

# Mobile and Digital Wallets: U.S. Landscape and Strategic Considerations for Merchants and Financial Institutions

Version 1.0 Date: January 2018

## **U.S. Payments Forum**

191 Clarksville Road Princeton Junction, NJ 08550

www.uspaymentsforum.org



## About the U.S. Payments Forum

The U.S. Payments Forum, formerly the EMV Migration Forum, is a cross-industry body focused on supporting the introduction and implementation of EMV chip and other new and emerging technologies that protect the security of, and enhance opportunities for payment transactions within the United States. The Forum is the only non-profit organization whose membership includes the entire payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on, and have a voice in the future of the U.S. payments industry. Additional information can be found at <a href="http://www.uspaymentsforum.org">http://www.uspaymentsforum.org</a>.

EMV is a trademark owned by EMVCo LLC.

All registered trademarks, trademarks, or service marks are the property of their respective owners.

## About the Mobile and Contactless Payments Working Committee

The Mobile and Contactless Payments Working Committee was formed in November 2016 as part of the expanded U.S. Payments Forum charter. The goal of the Mobile and Contactless Payments Working Committee is for all interested parties to work collaboratively to explore the opportunities and challenges associated with implementation of mobile and contactless payments in the U.S. market, identify possible solutions to challenges, and facilitate the sharing of best practices with all industry stakeholders.

Copyright ©2018 U.S. Payments Forum and Secure Technology Alliance. All rights reserved. The U.S. Payments Forum has used best efforts to ensure, but cannot guarantee, that the information described in this document is accurate as of the publication date. The U.S. Payments Forum disclaims all warranties as to the accuracy, completeness or adequacy of information in this document. Comments or recommendations for edits or additions to this document should be submitted to: info@uspaymentsforum.org.



## Table of Contents

1.	1. Introduction5				
1	.1	Bacl	kground and History	5	
2.	Wal	let M	lodels	7	
2	.1	Dev	ice-Centric Mobile Proximity Wallet	7	
2	.2	Dev	ice-Centric Mobile In-App Wallet	7	
2	.3	Card	d-Not-Present Card-on-File Wallet	8	
2	.4	QR	Code Wallet	8	
2	.5	Digi	tal Checkout Wallet	9	
3.	Wal	let D	esign Choices, Technologies and Processes1	0	
3	.1	Wal	let Design Choices1	0	
3	.2	Wal	let Technologies and Processes1	2	
	3.2.	1	Near Field Communication1	2	
	3.2.	2	Cloud-Based Wallets1	4	
4.	Mol	oile V	Vallet Security Technology and Approaches1	9	
4	.1	NFC	Security	9	
4	.2	NFC	and Embedded Secure Elements1	9	
	4.2.	1	HCE with Virtual Cloud-Based SE1	9	
	4.2.	2	NFC, HCE, and Trusted Execution Environments2	0	
4	.3	Clou	ıd2	1	
4	.4	Ider	tification and Verification and Customer Authentication2	1	
4	.5	3-Do	omain Secure Customer Authentication2	2	
4	.6	QR	Code Security2	3	
5.	Mot	oile V	Vallet Landscape2	5	
5	.1	Curr	rent Wallet Examples2	5	
5	.2	Con	sumer Adoption2	8	
	5.2.	1	What Has Driven Usage?2	8	
	5.2.	2	Industry Forecasts	8	
5	.5	Less	ons Learned	9	
6.	Stra	tegic	Considerations for Merchants	2	
6	.1	Cust	tomer Experience and Adoption3	2	



6	i.2	Product Features and Roadmap			
e	i.3	Data Management			
6.4		Acceptance Terms			
е	5.5	Financial Considerations			
е	5.6	Technology Considerations			
7.	Strat	tegic Considerations for Financial Institutions			
7	'.1	Third-Party Wallets			
7	.2	Beyond Third-Party Wallets			
	7.2.1	1 Mobile Banking with an Integrated Wallet			
	7.2.2	2 Separate Mobile Wallet App40			
7	.3	No Mobile Wallet Strategy40			
8.	Cond	clusions			
9.	Lega	al Notice42			
10.	0. Appendix A: Glossary43				
11.	1. Appendix B: Stakeholders				
12.	.2. Appendix C: Standards				
13.	. Appendix D: Project Team50				



## 1. Introduction

This white paper was developed by the U.S. Payments Forum Mobile and Contactless Payments Working Committee to provide guidance to merchants and financial institutions regarding mobile and digital wallets. Sections 2 through 4 introduce different wallet models, technologies, and security approaches. Section 5 discusses usage drivers and lists the lessons learned from wallet launches and experiments.

The remaining sections identify factors and considerations key to developing a mobile wallet strategy. These factors can include fit with overall business strategy, desired customer experience, costs compared with expected benefits, partnerships, and technology. The appendices include information on the introduction of new stakeholders into the payment ecosystem, and work being done by standards' bodies in the field of mobile payments. The intention is to synthesize the early information from the market to help mobile and digital wallet ecosystem participants make appropriate strategic choices and to drive adoption of new payment technologies that ultimately improve customer experience.

## **1.1 Background and History**

Since 2007, innovations in mobile and digital wallets have resulted in a proliferation of wallet models and solutions, all intended to improve consumer convenience, leverage data, serve up offers, lessen friction, or lower the cost of payments.

The earliest wallet innovators, staring around 2007, were financial technology companies. Startups, including Braintree, Klarna, and Ayden, were launched to solve the problem of enabling in-app and m-commerce payments.

In 2010, AT&T, Verizon, and T-Mobile formed Softcard (formerly Isis) to realize the vision of a Near Field Communication (NFC) wallet with payment credentials securely provisioned in the secure element (SE) by the mobile network operators (MNOs). That same year witnessed the launch of Stripe. Stripe reduced the amount of time it took a new merchant to accept online card payments from weeks to minutes.

A flurry of merchant wallet introductions followed, including LevelUp and Starbucks in 2011, and Dunkin' Donuts in 2012. Also in 2012, the Merchant Customer Exchange (MCX) consortium was created, with the intent to launch a multi-merchant mobile wallet, called CurrentC. MCX, owned by more than a dozen large U.S. retailers comprising convenience store, fuel, grocery, big box retail establishments, and restaurants, claimed to serve nearly every smartphone-enabled American and account for approximately \$1 trillion in annual sales.

October 2014 marked a seminal moment in the history of mobile wallets with the announcement of Apple Pay. Although Google had announced the first device-centric NFC wallet, Google Wallet, in 2011, the industry had been eagerly awaiting Apple's technology decision.

In 2016, a year of retrenchment, Google recast its wallet for person-to-person (P2P) purposes only, Android Pay was launched, Softcard shut down and sold its assets to Google, and Amazon closed down its mobile wallet. At the same time, a proliferation of bank-centric wallets appeared (Capital One, Chase Pay, and Wells Fargo). Walmart Pay was launched at almost the same time that MCX apparently shut down after a series of delays and bad publicity.

Figure 1 illustrates the chronological development of mobile wallets.



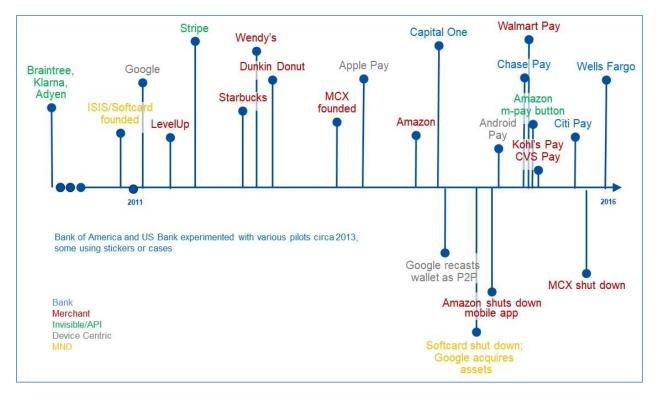


Figure 1. Mobile Wallet History and Timeline in U.S.



## 2. Wallet Models

Digital or mobile wallets enable transactions to be initiated by a mobile device at a point of sale (POS), online or in-app.

There are currently five different wallet models that use a variety of technology platforms, processes, and security tools:

- 1. Device-centric mobile proximity wallet
- 2. Device-centric mobile in-app wallet
- 3. Card-not-present card-on-file wallet
- 4. QR code wallet
- 5. Digital checkout wallet

## 2.1 Device-Centric Mobile Proximity Wallet

The device-centric mobile proximity wallet stores payment credentials in the mobile device. Near Field Communication (NFC) technologies or Magnetic Secure Transmission (MST) are leveraged to enable proximity payments at the POS. The POS must interact with the mobile device physically (a wave, a tap, a magnetic transmission).

This wallet is enabled through explicit permission from the financial institution that owns the payment account and performs issuer identification and verification (ID&V) before a payment token is provisioned to the wallet during consumer enrollment. The wallet is considered an open wallet because it accepts any eligible credit or debit card from any participating financial institution for funding, and it can be used at any contactless-enabled merchant (or if MST-enabled, any POS that accepts cards).

The wallet is operating-system specific: the wallet application in the mobile phone is integrated with the device operating system. Apple Pay works only on Apple devices, and Android Pay and Samsung Pay work only with eligible Android and Samsung mobile devices.

This wallet adheres to the "*EMV Payment Tokenization Specification – Technical Framework.*"<sup>1</sup> A payment token is substituted for the primary account number (PAN) and provisioned to the wallet during consumer enrollment. The payment application in the wallet generates a dynamic cryptogram that is carried with the token throughout a transaction. Tokenized credentials that are stored on the device or in the cloud are accessed using the wallet application. The wallet application also provides for access security that enables the consumer to use the payment method and stored data.

## 2.2 Device-Centric Mobile In-App Wallet

The device-centric mobile in-app wallet is used for an in-app card-not-present (CNP) mobile purchase. Unlike purchases made using a specific merchant's native mobile app, this wallet model uses EMV payment tokenization and issuer ID&V for an in-app payment. The tokenized payment credentials can be stored in the mobile phone or in the cloud. The device-centric in-app wallet model works with ecommerce "in-app" and browser-based tokenized mobile payments through participating merchants'

<sup>&</sup>lt;sup>1</sup> "EMV® Payment Tokenization Specification – Technical Framework," Version 2.0, EMVCo, September 8, 2017.



native mobile apps or mobile browsers (for example, an Apple Pay button). Consumers authenticate themselves and authorize a payment with a biometric or passcode.

## 2.3 Card-Not-Present Card-on-File Wallet

The CNP card-on-file (CoF) wallet uses previously stored payment credentials for transactions. Card-on-file is the term used to refer to the authorized storage of a consumer's payment credentials by a merchant or payment service provider (PSP) that allows the consumer to make repeated or automatic CNP payments without re-entering payment credentials each time. The stored payment data can be used by a single merchant or by multiple merchants that have integrated the PSP wallet solution. Examples include PayPal, Pay with Amazon, or a merchant's mobile app.

Consumers are authenticated using some type of verifiable access methodology (e.g., password, fingerprint), but the payment method is not provisioned by the financial institution that issued the card or account.

CoF wallets offered by PSPs are considered to be open, because they are mobile device-agnostic and can be used at any participating merchant through a mobile browser or mobile app. Both merchant and PSP CoF wallets accept multiple payment methods as funding sources (e.g., credit cards, debit cards, prepaid and gift cards, ACH, loyalty, private-label store cards).

In addition to creating their own wallet within an app, merchants can use application programming interfaces (APIs) to add Amazon or PayPal wallets to their mobile apps or mobile websites. After creating a PSP wallet account, the consumer enrolls a payment method. To pay, the consumer selects that wallet option on the participating merchant's mobile website or in the merchant's mobile app and then logs into the PSP to complete the purchase. Consumers using a merchant CoF wallet must create an account with a merchant and enroll a payment card to be used for future purchases.

Most PSPs and large merchants require the consumer to create a username and password to establish and log into the account. The PSP may also ask the consumer to select and create responses to knowledge-based security questions that can be referenced when additional authentication is needed<sup>2</sup> (e.g., because of a forgotten password, suspicious transaction, or unrecognized device). The first time a cardholder uses a wallet, the cardholder authenticates with the login credentials. The PSP or merchant matches the name to the payment card on file to verify that the transaction is legitimate. The PSP or merchant may also ask for the card security code to determine whether the cardholder is in possession of the physical card and use an address verification service (AVS) for further authentication.

## 2.4 QR Code Wallet

QR code wallets are similar to CNP wallets in that they are cloud-based and device-agnostic. These wallets use QR codes to complete purchases at the POS. They may be merchant or financial institutionbranded and are usually closed loop. QR codes are also used by petroleum merchants to identify or authorize fuel pumps. (See Section 3.2.2.2 for additional information.)

<sup>&</sup>lt;sup>2</sup> There are different types of payment authentication dealing with the card, the customer, and the device. For purposes of this paper, authentication refers to the customer, and is defined as the process used to verify the identity of the party enrolling in a wallet or initiating a payment transaction, using different types of credentials to prove the person is who he or she claims to be.



