digital-payments/chase-pay/#shopwithchasepay>.

⁵³ PYMTS.com (2016, Nov. 30). *Walmart Pay Ecosystem: Mobile Pay Push Heats Up*. Retrieved from <http://www.pymts.com/news/mobile-payments/2016/walmart-pay-ecosystem-mobile-push-heats-up/>.

User Account set-up, Enrollment and Payment Experience

The consumer downloads the Walmart mobile app and creates a Walmart.com account if he does not already have one. Next the consumer responds to the request for permission to allow the app to use his location. He creates a username and password or PIN, and can opt to use Touch ID to authorize transactions. The consumer activates Walmart Pay from within the Walmart mobile app.

To enroll credit, debit, prepaid, or Walmart gift cards in the wallet, the consumer launches the app, locates the Walmart Pay icon and manually enters the PAN, expiration date, CVC, phone number, and billing address. The consumer must also accept the Walmart Pay terms and conditions and privacy policy. The wallet team members found this process somewhat cumbersome.

User Authentication at Time of Transaction and Payment Experience

To make a purchase the consumer opens the Walmart mobile app and selects Walmart Pay, which activates the phone's camera to scan the dynamic QR code displayed on the POS terminal. The consumer either enters his PIN or scans his fingerprint with Touch ID to authenticate. When the transaction is complete, the customer receives a digital receipt on his mobile phone.

Merchant mobile apps, such as Walmart Pay, are limited to those specific merchants, so customers must add separate mobile apps for each retailer with which they want to make mobile purchases. To try to offset the stand-alone nature of a retailer wallet some merchants add incentives. Walmart Pay's appeal is that it is automatically linked to all Walmart reward and loyalty programs, such as Savings Catcher.⁵⁴

Wallet team members found the Walmart Pay app easy to use at the POS and continue to use it regularly at Walmart, even though the entire process (i.e., opening the Walmart app, finding Walmart Pay and presenting the QR code to the POS) involves more steps than using an NFC Pay wallet. Despite the additional steps, team members still found it to be convenient and fast, particularly at self-checkout terminals.

User Security Experience

During the transaction process Walmart protects payment credentials by generating a QR code which serves as a token to authorize a payment without exposing the PAN. On the backend, Walmart generates and stores a security token in lieu of the PAN. However, unlike some other merchants, Walmart stores credit and debit card data (captured during enrollment) in its secure proprietary cloud for post-transaction processing.

⁵⁴ Walmart's "Savings Catcher" checks top competitors in the customer's area for advertised deals on eligible items and if a lower price is found for merchandise purchased with Walmart, the customer receives an e-gift card for the difference in price.

III. Mobile Wallet Model Comparative Analysis

This section provides a high level comparison of the wallet models addressed earlier, based on user experience and insights from other research conducted by Payment Strategies and the Mobile Payments Industry Workgroup.⁵⁵

Comparing the wallet solutions within each model yielded few differences. When looking at wallets across the four models, variations existed in underlying technology platforms, the enrollment and authentication processes, and where the solutions could be used – by channel and location. Across all wallets regardless of model, the greatest variations were customer-facing, i.e., how they were presented and accepted at merchants. Yet, these differences are likely easily addressed through best practices and can have the greatest impact on user experience and adoption.

Providing a convenient and frictionless payment experience at time of purchase is a common consumer theme for all wallets. Some wallets tested were better at customer-facing features to minimize friction, such as easy login/checkout, email notifications to confirm enrollment and complete transactions, and return policies.

The account set-up and enrollment processes for the wallets were similar, although some wallets added steps that made the process more time-consuming. The ability to use the phone's camera to scan an image of a card versus manual entry proved faster, less error prone, and was clearly preferred by the wallet team members, highlighting a general consumer preference.

Security plays a key role in all the wallets and continues to be top of mind for consumers. Some of the current wallet models provide stronger, more sophisticated security, i.e., the Pay wallets that implemented payment tokenization and fingerprint authentication. These security measures enhance the level of comfort consumer comfort with the knowledge that their payment credentials are secure. The card network digital wallets are also likely to achieve a high level of comfort among consumers in terms of security, largely due to the positive reputation of the networks to provide sophisticated levels of security and their use of payment tokenization. PayPal has partnered with the card networks (Visa, Mastercard, and Discover) to access their tokenization services for payment cards used with the PayPal mobile app at any POS where contactless NFC transactions are enabled. Other wallet providers are considering payment tokenization as well.

The wallets had different approaches to authentication performed at time of purchase. Entering usernames and passwords on a small mobile phone screen can be burdensome and less secure, difficult to remember, and error prone. The Pay wallets, PayPal, and Walmart Pay allow the use of fingerprints to authenticate, which is a faster and more convenient option. Pay with Amazon makes authentication seamless by allowing customers to stay logged in for two weeks at a time. Some wallets (e.g., Chase Pay and Walmart Pay) require consumers to unlock their mobile phones and open the app to login, creating more friction and exposure to compromise. These and other wallets still use QR codes (vs. payment tokens) as part of the POS authentication process, which is not optimal because of the security limitations.