## 2.5 Digital Checkout Wallet

The payment networks offer digital checkout wallets or digital acceptance services to both issuers and merchants. The networks support web browser, mobile app, and in-app channels. The consumer can then pay online or in-app for CNP purchases, and one payment network has also enabled the checkout service for POS contactless purchases. The wallet can be accessed on an issuer's website and through their mobile app using the consumer's banking credentials. This approach enables a single banking and payment app for use by the consumer. Issuers can also automatically tokenize the card credentials to deliver a high level of security. Merchants can add the digital checkout wallet payment option to their mobile browser or mobile app checkout cart.

Consumers can be enrolled automatically in the wallet by their issuing bank. Their payment credentials can be stored and used as CoF credentials, so that the consumer need not enter the credentials to make a purchase using the wallet. Depending on the channel, consumers may have to authenticate with a password or biometric factor, such as a fingerprint.

Additional information on this wallet model can be found in Section 3.2.2.1.



## 3. Wallet Design Choices, Technologies and Processes

Providers determine what wallet model they support based on the technology they're implementing and solution they want to enable.

### 3.1 Wallet Design Choices

The technology and processes implemented determine how payment is presented and where and how payment credentials are stored. These options determine where payment can be accepted (for example, in store and online). They also affect how transactions are processed and reported.

Wallet design choices include:

- Interaction method for proximity payments: contactless NFC, QR code, MST.
- **Storage of payment credentials**: handset secure element (SE), Host Card Emulation (HCE)/cloud, card-on-file. HCE/cloud implies that the credential provisioning is related to NFC-based mobile payments, whereas card-on-file is a purely web-oriented solution (the payment credential is not tied to the mobile device).
- **Payment options**: proximity in-store payment, in-app, remote e-commerce or m-commerce (web browser).
- Acceptance mode: card/device present, card not present. The choice made affects the cost of acceptance for the merchant.
- Payment credential use: staged or pass-through wallet
  - The payment credential presented to the merchant in a staged wallet is a front end for the funding source.<sup>3</sup> This may affect the availability of transaction data or make it difficult to identify the merchant on the card statement.
  - A pass-through wallet uses a stored payment credential for transactions. The wallet provider stores the payment credential and only passes it along when the cardholder initiates a transaction with a merchant.
- **Push or pull payment**: Traditional card payments are pull—the consumer authorizes the merchant to pull payment from the consumer's account. However, some emerging payment models push the payment to the payee. Push payments are initiated when the consumer sends money to a merchant, without disclosing personal or financial information. Since the sender knows how much money is available, there is no need for authorization. In some systems, push payments are considered non-repudiable (i.e., they are final and cannot be disputed).
- Use of PAN or token: Providers will need to determine whether their solution stores the PAN or a token. This decision may be a choice or a specific requirement, based on issuer participation and payment network.

Table 1 describes various wallet models and how they have been pioneered to date. Also included are three emerging models (invisible in-app, alternative rails and person-to-person (P2P)) that are important to understand, but that are not covered in detail in this white paper.

<sup>&</sup>lt;sup>3</sup> The original Google Wallet operated as a staged wallet.



Model	Type of Implementation	User Experience and Considerations	Typical Technologies/Approaches Used
Device-Centric Mobile Proximity	<ul> <li>"Bank-centric"</li> <li>Application provided by bank</li> </ul>	<ul> <li>Holistic banking experience integrated with mobile banking app</li> </ul>	<ul> <li>NFC (Android only) or QR</li> <li>Cloud credentials (HCE)</li> <li>In-store payment</li> <li>CNP payment may be supported through a digital wallet provider</li> </ul>
Device-Centric Mobile Proximity	<ul> <li>"Mobile network operator (MNO)- centric"<sup>a</sup></li> <li>Wallet provided by MNO</li> </ul>	<ul> <li>Secure element provisioned by MNO with issuer permission</li> </ul>	<ul> <li>NFC</li> <li>SE</li> <li>In-store payment</li> <li>CNP payment</li> </ul>
Device-Centric Mobile Proximity/ Device-Centric Mobile In-App	<ul> <li>Wallet proprietary to handset manufacturer and/or operating system<sup>b</sup></li> </ul>	<ul> <li>Handset integration can optimize customer experience (e.g., open from lock screen)</li> </ul>	<ul> <li>NFC, MST</li> <li>SE or cloud credentials (HCE)</li> <li>In-store and in-app payment</li> <li>Card present for proximity payment in-store<sup>c</sup></li> <li>CNP for in-app payment</li> </ul>
Card-Not- Present Card-on- File/QR Code	<ul> <li>"Merchant-centric"</li> <li>Wallet provided by merchant, funded with private label, ACH or open loop card</li> </ul>	<ul> <li>Integrated with loyalty program</li> <li>Potential to optimize acceptance cost</li> <li>Support for features such as faster checkout, order ahead</li> </ul>	<ul> <li>QR, barcode, or numeric code</li> <li>Card-on-file, card not present</li> <li>In-store and in-app payment</li> </ul>
Digital Checkout	<ul> <li>"Payment network-centric"</li> <li>Digital cloud-based remote checkout solution that electronically delivers payment information to merchant</li> </ul>	<ul> <li>Easier e/m-commerce</li> <li>Enables others to build their own branded wallet</li> </ul>	<ul> <li>NFC (if POS) or QR code</li> <li>Cloud credentials</li> <li>In-app and e-commerce payment</li> <li>In-store payment for selected payment networks</li> <li>CNP</li> <li>May use tokenization</li> </ul>
Invisible In-App	<ul> <li>Other/hybrid</li> <li>Seamless transaction platform built into apps for specific businesses, where payment cards are stored</li> </ul>	<ul> <li>Ease checkout and eliminate friction</li> <li>Some share payment credentials across merchants</li> </ul>	<ul> <li>No proximity payment</li> <li>Card-on-file</li> <li>In-app and e-commerce payment</li> <li>CNP</li> <li>Provider is merchant of record</li> </ul>



Model	Type of Implementation	User Experience and Considerations	Typical Technologies/Approaches Used
Alternative Rails	<ul> <li>Other/hybrid</li> <li>New types of real- time payments</li> </ul>	<ul> <li>Instant funds availability</li> <li>Easier P2P payments</li> <li>Potential to optimize</li> <li>payment efficiency</li> </ul>	<ul> <li>QR code</li> <li>Cloud credentials</li> <li>In-store, in-app, and e-commerce payment</li> <li>Typically does not use payment card infrastructure</li> <li>Can be push or pull</li> </ul>
Р2Р	<ul> <li>Other/hybrid</li> <li>Person-to-person payment scheme</li> </ul>	<ul> <li>Solutions originally designed for person-to- person payments are now sometimes being used to pay merchants</li> </ul>	<ul> <li>In-app payment, with receiver identified by telephone number or email</li> <li>QR codes sometimes used</li> <li>Typically ACH, debit-to-debit card (on-file), or account-to-account</li> </ul>

<sup>a</sup> Currently no MNO-centric wallets are available in the U.S.

<sup>b</sup> Samsung Pay and Android Pay can co-exist on a device.

<sup>c</sup> Generally, payment networks consider card-present transactions that originate from issuer-provisioned credentials onto contactless or mobile EMV chip applets as a card form factor not a wallet.

## 3.2 Wallet Technologies and Processes

As discussed, a number of different technologies and processes are used in commercial wallet solutions. This section provides a high-level overview of the technologies used by the wallet models covered in this white paper. See also Appendix B, which includes information on a number of new stakeholders who fill roles that are not required with card-based payments, and Appendix D, which includes additional information on standards bodies' work that targets mobile payment solutions.

#### 3.2.1 Near Field Communication

NFC is a standards-based wireless communication protocol based on radio-frequency technology that allows data to be exchanged between devices that are a few centimeters apart. NFC payment transactions between a mobile device and a POS terminal use the same ISO/IEC 14443 standard communication protocol used by EMV and U.S. contactless credit and debit cards, allowing the mobile device to simulate a contactless card.<sup>4</sup>

NFC is used with the device-centric proximity mobile payment model across multiple mobile device operating systems. A wallet on an NFC-enabled mobile device is a software application stored on the mobile phone that manages and initiates payments. The mobile wallet accesses payment credentials such as tokenized payment cards, bank accounts, coupons, loyalty cards, or transit tickets, or financial information stored on the mobile phone in a trusted environment. The consumer must have the physical phone to initiate a payment transaction by tapping or holding the mobile device near a contactless-enabled POS terminal at a retail location.

<sup>&</sup>lt;sup>4</sup> NFC wallets also work with contactless POS devices not yet configured to support EMV by presenting a Magnetic Stripe Data (MSD) transaction. For more information, see the Secure Technology Alliance white paper, "<u>Contactless EMV Payments:</u> <u>Benefits for Consumers, Merchants and Issuers</u>," June 2016



Figure 2<sup>5</sup> illustrates the device-centric POS wallet transaction flow used by Apple Pay, Android Pay, or Samsung Pay with NFC and EMV payment tokenization.

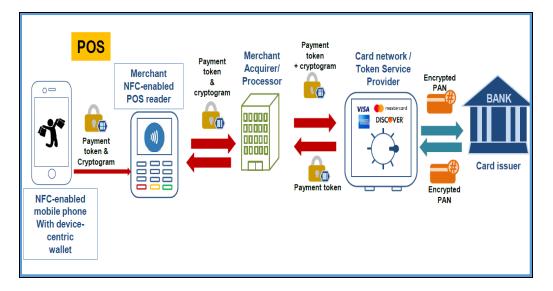
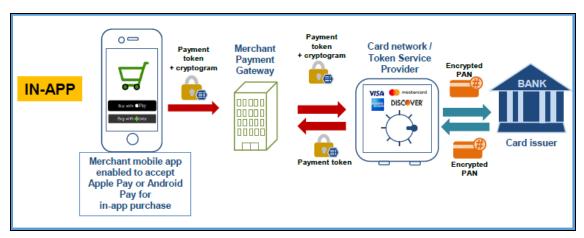


Figure 2. Device-Centric POS Transaction Flow

Figure 3<sup>6</sup> illustrates the slightly different process used for in-app mobile payments. The customer authorizes the payment within the merchant app using Touch ID or Face ID on the mobile phone for Apple Pay or selects "Buy with Android Pay" in the app. This sends the tokenized payment credentials that are securely stored in the phone and the cryptogram to the merchant app. The customer's billing information may be passed to the merchant app along with the payment credentials when the customer authorizes the purchase.





<sup>&</sup>lt;sup>5</sup> Source: Federal Reserve Bank of Boston.

<sup>&</sup>lt;sup>6</sup> Source: Federal Reserve Bank of Boston.



#### 3.2.1.1 Android: NFC and HCE

Android phones used with the device-centric proximity mobile payment model use NFC, but may use a different method for storing and routing payment card information.

Host Card Emulation (HCE) is a software-based payment card emulation solution that enables a mobile wallet app to communicate through the NFC controller to pass payment card credentials or payment tokens to a contactless NFC-enabled POS terminal or reader, eliminating the need to use a secure element (SE). HCE redirects NFC transaction requests to a mobile application rather than to an applet in the SE. HCE is used by the Android mobile device OS to support Android Pay and Samsung Pay.

An HCE transaction takes place as follows:

- 1. To initiate an HCE mobile payment, a customer taps the mobile phone at the POS contactless reader.
- 2. HCE enables the NFC controller in the mobile phone to route communications from the POS reader to the mobile wallet app to request access to the payment token.
- 3. The payment token and accompanying dynamic cryptogram are passed to the POS to complete the transaction.

HCE was developed so that stakeholders, including issuing banks, could access NFC capability without having to depend on mobile network operators or device manufacturers to secure space on the SIM SE. HCE implementations use other security techniques such as tokenization and/or a Trusted Execution Environment (TEE) to meet payments industry security requirements. For more information about TEE, see Section 4.2.2.

#### 3.2.1.2 Samsung: Trusted Execution Environment, Magnetic Secure Transmission and NFC

Samsung Pay uses the TEE with NFC, but also supports a second POS wallet technology, MST. MST enables compatible Samsung mobile phones to transmit payment data to a POS magnetic stripe card reader, without requiring NFC technology. The mobile phone emits a secure magnetic signal that mimics the magnetic stripe on a traditional payment card. This emulates swiping a physical payment card when a customer holds the phone over the POS magnetic stripe reader swiping slot. Samsung Pay defaults to using NFC if the mobile device detects an NFC field on the POS terminal but otherwise uses MST. Samsung Pay supports EMV payment tokenization for both NFC and MST transactions.

#### 3.2.2 Cloud-Based Wallets

Mobile payments using one of the wallet models described in Sections 2.3 or 2.4 may use a wallet app stored in the phone or a cloud-based wallet.

A cloud-based wallet stores payment information on a secure remote server (i.e., in the cloud) instead of in the mobile phone. The stored payment credentials are used to initiate the authorization of payment transactions. The cloud-based wallet sends only tokens or authorizations to the phone to initiate and authorize payment. Wireless service, either cellular or WiFi, is needed to complete a cloud-based wallet transaction.

The cloud wallet can be managed by a merchant or a PSP. From the merchant's perspective, cloudbased mobile payment services may be more flexible, as such payments avoid certain POS constraints. For example, the cloud wallet decouples a purchase from the payment and can support traditional



electronic and alternative payment methods that may offer the merchant less expensive payment options. Implementation of the mobile payment solution may be easier, since new POS hardware may not be required. Because the cloud model is hardware-agnostic, consumers do not need to move their data if they switch mobile devices or mobile carriers or upgrade their phones, although they would have to download the wallet app again to the new phone.

Use of cloud-based wallet services requires both the merchant and the consumer to subscribe. Merchants may need additional infrastructure to accept cloud payments at the POS. Depending on the wallet solution, customers may need to register with a wallet provider before making a payment. Merchants should also be aware that some cloud-based transactions may be treated as CNP transactions, typically resulting in higher payment acceptance costs.

The typical process requires the consumer to download the cloud-based app and subscribe to the service. The mobile device becomes an extension of the POS terminal, which communicates information about the mobile payment transaction to the cloud for authorization. Consumers can access their account information in the cloud using a browser or application. Once a cloud payment is completed, payment notification can take place using e-mail or text messages.

#### 3.2.2.1 Payment Network-Centric Digital Checkout Wallets

The payment-network-centric cloud-based wallets eliminate the need for merchants to collect or store payment credentials in the clear. American Express, Mastercard and Visa and have developed checkout services for online purchases.

Each payment network offers a different approach. Amex Express Checkout allows cardholders to seamlessly autofill their data on merchant sites. Merchants benefit from Amex Express Checkout through improved conversion, subsequent card-on-file transactions, and tokenization, with no changes to their existing payment processing. Mastercard typically works with the issuer to deliver the Masterpass<sup>™</sup> service for online and POS transactions, but the wallet functions can also be delivered directly by Masterpass. Issuer-hosted wallets connect to the Masterpass network of wallets through APIs. Alternatively, issuers can enroll through a Masterpass variant if they do not have their own wallet. Visa Checkout also works with issuer wallets but is only used for e-commerce.

Consumer enrollment is a prerequisite for these wallets but does not have to occur before the initial transaction. There are three enrollment options:

- 1. Pre-enrollment through the issuer's online or mobile banking platform
- 2. Pre-enrollment through a destination site hosted by the provider
- 3. Enrollment as part of the initial purchase

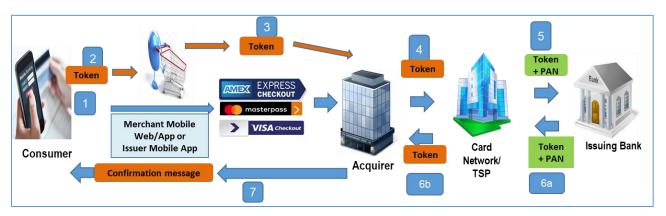
To enroll, the consumer creates a user name and a password. The consumer also enters his or her name, e-mail address, and mobile phone number. Consumers can add personal information and payment credentials either manually or using the camera on the mobile device to scan their payment card. If the information is scanned, the card security code must be entered manually. Because Visa Checkout and Masterpass are card brand-agnostic, consumers can add any eligible credit or debit cards from any brand. The consumer may also need to answer security questions to facilitate future authentication or reset a forgotten password. When enrollment is complete, the consumer receives email confirmation.



To make a purchase, the consumer clicks on the checkout wallet icon on the merchant's web page, logs into the checkout account or uses the issuer's mobile banking account credentials, and confirms payment. For added protection, the full PAN is not displayed during the checkout process on the merchant website.

To prevent unauthorized access to payment credentials, these solutions apply multiple layers of security, and robust risk management systems monitor cardholder and account behavior to prevent fraud. The providers use various techniques to secure the payload, such as by working through the card issuers to provision payment tokens to the wallets in lieu of PANs, or encrypting PANs stored in proprietary clouds.

Figure 4<sup>7</sup> illustrates a checkout process when the consumer has already enrolled, and the merchant displays the wallet checkout logo.





The process works as follows:

- 1. The consumer logs into the merchant site via the mobile browser or the issuer's mobile app. At checkout, the consumer logs into the digital wallet to confirm shipping information and authorize payment.
- 2. When the consumer initiates payment, the previously provisioned payment token is sent to merchant site.
- 3. The merchant (e.g., the wallet, e-commerce merchant, or app) passes the token to the acquirer/gateway as part of the authorization request.
- 4. The acquirer receives the token and routes it, along with the authorization request, to the card network to process.
- 5. The payment network/token service provider (TSP) sends the token/PAN, payment card details, and authorization request to the issuer for a decision.
- 6. The issuer returns the authorization decision and token/PAN to the payment network, which routes the token and authorization message back to the acquirer.
- 7. The acquirer/merchant sends a confirmation message to the consumer.

<sup>&</sup>lt;sup>7</sup> Source: Federal Reserve Bank of Boston.



#### 3.2.2.2 Cloud-based QR Code Wallet Model

A QR code or 2D barcode encodes numeric, alphanumeric, or binary data into a two-dimensional bar code that can be scanned and decoded quickly. The data representing a card number in the QR code may or may not be encrypted. The card number may also be tokenized or replaced with a virtual number, but the real PAN does not reside in the QR code.

There are currently two ways to use a QR code to perform a POS mobile payment at checkout.

#### 1. Consumer-Presented QR Code

One version of a QR code wallet works as follows: either a mobile app displays a QR code that was previously downloaded and stored in the mobile wallet, which the customer scans at the POS reader (e.g., Chase Pay, Dunkin' Donuts or Starbucks), or the app generates a one-time dynamic QR code (e.g., transit commuter rail), which is presented to the merchant.

The technology is considered a quick, easy, and inexpensive way for merchants to implement mobile wallet solutions, partially because NFC is not required. QR codes work with any phone with mobile app capability and typically with any credit, debit, prepaid, or store gift cards. The merchant POS needs only a scanner and QR code reader software to generate and read the QR code.

One example is Chase Pay<sup>®</sup>. Chase Pay is a digital payment option that works in a store, with mobile apps, online, and at a fuel pump. The mobile app uses QR codes with dynamic and tokenized data to keep information secure and to facilitate in-store purchases. The app is available to Chase customers with eligible cards. The cards are automatically enrolled in Chase Pay for online and mobile app purchases, which simplifies the provisioning process by preloading card and shipping information. Customers need not create new login credentials to activate the app.

The checkout experience varies by location:

- At a POS, the customer logs into the Chase Pay app and taps "pay" to create a secure QR code to be scanned by the cashier.
- At participating restaurants, order and pay ahead allows the customer to skip the line and adds coupons and loyalty rewards to eligible orders at checkout. To start browsing menus, the customer logs into the app and taps "order."
- Online, the customer clicks the Chase Pay button at checkout and then logs in to check out. Card information is never shared with the merchant.
- At a fuel pump, customers can pay for gas without leaving the car. To find participating stations nearby, the customer logs in to the app, taps "pay," and selects the "at the pump" option.
- In other apps, customers can also choose Chase Pay at checkout where it is available.
- If using points, when checking out with the Chase Pay mobile app or using the Chase Pay button online, the customer can redeem rewards with eligible cards by toggling on the "use points" option in the card details in the Chase Pay app, or selecting this option at checkout when shopping online.



#### 2. Merchant-Presented QR Code

The second version of a QR code mobile wallet uses a QR code generated by the merchant POS terminal, which the customer scans with the mobile phone's camera. The consumer's app uses the merchant information obtained from the QR code to initiate the payment transaction. The consumer's payment credentials are not stored on the mobile phone or merchant terminal.

One example is Walmart Pay. When items are scanned at checkout, a unique QR code is displayed on the POS screen. The customer opens the Walmart app, launches Walmart Pay, and enters a 4-digit PIN or uses biometric verification for security. The mobile phone is held over the QR code on the POS screen to sync with Walmart Pay. The QR code can be scanned before, during, or after items have been scanned at the register. When the transaction is complete, the customer hears a sound on the phone and receives an electronic receipt.

Use of QR codes with mobile wallets has become popular with several financial institutions and merchants due to the following benefits:

- Ease of implementation. Merchants can use their current barcode scanners at the POS to read QR codes, which are based on industry design standards.
- Broad market. NFC is not required on the mobile phone.
- Ubiquity. QR codes work with any smartphone and typically with major credit, debit, prepaid, and store gift cards. The merchant POS needs only a scanner and QR code reader software.
- Better payment experience. Using a mobile phone camera and related mobile app, consumers can scan QR codes not only to make payments but also to access sites on the Internet, download products, or find reviews and product information.<sup>8</sup>

However, this solution also presents challenges:

- Inconsistency. There are no standards for using (as opposed to designing) QR codes for payments. Different QR code implementation solutions have different technical specifications, resulting in inconsistent user experiences.
- Usability at the POS. The QR code process is not as seamless as an NFC "tap and pay" payment and more steps may be required for both the merchant and the consumer to complete the transaction. Finally, QR code readability may be unreliable due to lighting or size.
- Security concerns. See Section 4.6 QR Code Security.

QR code technology has been applied differently in different environments, and current standards are not interoperable. EMVCo recently published a new payment design specification<sup>9</sup> to address these inconsistencies and enable either consumers or merchants to scan QR codes while enabling merchants to accept different QR code payment solutions using the same process. For more information, see Section 12.

<sup>&</sup>lt;sup>8</sup> "<u>OR Codes: How Apple Passbook Changes the Merchant Equation</u>," Javelin Strategy & Research, July 2012.

<sup>&</sup>lt;sup>9</sup> <u>https://www.emvco.com/emv-technologies/qrcodes/</u>.



## 4. Mobile Wallet Security Technology and Approaches

This section describes the technology platforms and tools used to secure different wallet models.

## 4.1 NFC Security

Mobile payments using NFC are an extension of EMV chip transactions. When a mobile payment is initiated, EMV secures the payment transaction using dynamic data. Unique dynamic data values are generated using an encryption key; the dynamic data is used to authenticate<sup>10</sup> the transaction when it is authorized by the payment network. These values are only valid once. If a thief tries to re-use the payment transaction data, the transaction is rejected by the card issuer, making it harder for thieves to skim usable data.

The three primary NFC mobile payment solutions available in the U.S. today, Apple Pay, Android Pay, and Samsung Pay, use NFC but manage and store the EMV payment tokens<sup>11</sup> differently. Apple Pay stores payment tokens in the SE embedded in the mobile phone. Android Pay<sup>12</sup> uses HCE to store tokens in Android operating system KitKat v4.4 or higher. Samsung Pay uses NFC and HCE but stores the payment token and cryptographic keys in the TEE in the mobile phone. Card-issuing banks use NFC with HCE to offer their own NFC wallets, but because Apple controls access to the SE in Apple mobile devices, HCE solutions are limited to Android devices.

NFC wallet apps relying on SEs do not work on rooted/jail-broken mobile phones.

## 4.2 NFC and Embedded Secure Elements

An embedded SE is soldered onto hardware in the phone, as opposed to being on a removable SIM card. The mobile phone includes an antenna that is built into the handset and offers a strong communication signal between the mobile phone and the merchant terminal. SEs are tamper-resistant chips that can securely host multiple applications and cryptographic data, such as keys, in a smart phone. Apple Pay uses the SE embedded in its phones to store the payment token representing the PAN. As the mobile device manufacturer, Apple controls access to the SE in an Apple phone.

#### 4.2.1 HCE with Virtual Cloud-Based SE

Android Pay uses HCE instead of the SE in a mobile phone and stores a master domain key representing the PAN in the cloud. Payment tokens and limited-use or single-use token keys (LUKs) generated by the master domain key in the cloud are stored in a secure area of the mobile OS, which uses software-based security, such as white box cryptography, to obfuscate the key. LUKs generate cryptograms that are passed with the EMV payment token for each transaction. The keys are refreshed each time the user connects to a network, which enables transactions to be completed without network connectivity. Rather than requesting a token from the cloud each time it is needed to make a payment, solutions using LUKs address the possibility that an Internet connection might not be available to download a token. LUKs also are restricted and expire quickly, to minimize their value to fraudsters.

<sup>&</sup>lt;sup>10</sup> Note that this use of authentication is an exception to the definition provided in footnote 2.

<sup>&</sup>lt;sup>11</sup> For more information on the use of payment tokenization, see "<u>Is tokenization ready for primetime? Perspectives from</u> <u>industry stakeholders on the tokenization landscape</u>," Crowe, M., et al., June 2015.

<sup>&</sup>lt;sup>12</sup> Google Wallet was redesigned to support only person-to-person payments.



Storing payment credentials and cryptographic keys in the mobile phone OS is not as secure as using the SE, thus additional security measures, like payment tokenization, are needed with HCE.

#### 4.2.2 NFC, HCE, and Trusted Execution Environments

Payment credentials and the associated keys that generate a dynamic cryptogram for each transaction can also be stored in the TEE. The TEE is not as secure as an SE because it is not tamper-resistant; however, GlobalPlatform<sup>13</sup> specifications describe how applications can reside securely in the TEE, including how to interface trusted applications with the TEE and how applications running in the mobile OS can communicate with trusted applications residing in the TEE.<sup>14</sup>

#### 4.2.2.1 HCE Security

Rooting makes a mobile phone more susceptible to hacking and exposes HCE-based mobile payments to several vulnerabilities.<sup>15</sup> Rooting the mobile device can expose sensitive information such as payment credentials and make it easier for malware to access the confidential data. Malware itself can root a mobile phone. Fraudsters can root a lost or stolen device to gain access to sensitive information stored in the wallet app and use it to conduct fraudulent payments.