⁵⁵ Crowe, M. et. al. (2016). *Getting Ahead of the Curve: Assessing Card-not-Present Fraud in the Mobile Payments Environment*. Available at <https://www.bostonfed.org/payment-studies-and-strategies.aspx>.

As leaders in the e-commerce payments business for many years, PayPal and Amazon have been able to leverage their maturity and reputation in risk management to expand into POS mobile wallet payments.

Most of the wallet providers understand the need for value-added services and have begun to offer various incentives and loyalty programs, which differ in how the rewards are linked to the wallet and redeemed. For example, Walmart customers are incented to adopt Walmart Pay to earn rewards and savings for shopping at Walmart. The Pay wallets recently began to add loyalty and reward programs to their platforms, but it is too soon to assess the impact on consumer adoption and usage. Amazon customers receive discounts on shipping costs for eligible goods when they use Amazon Prime. PayPal offers weekly deals to its customers for shopping with featured merchants.

IV. Recommendations

Enhance Consumer and Merchant Education on Mobile and Digital Wallets

For now, the payments industry seems to have settled on four wallet models built on variations of three different technology platforms. However, the differences across these wallets create market fragmentation and confusion among consumers and customer-facing retail staff. Poorly trained employees are not equipped to assist or educate shoppers, which discourages consumer adoption. Merchants have the added burden of training their employees on the wallets they accept, which may be one cause of slow merchant acceptance.

To provide effective education the industry needs to collaborate on developing best practices and some common standards around the issues noted in the previous section. This will ensure consistency and reach the broadest audience. Education should address: (1) how to use each wallet to make a payment; (2) how to provide consistent messaging that underscores their speed, convenience, and security strengths; (3) information on problem resolution; (4) and guidelines on how consumers can protect their mobile phones.

Increase Targeted Marketing

Merchants, FIs, and solution providers should increase their marketing of mobile/digital wallets to improve consumer adoption. Targeted marketing of a specific wallet, coupled with education, has been shown to bolster mobile wallet usage. For example, USA Technologies conducted a six-month test of targeted POS advertising of Apple Pay at their self-service retail locations, which resulted in increased overall sales, total transaction volume, and total contactless average ticket. The biggest gain was a 135 percent increase in overall mobile payment usage.⁵⁶ Marketing is a potential collaborative opportunity where wallet providers can work with merchants to develop appropriate strategies to increase consumer adoption.

⁵⁶ USA Technologies (2016, Nov. 21). *Apple Pay Messaging at Point-of-Sale Drives 135% Increase in Mobile Payments Usage*. <http://investor.usatech.com/releasedetail.cfm?ReleaseID=1000521>.

Offer Wallet Loyalty and Rewards Programs

Consumers have grown accustomed to receiving rewards and other loyalty offers from use of their payment cards and their online bank accounts. If the basic wallet process functionality can be standardized, then wallet providers and merchants can focus on differentiating their services with unique features including value-added loyalty and rewards programs. Because existing card payment methods work well for most consumers, such value-added services are needed to motivate them to use mobile/digital wallets more often. In the future, wallet providers may want to consider supporting other types of programs related to employee benefits (e.g., WageWorks) or transit, given the added convenience it would provide to consumers and to drive further adoption.

V. Conclusion

The good news is that most consumers have mobile phones capable of supporting a mobile wallet. However, the value proposition must be clearly stated to customers to change their behavior from using payments cards to using their mobile phones. While security issues remain a major barrier to mass mobile payment adoption and are being addressed by the industry, general consumer adoption is the real hurdle. Mobile wallet adoption in the U.S. is projected to grow considerably over the next three to five years, particularly with younger consumers, who are more inclined to use their mobile devices for payments. Opportunities to make mobile payments in new venues, such as transit, ticketing (movies, sporting events, etc.), taxis, parking, and other locations will help to build familiarity and generate habitual spending, which will augment adoption.

It is unclear how many mobile/digital wallets the market can effectively support. Since not all consumers have the same preferences or needs, they need multiple choices. For some purchases, consumers may want wallets that are accepted at a large number of merchant venues. They may want to use different wallets for e-commerce purchases or select their FI-issued wallets for other needs. However, it will not be efficient or convenient for most consumers to use (or even store) more than three or four wallets on their mobile phones. Too many wallets will dilute transaction volume and impact habituation.

To make the above projection a reality, it will be important for all wallet solution providers to look at wallet features for best practices, and consistency where feasible, particularly for customer-facing activities at merchants. It will also be important to develop adoption metrics to measure the success of mobile wallets to allow businesses to adjust their strategic responses to marketing, education, security, and incentives.