In the HCE model, communication passes through the Android OS. Basic security controls are limited, because Android does not prevent rooting. However, if a phone is rooted, the Android OS will not allow the user to download Android Pay or Samsung Pay. There is also an Android application for HCE wallets that verifies system settings and detects whether a device has been rooted. Users who try to use Android Pay or Samsung Pay on a rooted phone will receive a message that the wallet app has been locked because of an unauthorized modification to the phone. Given the risks associated with rooting, HCE wallet solution providers should make sure that their mobile wallet solutions check for this setting (developer options and root access) and take appropriate action as soon as the setting is detected.

Aside from rooting, the primary risk associated with HCE is the use of non-tokenized payment credentials, regardless of where the credentials are stored. Software storage, such as the cloud, is more vulnerable to security breaches and fraud than hardware storage, such as in the SE, and stronger security controls are necessary to protect the PAN.

EMVCo is working to enable a security foundation for software-based mobile payment solutions in response to the increasing number of solutions being deployed that use software applications to perform payment transactions.<sup>16</sup> Mastercard and Visa contactless specifications also support single or limited use keys and cloud cryptograms that recognize HCE tokens as valid payment credentials.<sup>17</sup> Methods that enhance the security of HCE mobile payment transactions include:

• User and hardware verification by something the user knows (username-password or PIN); something the user has (e.g., the phone, a smartcard reader); something a user is (e.g.,

<sup>&</sup>lt;sup>13</sup> <u>Global Platform</u> is a certification authority. Its specifications are considered best practices and are endorsed by the industry and internationally recognized.

<sup>&</sup>lt;sup>14</sup> "The NFC security quiz v2.0: Updated with HCE & tokenization," Fime, Aug. 2015

<sup>&</sup>lt;sup>15</sup> "HCE Security Implications, Analyzing the Security Aspects of HCE," UL, Jan. 2014.

<sup>&</sup>lt;sup>16</sup> In December 2016, EMVCo published "<u>EMV Mobile Payment: Software-based Mobile Payment Security Requirements</u>," Version 1.0, which provides security guidance and defines related generic security applications and interfaces. See <u>https://www.emvco.com/</u> for more information.

<sup>&</sup>lt;sup>17</sup> Visa uses limited use keys derived from the master key and Mastercard uses single use keys (SUKs). See "<u>Samsung Pay will</u> transform the mobile wallet experience," Gartner, 2015.



biometrics); and/or something a user does (e.g., determining how the user behaves; for example, multiple transactions made very quickly in several geographically distant locations could be denied). A device ID can also be used to validate the mobile phone being used for the transaction.

- **Transaction constraints**, to limit transactions to certain channels, such as online or POS, to specific merchants, or by dollar amount or country, thus reducing token exposure and fraud risk.
- **PAN tokenization,** replacing the PAN with a substitute value, increasing the security of an HCE mobile payment.
- **Data analysis**, to provide real-time transaction assessments to monitor activity and identify anomalies. HCE must rely on third-party managed intelligence services that provide tools to strengthen authentication at the device and OS levels by leveraging big data ecosystems. The more data that is available for measurements and analysis, the better the overall security.
- White box cryptography, preventing a key from being retrieved even when the original source code is available and can be used to hide payment credentials in the HCE application.

#### 4.2.2.2 Payment Tokenization

Tokenization replaces the consumer's payment card PAN, expiration date, and security code with a substitute value, called a token. De-tokenization reverses the process and redeems the token to access the associated PAN value. The true PAN value is protected because it is not exposed during the transaction.

When a payment card is provisioned to a mobile wallet, the TSP tokenizes the PAN and stores the token in the phone SE, mobile OS, or TEE. Biometric authentication on the device prevents unauthorized use of the device for payments. When the token is used in a mobile payment transaction, a dynamic cryptogram is generated by the phone and passed with the token through the payment process. If the token is stolen, it is useless to the fraudster, because the cryptogram only works for one transaction.

Samsung MST payments are also tokenized. When a consumer loads a card into the Samsung wallet, an EMV payment token is generated. During the payment transaction, tokenization protects the PAN, regardless of whether NFC or MST is used to transmit the token and cryptogram to the POS.

#### 4.3 Cloud

Cloud wallet solutions secure payment credentials by not storing them on the mobile phone. Because account credentials and sensitive data are stored in the cloud, the phone doesn't need to protect payments data.

#### 4.4 Identification and Verification and Customer Authentication

ID&V plays a key role in determining whether a consumer is the legitimate owner of the account credentials linked to a wallet; if not performed effectively, ID&V is a critical point of vulnerability. The level or strength of the authentication method should match the risk being mitigated. Despite the broad range of solutions available, authentication is the most serious fraud challenge merchants and issuers face for both e-commerce and m-commerce.



For device-centric wallets, tokenized payment credentials are not provisioned to the secure area of a mobile phone until the issuer has vetted the cardholder and the account. During the provisioning process, the device-centric wallet provider may send the issuer a risk score to aid the risk evaluation process. Risk scores are based on data that the wallet provider collects, such as device ID, device fraud scoring (a history of fraud on the device), geolocation, phone model, type of mobile OS, and history of an iTunes or Google account.

For a digital cloud-based wallet, after the consumer has added payment credentials, the digital wallet provider performs an additional risk management process that verifies the e-mail and billing addresses and collects information about the mobile device, including the device ID and IP data checks.<sup>18</sup> The provider may also perform velocity checks, issuer card security code verification, account monitoring, review of consumer enrollment attributes or transaction history, and proprietary fraud tests.

During the transaction process, a customer is also validated to the online merchant, PSP, or wallet service provider (WSP). Several common authentication solutions are customer-facing, such as username and password, knowledge-based authentication, one-time passwords or tokens, biometrics, and out-of-band authentication. Other authentication methods include device and location-based authentication, such as device ID, geolocation, data verification, risk-based authentication, and behavioral analytics.

Strong authentication practices do not rely on one test for authentication, but employ layered or multifactor authentication. Layered authentication employs multiple methods of single-factor authentication, such as username and password plus certain knowledge. Multifactor authentication creates a layered defense and makes it more difficult for an unauthorized person to access the physical location, computing device, network, or database. If one factor is compromised or broken, the attacker still has at least one additional barrier to breach.

## 4.5 3-Domain Secure Customer Authentication

The protocol called 3-Domain Secure (3DS) is a messaging protocol used to reduce fraudulent use of cards online and protect merchants from exposure to fraud-related chargebacks.

EMVCo recently published a new version of 3DS (version 2.0<sup>19</sup>) that allows issuers and merchants to exchange risk data, such as device ID and geolocation, during the ID&V process and during transactions. Merchants can decide whether more robust authentication is needed for a higher risk transaction and can invoke 3DS. The 3DS 2.0 risk engine challenges transactions that merchants deem high risk. When a consumer checks out on a merchant's mobile website, the purchase information, device data, and other details, are sent to the issuer to authenticate the cardholder and confirm the purchase. The issuer can passively authenticate the cardholder or, based on the risk profile, use stepped-up authentication and ask the cardholder to enter a one-time password or respond to a phone call.

Merchants control when to use 3DS, but issuers still control the message stream, because they own the liability for all 3DS-supported transactions that they approve. Merchants supply more data (e.g., e-mail address, mobile phone number, shipping, billing, and IP addresses) to help issuers with authorization decisions.

<sup>&</sup>lt;sup>18</sup> 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.

<sup>&</sup>lt;sup>19</sup> "EMV 3-D Secure–Protocol and Core Functions Specification v2.1.0," EMVCo, Oct. 2017



Unlike 3DS 1.0, version 2.0 can automatically register customers who have accounts with participating issuers, so those consumers do not need to enroll to use the service. Version 2.0 also supports mobile browser and mobile app transactions.<sup>20</sup>

## 4.6 QR Code Security

Use of QR codes involves several risks, due to QR code susceptibility to fraud and absence of governing standards.<sup>21</sup>

First, malicious QR codes can contain URLs with hidden malware, or redirect to fake websites for fraudulent purposes. If the QR code implementation is not for a proprietary system, the risk of fraud increases. In addition, completion of a QR code transaction at the POS relies on a smoothly functioning and secure in-store WiFi network or cell phone service. A denial of service attack can short-circuit the QR code transaction or a rogue WiFi network can steal user IDs.

And finally, if a fraudster obtains control of a lost or stolen mobile phone that is not password protected, and a merchant does not require customer verification, the fraudster can open the app and use the QR code to make a purchase or access the PAN and other account information stored in the cloud.

Several tools can help minimize the security risks associated with QR codes:

- Consumers should implement anti-virus and anti-malware software on their mobile phones.
- Some QR code payment apps (such as Starbucks) allow customers to add passcode protection to prevent use of the app if the phone is lost or stolen. The customer must enter an ID and password to reload the Starbucks account.
- The wallet provider, merchant, or other third-party vendor, such as a payment processor, should securely store customer payment credentials. They should encrypt all financial information during transmission and at rest, complying with PCI requirements, and not share personal information with other third parties.
- The QR code should never include credit or debit card information, as this information is typically randomly generated to map to the PAN stored in the cloud.

Another tool to consider is tokenization. For example, in addition to using a QR code, Chase generates a unique token for each payment card in the Chase Pay mobile wallet, which is used in lieu of the PAN for purchases. Chase Pay does not share the PAN with the merchant and only shares the information that a customer typically provides when making an online purchase—payment token, e-mail address, phone number, and billing or shipping address. The Chase device-centric wallet can automatically update a PAN when a replacement card is issued.

Walmart also uses tokens to protect payment credentials. During the transaction process, Walmart generates a QR code that serves as a token to authorize a payment without exposing the PAN. On the back end, Walmart generates and stores a security token in lieu of the PAN. Walmart also stores credit

<sup>&</sup>lt;sup>20</sup> 3DS version 1.0 only supports cardholder authentication for online browser-based transactions. The merchant, issuer, and consumer all have to subscribe to the service and the consumer has to authenticate for each transaction invoked by a merchant, which created customer friction and increased shopping cart abandonment. 3DS v 1.0 has not been widely adopted in the U.S. due to merchant concerns with cart abandonment.

<sup>&</sup>lt;sup>21</sup> "Transforming the customer experience: The promise of mobile wallets," First Data, 2013.



and debit card data (captured during enrollment) in its secure proprietary cloud for post-transaction processing.

Level-Up randomly generates a token that maps to a second token on the Level Up server, which then maps to a third token in the Braintree cloud. The combination of these tokens and two other authentication factors is required to initiate a transaction.



## 5. Mobile Wallet Landscape

Since 2007, innovations in mobile and digital wallets have resulted in a proliferation of wallet models and solutions, all intended to improve consumer convenience, leverage data, serve up offers, lessen friction, or lower the cost of payments. The differences among the models are determined by the value proposition the wallet represents to consumers or merchants.

Handset limitations sometimes dictate what technologies a wallet uses. For example, since Apple prevents access to the iPhone SE, Apple Pay is the only NFC-capable wallet on the iPhone. Android provides access to NFC capability using HCE, enabling other entities to develop an NFC wallet for Android devices.

### 5.1 Current Wallet Examples

Table 2 provides examples of mobile wallets with a description of several key features of each wallet, including examples of value-added services offered by example wallets.

Wallet Type	Example	Description and Value-Added Services
	Apple Pay	<ul> <li>Fast, easy user experience when using wake on lock screen and Touch ID or Face ID (no PIN)</li> <li>Checkout in-app, in Safari browser, and at POS using NFC where contactless is accepted</li> <li>Secured with tokenization, biometrics, SE</li> <li>Supported on iPhones and Apple Watch</li> <li>Access to SE for NFC-based payments restricted to Apple only</li> <li>Ability to store loyalty cards</li> <li>Promotions offering discounts, rewards on select in-app and web purchases</li> </ul>
Device-centric	Android Pay	<ul> <li>Checkout in-app, online, and at POS using NFC where contactless is accepted</li> <li>Secured with HCE, tokenization, and PIN or biometrics (if present on device)</li> <li>In addition to credit and debit, supports gift cards and loyalty cards</li> <li>Supported on Android phones and Android Wear watches</li> <li>Loyalty integration with select merchant incentive programs</li> <li>Possible to co-exist with Samsung Pay on same device</li> <li>Ability for merchants to provide offers to users</li> </ul>
	Samsung Pay	<ul> <li>Uses NFC and MST; can be used at nearly all merchants even if not contactless-enabled</li> <li>Swipe up from lock screen</li> <li>Checkout in-app and at nearly any POS (except fuel or ATM requiring card insertion)</li> <li>Secured with HCE, tokenization, and PIN or biometrics</li> <li>Provides wallet reward tiers based on frequency of usage</li> <li>Integrated and location-based offers with selected merchants</li> </ul>

#### Table 2. Examples of Different Wallet Types



Wallet Type	Example	Description and Value-Added Services
		• Ability to store and sort loyalty cards and merchant offers based on factors such as location proximity, expiration date, or savings amount
	Capital One	<ul> <li>Uses HCE to enable contactless payment at the POS</li> <li>Limited to Android phones</li> <li>Only Capital One cards can be used</li> <li>Does not require customer enrollment</li> <li>Integrated with Masterpass for in-app and online channels</li> <li>Real-time transaction notifications</li> <li>Easy access to balance and transaction history</li> <li>Instant rewards redemption options</li> </ul>
Bank-centric	Citi Pay	<ul> <li>Uses HCE to enable contactless payment at the POS</li> <li>Limited to Android phones</li> <li>Available to Citi customers for online and in-app purchases</li> <li>Does not require customer enrollment</li> <li>Integrated with Masterpass for in-app and online channels</li> <li>P2P functionality (send and receive) for online and mobile banking customers</li> </ul>
	Chase Pay	<ul> <li>Browser, in-app, and POS transactions</li> <li>Shared banking credentials with mobile banking platform</li> <li>Supports multiple payment methods at the POS (QR code, receipt capture)</li> <li>Only Chase cards can be used in the wallet</li> <li>Featured as a payment option on Walmart web site and in app; agreements in place with Best Buy and Starbucks</li> <li>Automatically updates card information upon expiration</li> <li>Integrated offers with select merchants</li> </ul>
	Amex Express Checkout	<ul> <li>Autofill solution which enables merchants to save Card on File</li> <li>Consumers leverage existing Amex credentials and don't need to set up another wallet/account</li> <li>Tokenization included with no change to existing merchant card processing</li> <li>Desktop, mobile web, and native channels supported</li> </ul>
Network-centric	Masterpass	<ul> <li>Omni-channel solution for browser, in-app, and POS transactions</li> <li>Any major credit or debit card can be used. Only certain cards can be used to make payments at store locations with the Android app</li> <li>Issuers can connect their own bank-branded wallets using APIs</li> <li>API platform for integration of IoT, other solutions</li> <li>Plans to extend Masterpass to Mastercard cardholders in Android Pay, Samsung Pay, and Microsoft Wallet<sup>22</sup></li> </ul>
	Visa Checkout	<ul> <li>Online/browser only</li> <li>Any major credit or debit card can be used</li> <li>Direct to consumer</li> <li>Issuer enrollment supported</li> </ul>

<sup>22</sup> "<u>Mastercard Enables Microsoft Wallet, Android Pay and Samsung Pay Users to Shop Online Wherever Masterpass is</u> <u>Accepted</u>," Mastercard Newsroom, October 2016.



Wallet Type	Example	Description and Value-Added Services
		Integration with Android Pay and Samsung Pay
	Starbucks	<ul><li>Tied to loyalty program</li><li>QR code on phone</li><li>Funding replenishment model</li></ul>
	Level Up	<ul> <li>White label to fast food restaurants</li> <li>Integrated with loyalty coupon program</li> <li>Unique transaction bundling helps optimize cost of payment acceptance</li> <li>Combined with loyalty, offers, analytics</li> </ul>
Merchant- centric	Walmart Pay	<ul> <li>Integral part of Walmart mobile app</li> <li>Phone scans QR code on POS screen at any time during the checkout process</li> <li>Customer authenticates with PIN or fingerprint</li> <li>Electronic receipt provided, no need to wait for printed receipt</li> <li>"Scan &amp; go" at Sam's Club eliminates checkout</li> <li>Item locator</li> <li>Store receipts for returns or warranty</li> <li>Store gift cards</li> </ul>
	Yelp Eat24	<ul> <li>App combining food ordering, delivery/pickup and payment using PayPal or Android Pay</li> <li>Filters on reviews, cuisine</li> <li>35,000 restaurants in 1,500 cities</li> </ul>
In-App/invisible	Stripe	<ul> <li>Enables merchants to accept credit cards in browser or in-app channels</li> <li>Optimizes payment flow for consumers via turnkey and customized interfaces</li> <li>Consumers can store payment credentials for one-click use</li> <li>Supports merchant loyalty and offers integration</li> <li>Simplifies process for merchants to accept mobile wallets for payments</li> </ul>
Alternative rails	Dwolla	<ul><li>Enables instant secure payments and transfers</li><li>Does not require consumer enrollment</li></ul>
Р2Р	Venmo	<ul> <li>Allows users to make and share payment with friends</li> <li>Payment to anyone with a Venmo account is instant – funded by Venmo account or linked bank account or debit card</li> <li>Enables in-app payment with select merchants</li> <li>Ability for users to split bills, send gifts</li> <li>Emphasis on social aspects of payment experience – allows users to share on their feed what was paid or purchased, see friends in common</li> </ul>
ı∠r	Zelle	<ul> <li>Partnering with banks to allow users to send money to anyone, using a debit card</li> <li>Integrates into Bank of America's mobile banking app</li> </ul>
	Facebook Messenger	<ul> <li>Users can request, send, and receive money via Messenger</li> <li>Payments are funded by debit card (Mastercard or Visa)</li> <li>Starting to process social commerce transactions</li> </ul>



Wallet Type	Example	Description and Value-Added Services
	Popmoney	<ul> <li>Payments are transferred directly between sender's and recipient's checking accounts</li> </ul>

## 5.2 Consumer Adoption

This section reviews industry reports on consumer adoption of mobile wallets.

#### 5.2.1 What Has Driven Usage?

Industry metrics suggest that consumer usage of mobile wallets only increases when wallets include loyalty benefits, new payment types, and personalization, and improve the shopping experience.<sup>23</sup> For example, Starbucks attributes the rapid growth of its wallet usage to the tie with its popular loyalty program,<sup>24</sup> and saw usage jump nine points with the addition of ordering ahead. Starbucks now reports that 30 percent of its transactions go through its mobile payment app.<sup>25</sup>

Samsung<sup>26</sup> has reported a similar experience. Its Samsung Rewards feature corresponded to a surge in wallet use, with the average number of daily transactions nearly doubling. Samsung also reported that its "power users," those who use the wallet once a day, are doubling every week.

The functions that have been reported to drive adoption include:

- Incorporating loyalty functions
  - Storing and using loyalty cards
  - Presenting offers, deals, discounts, and rewards
- Offering new types of payments
  - o Transit fares
  - Scan and go, eliminating checkout
  - In-app and person-to-person
- Enhancing the shopping experience
  - Advance ordering
  - o Delivery
  - First access to sales
- Personalized recommendations based on customer preferences and history

#### 5.2.2 Industry Forecasts

According to eMarketer, U.S. proximity mobile payment transactions will total \$49.29 billion in 2017, up 78.1% from 2016.<sup>27</sup> Remote smart phone payments totaled \$47.6 billion in 2016, according to Juniper Research.<sup>28</sup> According to research from BetterBuyDesign, PayPal accounts for 56% of the online mobile payments volume (10% from its subsidiary Venmo), and Visa and Masterpass for 38%. Other wallets account for the remaining 6% of payments, \$2.6 billion of which is reported to be attributable to Apple

<sup>&</sup>lt;sup>23</sup> "Mobile wallet adoption depends on understanding four basic needs," PaymentsSource, December, 2016.

<sup>&</sup>lt;sup>24</sup> "<u>Why Is The Starbucks Mobile Payments App So Successful</u>?," Forbes, June 2014.

<sup>&</sup>lt;sup>25</sup> "Mobile payments now account for 30% of Starbucks transactions," GeekWire, July 2017.

<sup>&</sup>lt;sup>26</sup> "Samsung Pay shows how rewards can boost adoption," Business Insider, January 2017.

<sup>&</sup>lt;sup>27</sup> "<u>eMarketer Releases Latest Estimates for US Proximity Mobile Payments</u>," eMarketer, Sept 2017.

<sup>&</sup>lt;sup>28</sup> "<u>War of the Wallets</u>," Juniper Research, April 2017.



Pay. It is estimated that contactless NFC payments made up 58 percent of the dollar volume but only 38 percent of the transactions. Thus, 62 percent of mobile wallet transactions used barcodes or some other technology. Most of the transactions bought coffee, donuts, and fast food.<sup>29</sup>

Usage forecasts have traditionally varied widely. The Financial Brand remains somewhat pessimistic, citing flat usage at 19 percent and predicting that usage will pick up only as consumers see value.<sup>30</sup> Business Insider forecasts a healthy growth rate of 80 percent for the next 5 years but acknowledges that U.S. consumers are still waiting for value added features. Their study found that top features consumers want for mobile wallets were: loyalty cards, coupons, order delivery update and mobile payment via credit card.<sup>31</sup>

### 5.5 Lessons Learned

In the five years since May 2011, when Google announced its NFC wallet, the technologies available to support wallet payments and loyalty and rewards programs have expanded. However, the marketplace for these services has experienced limited growth.

The industry can take some lessons learned from the examples shown below, where degree of success was measured by whether the wallet was ever launched, and the degree of consumer adoption.

Example	Result
Starbucks	<ul> <li>Highest adoption of any U.S. wallet at 30% of transactions<sup>32</sup></li> </ul>
Apple Pay	• 90% of U.S. mobile contactless transactions <sup>33</sup>
Walmart Pay	<ul> <li>In 12 months, achieved adoption nearly surpassing device-centric wallets<sup>34</sup></li> </ul>
Level Up	<ul> <li>100K restaurants, &gt;1M users<sup>35</sup></li> </ul>
CurrentC	<ul> <li>Delayed introduction, shut down after 4 years<sup>36</sup></li> <li>Assets acquired by Chase Pay in 2017<sup>37</sup></li> </ul>
Google Wallet	<ul><li>Phased out, rebranded as Android Pay</li><li>Google Wallet today is P2P only</li></ul>
Softcard	• Shut down after 2 years, acquired by Google <sup>38</sup>

Table 3. Examples of Mobile Wallets Lessons Learned

<sup>29</sup> "Can Mobile Offers Make Mobile Wallets Cool Again?," Steve Mott, Better Buy Design, Payments Summit, March 2017.

<sup>&</sup>lt;sup>30</sup> "<u>US Consumers Won't Change Payment Habits</u>," Financial Brand, December 2016.

<sup>&</sup>lt;sup>31</sup> "Mobile wallets are on fire," Business Insider, March 2017.

<sup>&</sup>lt;sup>32</sup> "Mobile payments now account for 30% of Starbucks transactions as company posts \$5.7B in revenue," GeekWire, July 2017.

<sup>&</sup>lt;sup>33</sup> "<u>Apple Pay adoption is 'underwhelming to date by nearly every objective standard</u>," says Goldman Sachs," Business Insider, August 2017.

<sup>&</sup>lt;sup>34</sup> "What Walmart Pay Knows That Apple Pay Doesn't," PYMNTS.com, August 2017.

<sup>&</sup>lt;sup>35</sup> "Meet Alex Shuck of LevelUp," Boston Voyager, Oct. 2017.

<sup>&</sup>lt;sup>36</sup> "MCX postpones rollout of Apple Pay rival CurrentC, lays off 30, will focus on bank deals," Tech Crunch, May 2016.

<sup>&</sup>lt;sup>37</sup> "JP Morgan Chase buying up MCX technology after Apple Pay competitor CurrentC failed to launch," 9to5Mac, March 2017.

<sup>&</sup>lt;sup>38</sup> Google benefitted by agreement to preload Android Pay on AT&T, Verizon and T-Mobile handsets and access to SmartTap and other technology assets. Google demonstrated its interest in Softcard's SmartTap solution (single NFC tap for payment,



As discussed in Section 3.2.2.2, some merchants have gravitated to QR codes due to ease of implementation, ubiquity and user experience. Merchants have used scanning devices for decades, and POS systems can be configured fairly easily to read QR codes for payment transactions. The Starbucks deployment, in which 30% of total transactions are processed using mobile devices and two-dimensional barcodes, the emergence of QR code standards,<sup>39</sup> and the ubiquitous adoption of QR codes in China and India<sup>40</sup> suggest that these codes will be around for quite a while.

According to a BetterBuyDesign study,<sup>41</sup> security continues to be an impediment to consumer mobile and digital wallet adoption. Another impediment is wallet operability—particularly at brick-and-mortar stores. Tests continue to demonstrate issues with consistent wallet operation, checkout clerk awareness and training, and consumer experience. Most consumers try making payments using their wallets rather than a physical card only when offered an incentive, but, after two or three attempts, many quit using the wallet. Lack of merchant acceptance is also a problem; but perhaps a bigger factor is the proliferation of technologies: consumers wonder what to do in a particular location. Should they tap, for contactless; wave, for NFC; hover, for MST; scan, for QR and barcodes; knock, for wearables; or turn on Bluetooth, for use beyond the checkout lanes?

The complexity of the POS infrastructure can make implementing loyalty and rewards applications timeconsuming and expensive—especially posting discounts from promotions in real time and using rewards "currencies" at checkout. As a result, wallet providers have tended to offer loyalty or rewards components that are typical of the physical checkout world, such as coupons, post-purchase application of points or other rewards currencies, and volume discounts.

Providers are struggling to meet consumers' expectation for real-time rewards redemption.<sup>42</sup> Merchants are constrained by rudimentary back-end integration support for order updating, inventory, and accounting systems. However, emerging technologies such as mobile, cloud, APIs, and open software are paving the way for instant redemption at POS to become common-place.

These lessons learned suggest that next generation mobile or digital wallets may benefit from considering:

- 1. Provision of a consistent level of security that is adequate to address current requirements and scalable to address future threats.
- 2. Interoperability across a diffuse and diverse set of transaction environments (that are also undergoing major changes due to a variety of technology developments).
- 3. Current limitations on more innovative loyalty and rewards programs, to encourage greater consumer acceptance before too many consumers are permanently discouraged by disappointing early experiences.

loyalty and offers) by <u>publicly demonstrating its integration with Android Pay at a Coke vending machine</u>. At the time of the acquisition, SmartTap was available on 20 production models of payment terminals, and was up and running at almost 300,000 merchant locations around the U.S. Google can benefit from the following assets and arrangements it acquired during the deal: wallet design, credential provisioning, and security, merchant relationships and contracts to help jump start Android Pay, agreement by AT&T, Verizon and T-Mobile to pre-load Android Pay on applicable handsets, providing a path forward for Android customers.

<sup>&</sup>lt;sup>39</sup> <u>EMVCo</u>, July 2017.

<sup>&</sup>lt;sup>40</sup> "<u>Developing markets mimic China for QR code digital payments</u>," Global Data, April 2017.

<sup>&</sup>lt;sup>41</sup> BetterBuyDesign, op.cit.

<sup>&</sup>lt;sup>42</sup> "Instant Rewards Redemption at the Point of Sale: Is it Ready for Prime Time?," TSYS, May 2017.



Past successful wallet launches appear to share the following attributes:

- Positive consumer experience and ease of use
- Incentives that drive consumer behavior, such as loyalty rewards and offers
- Making payments recede into the background (make them invisible)
- Confidence in strong security
- Collaboration with industry stakeholders
- Avoiding POS changes and additional fees

Past unsuccessful wallet launches appear to share the following attributes:

- Requiring merchants, particularly large merchants, to change POS hardware or software
- Not collaborating with ecosystem players, such as merchants, banks, and MNOs
- Attempting to monetize data or charge additional fees
- Designing by committee or consortium. While in the past, consortiums have led to major success (i.e., payment networks started as bank-owned associations), this governance model can also lead to delays and lack of decisions.



## **6. Strategic Considerations for Merchants**

The changing mobile landscape and the volatility of wallet providers make it difficult for merchants to know with whom to partner or how to prioritize mobile features and products. When making strategic decisions, important factors include mobile wallet acceptance and its subsequent impact on retail businesses. Acceptance decisions may be different for different retail verticals. For example, petroleum has unique requirements compared to a mass merchant, who has significantly different requirements than a quick service retail merchant. Mobile commerce is not "one size fits all;" what works for one may not work for another.

The potential for increased growth of digital commerce is evidenced by the number of brick and mortar retailers who are introducing or planning to introduce mobile experiences. For example, McDonald's announced that it plans to deploy order and pay capabilities in 20,000 locations around the world by the end of 2017. In addition, McDonald's is offering curbside as a new service model, to increase throughput and improve order accuracy, while considering mobile ordering for table service to drive volume to underutilized in-store capacity.

Domino's and Subway have both announced partnerships with Facebook to enable customers to order and pay using chat bots. Although Subway has been accepting mobile payments for several years at some of its retail locations, chat bots are a new way for customers to engage in digital commerce.

Sam's Club has launched "Scan and Go," which enables customers to scan items using a mobile device. They can shop, check out, and pay on the mobile app, skipping the checkout line.

Waze and Dunkin' Donuts have partnered to enable mobile ordering with payment for pick up at the Dunkin' Donuts location closest to the consumer.

Consumer expectations for commerce continue to change, and merchants are finding new ways to meet those demands. How to meet expectations using basic mobile commerce is quickly becoming an essential consideration in retailer payment acceptance strategies and plans. Considerations include the following:

- Consumer experience and adoption
- Product features and roadmaps
- Data management
- Acceptance terms
- Costs and ROI
- Technology

#### 6.1 Customer Experience and Adoption

Various considerations can help merchants define their strategies for mobile commerce. These include identifying the specific problem a mobile payment solution will solve and how (and whether) the mobile payment solution will support the commerce experience seamlessly. Some questions to consider are:

• Is the experience to be about payment only, or is payment intended to be complimentary to other customer engagement levers, such as offers or deals, loyalty, access to information (e.g.,



grocery lists, product costs, receipts, returns, warranties), or even awareness of the environmental or sustainable efforts a merchant supports?

- What opportunities does the payment solution offer for integration into other platforms, such as loyalty, offers and promotions, or customer profile databases?
- What are the channels through which the customer can access the mobile payment product and how does that fit into the experience?

For example, a retailer who offers a mobile in-app payment may prefer to enable that same payment alternative through an in-store kiosk to maintain a consistent customer experience across channels.

• How much control or influence will the merchant have over the customer experience?

Analysis of the customer experience can identify points that could be improved by changing the experience. However, to change the experience, merchants have to be able to control or influence the enhancements. Proprietary mobile solutions typically offer more control over the customer experience. In addition, proprietary wallets often leverage existing customer/merchant relationships and inherent trust, which may be more successful in promoting adoption. The open wallet model may result in many merchants participating in the acceptance, but the consumer must develop trust in the wallet provider.

• What are the current enrollment and use (penetration and demographics, by industry vertical) of a mobile payment alternative?

This information helps a merchant evaluate relevance and potential impact of a mobile payment solution on its customer base.

#### 6.2 Product Features and Roadmap

The products and features of a mobile payment solution should complement the experience a merchant is trying to create. Considerations include:

- What payment methods to support. Some third-party payment applications support only credit or debit card products. If support for closed loop gift cards, ACH, or private label products is required, such solutions may not be a good fit.
- Whether loyalty is supported. Some solutions may offer loyalty as part of the platform. If so, consider whether the solution is flexible and suitable, and whether it can be integrated into an existing loyalty platform.
- Whether features are available that attract the merchant's targeted consumer. For example, if millennials make up a significant percentage of the customer base, a split payment feature would fit well, given that millennials are primary users of P2P payments.
- Whether features are available that solve a consumer experience issue. For example, capabilities that support streamlining the redemption of loyalty, rewards, or offers with payments in a single scan and supply a new offer for the next visit could improve the overall experience.
- What technology is required to support a solution. Certain technologies may require additional hardware and software integration development, deployment, and training.



What the solution roadmap is. Considerations include potential technology partnerships and
risk factors. It is also important to understand whether the feature roadmap is expected to
evolve and by how much. Also evaluate whether the provider is likely to support specific
merchant business strategies, and calculate the ROI on the investment required for
development or integration, considering the longevity of the solution provider.

### 6.3 Data Management

Merchants are on the front lines of the retail experience and customer relationships. Therefore, merchants need to understand how much and what kind of data is passed by a mobile or digital payment solution. Merchants need to manage data security concerns and protect against negative brand exposure or financial loss, including preventing fraudulent provisioning of accounts and protecting sensitive cardholder data. For this reason, merchants have a strong incentive to understand how the mobile payment solution provisions, uses, and stores consumer payment information. Some considerations are:

- Where cardholder payment information is stored (including data at rest) and whether transmitted data is secured adequately in accordance with data security standards.
- Whether tokenization and encryption product solutions are available to protect the PAN and other personally identifiable data in transit and at rest.
- How the choice of technology or the use of in-app wallets or specific cardholder verification methods (CVMs, including biometric CVM or on-device CVM) affect the processing environment, routing choice, authentication decisions, declines, liability, and customer experience.

For example, debit networks may not have business relationships in place that are able to process and route biometric and on-device CVMs, resulting in potential declines.

• Whether the data in the mobile application includes only cardholder payment data or also passes loyalty information, basket/product mix, or other information.

The business terms governing the collection, use, and management of data are critically important to the merchant to ensure preservation of customer relationships and acceptable use by any third parties involved in the mobile payment transaction. Merchants should endeavor to understand these terms.

Merchants should consider implementing the practices outlined in ISO12812, Mobile Payments.<sup>43</sup> Part 2 and Part 3 are particularly relevant, as they discuss application and life cycle management, provisioning, security, and data protection.

### 6.4 Acceptance Terms

It is critical that merchants review and understand the acceptance terms and associated payment network rules governing any mobile payment solution they implement. These terms are binding, should be reviewed with appropriate professional advisors, and may have significant implications for costs, security, risk, data use, and operational matters, such as what mobile payment solutions can be accepted and how they perform in terms of up time, use, conversion, and related criteria. Among other

<sup>&</sup>lt;sup>43</sup> "ISO/TS 12812-2:2017, Core banking -- Mobile financial services -- Part 2: Security and data protection for mobile financial services," and "ISO/TS 12812-3:2017, Core banking -- Mobile financial services -- Part 3: Financial application lifecycle management."



things, merchants considering whether to enable NFC or contactless payments should be aware that once NFC/contactless transactions are accepted at the POS:

- Merchants may not be able to have direct contractual relationships with individual mobile wallet providers.
- Merchants may not be able to distinguish or select among, or reject transactions from, particular wallets or wallet providers. (There is currently no standard wallet identifier enabling merchants to differentiate transactions by wallet provider.) This can potentially impact merchant customer service and promotions.
- Merchants may not know how the data collected by a wallet in connection with an NFC mobile transaction is used or shared.

### 6.5 Financial Considerations

Financial considerations about whether to implement or accept a mobile solution include:

- **One-time implementation costs**. Implementation costs can include software development, software and hardware deployment, training, and promotion.
- **Ongoing costs**. Ongoing costs can include maintenance, hosting costs, licensing costs, and transaction fees.
- **Transaction fees for CNP transactions**. Many mobile payments other than contactless are classified by the payment networks as CNP transactions and transaction fees are generally higher than for standard card present transactions.
- **Fraud liability**. In a CNP transaction, the merchant is typically liable for any fraud. If the merchant uses 3DS, fraud risk is transferred to the issuer. However, merchants must balance any effects on the customer experience and conversion rates with reduced fraud risk. Note that 3DS 2.0 is expected to address issues customers experienced with the initial release of 3DS.

Mobile technology now has authentication tools and access to data points (e.g., device ID, geolocation, biometrics) that can significantly improve fraud mitigation if used effectively. By leveraging these tools, merchants can improve their customer authentication decisions and better manage risk. However, any fraud that does occur will predominantly be passed on to the merchant in the form of chargebacks. Effective fraud mitigation efforts and chargeback management require a combination of staff and tools. Although more alternative fraud mitigation and prevention practices are available in the digital space, they require merchants to incur additional investment costs and deal with ongoing risk considerations.

- **Mix of credit and debit transactions**. Another consideration is that a merchant's mix of credit and debit payments may be different for digital transactions as opposed to customer-present transactions, with corresponding cost implications because credit and debit transaction fees are different. In addition, merchant choice of debit transaction routing may be impacted by network payment tokenization and the digital channel.
- Alternative payment methods in the transaction mix. If a significant percentage of current (non-mobile) transactions originate from alternative payment methods, such as ACH, closed loop, or private label, consider whether these transaction types are available in a mobile



payment product. Switching from those lower cost customer payment types may result in higher costs.

• **Cost reduction potential**. Another consideration is whether merchant costs can be reduced by a digital solution. For example, eliminating ticketing and related paper production costs for industries such as transit or for paper gift certificates may increase the ROI of implementing a mobile payment solution.

In the end, merchants have to evaluate the opportunity to drive incremental sales lift as a result of digital payment acceptance in the context of potential costs and cost savings.

### 6.6 Technology Considerations

As new mobile payment solutions enter the market, merchants may struggle to implement new solutions quickly because of development lead times, technology requirements, and competing IT priorities.

One solution is white label alternatives, which may offer faster times to market than in-house development. However, white label solutions may be less flexible and provide less control over the customer experience. In addition, it may be more difficult for white label providers to integrate with inventory management and fulfillment systems, which are critical to enabling a positive mobile shopping experience.

In addition, mobile payment technologies need to integrate with current fraud prevention tools and practices. Fraud prevention for mobile commerce payments provides new data fields and behavioral analytics that can be leveraged to help authenticate customers and avoid decreasing legitimate customer purchases.

When additional hardware or software (or both) are required to support a payment solution, an important consideration is integration into the current POS platform, tokenization solution, customer database, and debit routing solution. Some merchants may be able to save time by requiring the use of industry standards. For example, a petroleum merchant may desire adherence to the Conexxus Mobile Payments Standard, which provides the messaging needed for a mobile application to communicate with on-site systems for dispenser control.

Multiple technologies are available for in-store mobile payments, each of which raises different hardware, operational, and other business considerations.

Some merchants have approached their acceptance strategy for NFC-enabled payment products as a way to satisfy all customers and their preferences for these various wallet providers. However, merchants should evaluate NFC/contactless carefully before enabling it:

- NFC may require additional terminal hardware or software. EMV migration provided an opportunity for hardware/terminal providers to incorporate EMV contactless acceptance into merchant terminals, but merchants must activate this capability.
- NFC acceptance does not currently enable merchants to select which wallet to accept. There is no standard identifier or protocol (such as a wallet ID) that supports acceptance selection.
- How the wallet provider is using data may not be clear, as there may not be a contractual relationship between the merchant and the mobile NFC wallet provider.



• EMV contactless development involves additional considerations to ensure that debit routing alternatives remain intact and also involves certification challenges, which may add to deployment timelines.

Other technologies also have their drawbacks. QR or bar code payments require scanners, which may not be traditional within certain industry verticals. Significant testing in different environments is critical for mobile payment technologies that require scanners. For example, external scanners may face environmental challenges (e.g., temperature, glare).

Bluetooth Low Energy (BLE) requires hardware for beacon support, and customers must have Bluetooth activated or at least available in the background. In addition, where Bluetooth beacons are located is critical to a positive in-store consumer experience.

Merchant-specific payment codes probably do not require additional hardware. However, their use requires an exchange with a cashier or attendant to execute a mobile transaction, or the customer must use an unattended terminal. Payment codes can offer an additional level of identification, to ensure that the consumer is at the correct terminal or to provide a backup if the technology fails (e.g., no GPS or Bluetooth, or the application crashes). However, codes can result in data entry errors, which turns a digital transaction back into a physical transaction.



# 7. Strategic Considerations for Financial Institutions

Issuers must take multiple considerations into account when developing a mobile wallet strategy. Such considerations include the technical development effort involved, wallet security, and wallet-specific issues. These considerations must then be evaluated based on the type of wallet solution (i.e., third-party wallet, integrated wallet app, or standalone wallet app). Issuers may also wish to consider whether to pursue a wallet strategy at all.

Certain wallet models (network-centric, merchant-centric, in-app/invisible) may use an issuer's cards without requiring the issuer to consent or perform any technical development. However, certain use cases may require an issuer's explicit participation and technical development (e.g., enabling cards for use at a POS in the Masterpass by Mastercard wallet). Issuers can usually choose which wallets they will enable and grant proximity access to cardholder account data. Issuers may choose to market these wallets in addition to solutions in which they actively participate.

#### 7.1 Third-Party Wallets

Once an issuer has decided to embark on a strategy that includes third-party wallets, the logical next step is to select the wallets. Two questions are key:

- 1. Should an issuer support all major third-party wallets (e.g., Apple Pay, Samsung Pay, Android Pay) or only certain ones?
- 2. Should supporting third-party wallets be part of a brand-centric strategy or be the only means of participation in a mobile wallet solution?

The answer to the first question is critical—it determines the extent to which issuers reach and support their customer base. Frequently, issuers choose to enable more than one wallet, to optimize consumer reach and because of the device and operating system limitations associated with different third-party wallets.

The answer to the second question is a matter of issuer choice. For some issuers, participation in thirdparty wallets can accelerate their entry into the mobile wallet space, enabling consumer choice while they work on developing their own branded integrated mobile wallet solution.

Third-party wallet support involves only minimal technical considerations for issuers. Issuers need to work with their processors and payment networks to tokenize the account ranges associated with cards to be added to a mobile wallet. In coordination with the payment network or token provider, the processor then takes the actions necessary to enable the issuer's cards. When an issuer's account ranges are supported by multiple processors or reside on multiple platforms, incremental technical development is likely.

Additional technical development may be required to support an issuer's chosen authentication strategy or integration with back-end systems. Depending on which methods an issuer uses for ID&V (issuer mobile application, one-time passcode), more development work may be required to enable back-end system integration.

When considering device-centric wallets, issuers must also consider how they will mitigate risks associated with consumer authentication. Third-party mobile wallets provide data elements that enable issuers to make eligibility decisions on digitization. This information can be used to facilitate ID&V.



Issuers are responsible for designing their own policies and processes for ID&V, leveraging whatever methods are supported or required by a wallet provider. Some wallets, such as Android Pay, require an issuer to support multiple methods of ID&V and present them to users.

Some wallets also offer issuers the ability to initiate card provisioning directly from their own mobile banking applications. This functionality enables an issuer to perform user ID&V within their own mobile banking application, with this step also accomplishing user ID&V for the wallet application.

Device access is another important security consideration for issuers. Device-centric wallets typically rely on security safeguards that are already incorporated into the device (such as biometric authentication, PIN or passcode entry). Many of these security methods are also used for validation at payment in accordance with the standards determined by the wallet provider. Some wallets always require a user to validate at payment, while others do not require this step if the device is unlocked.

#### 7.2 Beyond Third-Party Wallets

When looking beyond third-party wallet solutions, issuers should weigh the importance of having a mobile wallet solution over which they can have greater influence. Research has shown that the majority of consumers would prefer to have a mobile wallet solution from their banking institution.<sup>44</sup> By relying solely on third parties to provide a mobile wallet solution, issuers risk disintermediation and relinquish control over the consumer relationship.

Issuers who choose to pursue the development of their own mobile wallet solution as an accompaniment to third-party wallets should take care to ensure that the message to their cardholders is clear, in order to avoid confusion.

#### 7.2.1 Mobile Banking with an Integrated Wallet

Issuers who enable a solution in addition to third-party wallets—particularly one that integrates with their mobile banking platform—can typically influence the user experience directly while incorporating value-added services. For example, a mobile wallet integrated with a mobile banking platform can provide users with real-time account balances and account management functions and the ability to select and establish wallet preferences. Such a wallet could also include loyalty, offers, and other value-added services to enhance the overall consumer experience, which could drive wallet use.

When considering whether to integrate a wallet into their mobile banking platforms, issuers must decide whether to build the wallet capability themselves or adopt a solution from a third-party provider. Additional considerations include which device operating systems to support and which technology to leverage. Such considerations can significantly influence consumer adoption. Issuers must also ensure that their processor is able to support the wallet solution, particularly if integration with a third-party provider is required.

As with third-party wallets, security is an issue. Issuers must still consider how to mitigate the risks associated with cardholder ID&V. Here issuers may have an advantage in terms of their ability to leverage readily available information about their cardholders for purposes of ID&V at provisioning as well as at payment. Issuers will also need to ensure that adequate device access security is in place to prevent unauthorized transactions.

<sup>&</sup>lt;sup>44</sup> Mastercard Online Omnibus study, February 2017



The payment networks' solution-approval processes provide guidance on integration with mobile banking applications.

#### 7.2.2 Separate Mobile Wallet App

Some issuers may decide that it is better to enable a standalone wallet application than integrate wallet functionality into a current mobile banking application.

Consumers are growing accustomed to having separate applications from their issuing institutions, so a standalone mobile wallet application would be aligned with market trends without negatively impacting consumer adoption. Likewise, a standalone wallet application affords an issuer flexibility in making modifications and testing different strategies without risking impact to the more critical mobile banking application.

When considering whether to create a standalone wallet application, issuers must decide whether to build the wallet capability themselves or adopt a solution from a third-party provider. Additional considerations include which device operating systems to support and which technology to leverage. Such considerations can significantly influence consumer adoption. Issuers must also ensure that their processor is able to support the wallet solution, particularly if integration with a third-party provider is required.

Issuers must also consider how they will mitigate the risks associated with cardholder authentication and ensure proper levels of device security.

#### 7.3 No Mobile Wallet Strategy

For some issuers, not having an explicit mobile wallet strategy may be a viable strategy, at least temporarily. If technical or financial resources are constrained, it may make sense to postpone a decision until the situation improves or until the issuer can quantify the ROI expected for participation in the mobile wallet space. These issuers must weigh the benefits of participation against the opportunity costs of waiting.



# 8. Conclusions

The objective of this white paper is to provide information about and guidance for stakeholders regarding the rapidly changing mobile and digital wallet landscape. The white paper describes five wallet models (device-centric mobile proximity, device-centric mobile in-app, card-not-present card-on-file, QR code, and digital checkout), and typical wallet specifications, including interaction methods, credential storage, and tokenization. Eight types of wallets are identified, including bank-, MNO-, device-, merchant-, and payment network-centric, in-app, alternative, and P2P. The most prevalent technologies are reviewed, including NFC, HCE, TEE and MST, and check-out processes for QR code, and the benefits and challenges for QR codes are discussed. The evolving wallet landscape introduces new roles, including those fulfilling security and credential provisioning, such as TSPs and trusted service managers (TSMs).

Security is a critical consideration for any payment technology, and NFC security is discussed, both embedded in an SE or with HCE and TEE. The role of tokenization is described, as is the criticality of the identity verification and customer authentication processes.

The paper surveys wallet history, citing examples for each of the wallet types and identifying some of the factors that may have helped drive or impair adoption and usage. Because adoption is often driven by additional value-added features, such as order-ahead, the features that wallet providers are offering are described. Forecasts of future adoption and trends, such as social payments and "invisible" payments, are highlighted.

Various strategic considerations for merchants are listed, including the unique requirements of verticals such as petroleum vs. quick service vs. mass merchant. Merchants are advised to consider their wallet strategy within the context of the desired overall customer experience, addressing their particular challenges. Merchants will want to think about payment methods to support, loyalty programs, how to streamline check-out, technology to deploy, training, and a solution roadmap. They should also consider the management and protection of data, including secure provisioning of payment credentials, tokenization, CVMs and network support for biometrics, and potential for sharing customer information with third-party providers. Merchants will want to consider their payment acceptance terms, including NFC/contactless, and ROI for the mobile solution. When considering deployment, merchants will make tradeoffs between time to market and complexity when reviewing white label alternative technologies to deploy and industry standards.

Financial institutions can choose between participating in one or more of the device-centric wallets or deploying a bank-branded solution, either as part of the bank's mobile banking app or as a separate payment app. Participation in any wallet requires identification and verification, consumer authentication processes, and some integration with back-end systems. For some banks, a logical choice might be to hold off on any wallet strategy until they see how the industry evolves.



# 9. Legal Notice

This document is intended solely as a convenience to its readers, for purposes of providing interested payments industry stakeholders with an understanding of the rapidly changing mobile and digital wallet landscape. While great effort has been made to ensure that the information in this document is accurate as of the original date of publication, nothing herein constitutes legal or business advice or should be relied on for any purpose. All warranties of any kind regarding the information herein are disclaimed, including all warranties relating to or arising in connection with the use of or reliance on the information set forth herein. Any person that uses or otherwise relies in any manner on the information set forth herein does so at his or her sole risk.

References in this document to any specific stakeholder, product or service, or the use of any of the foregoing, are solely for the information and convenience of its readers, and do not constitute an endorsement or recommendation of any kind.

Note that payment industry rules, requirements, policies and procedures are complex, are subject to change, and may impact or be impacted by the specific facts, circumstances or decisions of a given product, solution or implementation. Prior to implementation of any product, solution or strategy, merchants, issuers, acquirers, processors and others are therefore strongly encouraged to consult with appropriate business, legal, professional and technology advisors, including payment networks and acquirers, regarding applicable industry and legal rules, requirements, policies and procedures.



# **10.** Appendix A: Glossary

Term	Definition
3DS	See Three-Domain Secure.
A2A	Account to Account.
ACH	Automated Clearing House, an electronic network for U.S. financial transactions. Processes large volumes of credit push and debit pull payment transactions in batches.
Address Verification Service (AVS)	A service offered by the payment networks to allow a merchant to validate all or a portion of the address provided by the cardholder during an authorization.
Authentication	<ul> <li>There are different types of payment authentication dealing with the card, the customer, and the device. For purposes of this paper, authentication refers to the customer, and is defined as the process used to verify the identity of the party enrolling in a wallet or initiating a payment transaction, using different types of credentials to prove the person is who he claims to be. Authentication methods include: <ul> <li>Something you are (signature, voice, other biometrics)</li> <li>Something you know (password, challenge question/answer)</li> <li>Something you have (payment card, mobile phone)</li> </ul> </li> </ul>
Card on File (CoF)	Payment credentials provided by the cardholder to a merchant with the authorization to use the stored "card on file" credentials for future payments (for individual or recurring payments).
Card Not Present (CNP)	Payment card transaction where the cardholder does not present the card for merchant examination at the time of purchase, such as a mail-order transaction or a purchase made over the telephone or Internet.
Card Security Code	A value encoded in the discretionary portion of track data that provides the card issuer with the ability to perform a cryptographic check on the contents of the track. Called card security code (CSC) by American Express, card verification code (CVC) by Mastercard, card verification value (CVV) by Visa, and card identifier (CID) by Discover.
Cloud	Cloud computing (not specific to mobile payments) is the use of shared hardware and software resources that are delivered as a service over a network (typically the Internet). Data and software are retrieved from remote servers using web-based tools and applications.
CSR	Customer Service Representative.
EMV	EMV is a set of specifications for smart card payments and acceptance devices developed to define a set of requirements to ensure interoperability between chip-based payment cards and terminals. EMV chip cards contain embedded microprocessors that provide strong transaction security features and other application capabilities not possible with traditional magnetic stripe cards. EMVCo manages, maintains and enhances the specifications, is owned by American Express, Discover, JCB, Mastercard, UnionPay and Visa, and includes other organizations from the payments industry participating as technical and business associates. See <a href="http://www.emvco.com">http://www.emvco.com</a> .
Encryption	Encryption mitigates fraud during a mobile payment transaction by converting payment data into a form unintelligible to everyone except holders of a unique cryptographic key and



Term	Definition
	is an important component of the secure element. Cryptographic keys determine the output of an encryption algorithm when transforming plain text to encrypted text. Key rotation is the process of decrypting data with the old encryption key and re-keying the data with the new encryption key. Encryption protects consumer and transaction-level information against unauthorized access or disclosure, from the initial encryption step to the decryption step. Encryption can protect data during transmission and while at rest.
Host Card Emulation (HCE)	A mechanism for an application running on the "host" processor (the mobile device's main processor–where most consumer applications run) to perform Internet based in-app and card-present NFC payment transactions.
ID&V	Identity and Verification. The " <i>EMV</i> <sup>®</sup> <i>Payment Tokenization Specification – Technical Framework</i> " describes ID&V as a set of functionalities and services that allow for a trusted association of the payment token to the PAN for an authorized cardholder. EMV ID&V validates the cardholder and the cardholder's account to establish a confidence level that the payment token is bound to a PAN. Examples of ID&V methods include account verification messages, PAN-based risk score assessments, and one-time passwords issued by the card issuer or its agent to verify the cardholder. Additional information can be found at: <u>https://www.emvco.com/emv-technologies/payment-tokenisation/</u>
In-app Payment	A mobile app that allows users to purchase goods and services directly from within a merchant native mobile app using a mobile wallet that has been provisioned with an EMV payment token (e.g., Apple Pay, Android Pay, Samsung Pay). To make a purchase, the consumer selects the mobile wallet icon within the merchant app and authorizes the transaction with a fingerprint, PIN, or passcode.
iOS	iPhone Operating System.
Knowledge Based Authentication (KBA)	A method of authentication which seeks to prove the identity of someone accessing a service, such as a financial institution or website. As the name suggests, KBA requires the knowledge of private information of the individual to prove that the person providing the identity information is the owner of the identity.
Magnetic Secure Transmission (MST)	Magnetic Secure Transmission and Wireless Magnetic Communication (WMC) are technologies from Samsung and LG respectively that generate magnetic data pulses to communicate over the air with magnetic stripe card readers, enabling these devices to make payments at POS devices that do not have a contactless interface.
MFA	See Multi-Factor Authentication.
Mobile Network Operator (MNO)	A wireless service provider that offers wireless communication services to end users.
MST	See Magnetic Secure Transmission.
Multi-Factor Authentication (MFA)	A method of access control in which a user is granted access only after successfully presenting multiple separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are).
Near Field Communication (NFC)	A set of standards that enables proximity-based communication between consumer electronic devices such as mobile phones, tablets, personal computers or wearable devices. An NFC-enabled mobile device can communicate with a POS system that currently accepts contactless payment cards.



Term	Definition
One Time Password (OTP)	Passwords that are used once and then discarded. One-time passwords are often delivered to the user via one of the following methods: text or e-mail, display card, or RSA token.
ООВА	See Out-of-Band Authentication.
Operating System (OS)	The software that supports a computer or mobile device's basic functions.
Original Credit Transaction (OCT)	A Visa term to describe a transaction where funds are sent to a Visa card account.
Out-of-Band Authentication (OOBA)	Cardholder verification thru a different channel than the payment. One example is a code sent via text message that is input on a website to complete a payment.
Payment Service Provider (PSP)	Non-bank service providers (e.g., providers of technology, software, network services, processing services, mobile wallets, equipment, security services, and program managers).
Person to Person (P2P) Payment	An online technology that allows customers to transfer funds from their bank account or credit card to another individual's account via the Internet or a mobile phone.
Point of Sale (POS)	The device (hardware and software) that is used to process transactions at the merchant location. While POS once referred specifically to the credit card terminal at the cash register, POS now includes mobile, wireless, and virtual terminals.
Primary Account Number (PAN)	The 14- to 19-digit number that appears on the account holder's payment card.
Quick Response (QR) Code	A type of 2-D (matrix) bar code that complies to ISO 18004:2006.
Radio- Frequency Identification (RFID)	Technology that is used to transmit information about objects wirelessly, using radio waves. Systems that use RFID technology are composed of two main pieces: the device that contains the data and the reader that captures such data.
Risk Based Authentication (RBA)	A non-static authentication system which takes into account the profile of the agent requesting access to the system to determine the risk profile associated with that transaction. The risk profile is then used to determine the complexity of the challenge.
Secure Element (SE)	A tamper-resistant chip that can securely host multiple applications and cryptographic data, such as keys, in a smart phone, following robust security requirements set forth by standards bodies. The SE resides in a microcontroller chip capable of performing cryptographic operations. The SE contains a dedicated microprocessor with an operating system, memory, an application environment, and security protocols. The SE is used to store and execute sensitive applications, such as payment applications, safely on a mobile device and to store associated payment credentials and financial data. If tampered with, it may self-destruct, and not allow unauthorized access.
Three-Domain Secure (3DS)	A messaging protocol to enable consumers to authenticate themselves with their card issuer when making card-not present (CNP) e-commerce purchase.



Term	Definition
Token Service Provider (TSP)	Entity within the payments ecosystem that provides registered token requestors with 'surrogate' PAN values, otherwise known as payment tokens by managing the operation and maintenance of the token vault, deployment of security measures and controls, and registration process of allowed token requestors. The <i>EMV tokenization specification</i> defines a token service provider as "an entity that provides a token service comprised of the token vault and related processing.
Trusted Execution Environment (TEE)	A secure area of the main processor in a mobile phone that stores, processes, and protects sensitive data in an isolated and trusted environment running alongside the smartphone operating system (OS), using trusted security software. Applications that run in the TEE provide end-to-end security by enforcing protection, confidentiality, integrity, and data access rights. The trusted applications access security resources and services, including cryptography, secure storage, trusted user interfaces and SE interfaces through TEE application APIs, which allow applications in the normal OS and application environment to access and exchange data with a trusted application running inside the TEE. The TEE comprises hardware and software components that make is more secure than the mobile OS. Because it is isolated from the OS and its applications, it is also protected from being compromised if the OS is rooted.
Trusted Service Manager (TSM)	A neutral third party that provides a single integration point to mobile operators for financial institutions, transit authorities and retailers that want to provide a payment, ticketing or loyalty application to their customers with NFC-enabled phones.
тѕр	See Token Service Provider.
Wallet Service Provider	Companies that offer specific wallet solutions that use various communications technology for mobile payments.
Wireless Magnetic Communication (WMC)	Similar to MST, a process that allows a portable device to generate wireless magnetic data pulses that can be used to transmit card data to a POS terminal's magnetic stripe reader.



### **11.** Appendix B: Stakeholders

The ecosystem of mobile and digital wallets includes a number of new stakeholders who fill roles that are not required with card-based payments:

• Wallet owner. The entity providing the payment wallet that is accessed through a cardholder's mobile device or housed in a merchant's website shopping cart.

Wallet owners are typically merchants, issuers, mobile device manufacturers, mobile device operating system owners, or a payment network. The wallet owner allows a cardholder to store payment card credentials in the wallet to process payments or transfer funds.

- Wallet acceptors. The merchant or other entity that accepts payments from a wallet.
- Token service provider (TSP). The entity that manages the life cycle of a token. Additional services typically include:
  - Creating and storing tokens
  - Managing the token lifecycle
  - Processing token transactions
  - Performing token-to-PAN mapping
  - o Cardholder validation, including provisioning services
  - Key management for device-based wallets using HCE
  - Verification services for transaction and device validity, including cryptographic validation and domain control restrictions
- Trusted service manager (TSM). The entity that connects service providers (such as issuing banks, token vaults, and merchants) and the party that controls the mobile payment device or mobile device operating system.

The TSM facilitates provisioning and managing secure items that are sent to the mobile device such as tokens and keys.



## 12. Appendix C: Standards

Standards facilitate interoperability between devices and entities by using prescriptive language to outline a process, describe a physical interface, or provide message interfaces for exchanging data and information. Standards eliminate the need to implement multiple protocols, reducing complexity. The result is reduced cost of development, maintenance, and validation, as well as increased opportunity for innovation.

Several standards bodies are doing work that targets mobile payment solutions.

The International Organization for Standardization (ISO) is a worldwide federation of national standards bodies that rely on ISO technical committees to create standards. ISO 12812 is a five-part document that describes the requirements and implementation recommendations for mobile payments and focuses on the development of mobile financial services applications. Part 1, "General Framework," includes definitions and terms and provides an overview of what expectations the standard has for mobile financial service implementations, regardless of the type of application (e.g., local to device, remote cloud-based). Part 2, "Security and Data Protection," provides requirements and recommendations for a framework to manage the security of mobile financial services as well as considerations for securing mobile financial applications (e.g., remote management, protection of sensitive data, consumer rights, customer education, customer enrollment, application download and deactivation). Part 3, "Financial Application Lifecycle Management," addresses lifecycle considerations, including roles and infrastructure for secure provisioning, credential authentication, terms of service, customer relationship, new features, and updates. Part 4, "Mobile Payments to Persons," and Part 5, "Mobile Payments to Businesses," present use cases, including for the use of mobile wallets, and requirements for interoperability. X9, the ANSI-accredited standards body for the financial services industry in the U.S., has begun work on the adoption of ISO 12812 as a U.S. national standard.

The World Wide Web Consortium (W3C) is an international community that develops open standards to ensure the long-term growth of the Web. W3C interest groups and community groups focus on Web payments and commerce. The initial offerings from W3C are specifications for a Payment Request API and a Payment Handler API (both nearing completion,) which support a variety of devices and technologies (e.g., mobile devices, automobiles, televisions, and virtual reality interfaces). The Payment Handler API specifically addresses key points for interfacing with payment information owned by a user (the wallet). Ongoing work addresses standards important to commerce, including digital offers (such as coupons or loyalty) and additional aspects of payment flow, including initiation of payment, recurring payments, receipts, and refunds. The W3C standardization efforts take into account emerging regulations, fraud reduction, and harmonization with other standards.

Conexxus is a trade association for the convenience and retail-fuels industry that creates standards specifically for that industry. The Conexxus *Mobile Payment Specification*<sup>45</sup> defines a standard interface for messages between site systems (POS, electronic payment server, forecourt device controller) and a mobile payment processing application to enable forecourt purchases and in-store transactions using a mobile device (smartphone, tablet, connected car). The specification provides a solution for common use cases (e.g., pay for merchandise inside, pre-pay for fuel inside (with or without additional merchandise), pay at the pump, buy a car wash outside) and supports loyalty functionality. The specification covers site-level processing (i.e., using current payment and/or loyalty rails) and above-site

<sup>45</sup> Conexxus web site



processing (i.e., the mobile payment processor interfaces directly with the payment and/or loyalty host), and provides messages to the site systems that control site specific functionality (pump authorization, car wash code generation). To provide flexibility, the way payments and loyalty are processed can be different. For example, loyalty can be processed above site while payment is processed at site level.

EMVCo facilitates worldwide interoperability and acceptance of secure payment transactions. Supported by dozens of banks, merchants, processors, vendors, and other industry stakeholders, EMVCo manages and revises the EMV specifications and related testing processes, including card and terminal evaluation, security evaluation, and management of interoperability issues. In July 2017, EMVCo released a two QR code specifications for payment systems.

- The EMV Consumer-Presented Mode specification<sup>46</sup> is compatible with EMV payment tokenization. The QR code payload consists of any payment token credentials already provisioned to the mobile device, which the consumer uses to make purchases. The consumer selects the QR option for payment within the mobile app, which displays a QR code to be scanned at the merchant terminal to complete the transaction.
- 2. The second specification is for the EMV Merchant-Presented Mode.<sup>47</sup> Consumers use a mobile app that can scan an EMV merchant-presented QR code and initiate a payment transaction. The mobile app may be a mobile banking app offered by an issuer or a third party. In either case, the request to process the payment transaction is ultimately directed to the issuer managing the account from which the funds will be withdrawn. Merchant QR codes can be static or dynamic.

<sup>&</sup>lt;sup>46</sup> "EMVCo QR Code Specification for Payment Systems: Consumer Presented Mode," Version 1.0, EMVCo, July 31, 2017.

<sup>&</sup>lt;sup>47</sup> "EMVCo QR Code Specification for Payment Systems: Merchant-Presented Mode," Version 1.0, EMVCo, July 31, 2017.



### 13. Appendix D: Project Team

Publication of this document by the U.S. Payments Forum does not imply the endorsement of any of the member organizations of the Forum.

The following members participated in the project team developing this white paper.

- Bharath Balasubramanian, American Express
- Deborah Baxley, PayGility Advisors
- Jenna Birch, CMS Payment Intelligence
- Bill Bondar, PNC Bank
- Charl Botes, Mastercard
- Steven Cole, Vantiv
- Marianne Crowe, Federal Reserve Bank of Boston
- Brady Cullimore, American Express
- Marie Doloc, Arroweye Solutions
- Melanie Gluck, Mastercard
- Amanda Guillen, Discover Financial Services
- Anne Hagen, Wells Fargo
- Nicole Jackson, TD Bank NA
- Farzad Janfaza, Chevron
- Sarah Hartman, TSYS
- Smrithi Konanur, Hewlett Packard Enterprise
- Eric Kuhn, FIS Global
- Christine Lopez, Vantiv
- Josh Martiesian, Metropolitan Transit Authority
- Scott McArthur, Walgreens
- Deirdre McGill, Metropolitan Transit Authority
- Diana Molitor, FIS Global
- Jackie Moore, Mastercard
- Steve Mott, BetterBuyDesign
- Bill Pitterle, Toshiba GCS
- Rod Reef, Reef Karson Consulting
- George Rice, Hewlett Packard Enterprise
- Todd Smith, Heartland Payment Systems
- Mateen Syed, Discover Financial Services
- Linda Toth, Conexxus
- Laura Townsend, Merchant Advisory Group
- Ahmet Urtan, First Data
- Clyde Van Blarcum, American Express
- Allan Whittemore, American Express