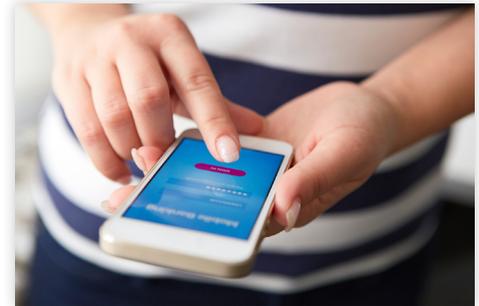


GUIDE



Mobile Wallets 101

By Robin Arnfield
Contributing writer, Mobile Payments Today



DEVELOPED & PUBLISHED BY:

mobile
paymentstoday
.com

SPONSORED BY:


CardLinX[™]
www.cardlinx.org



CONTENTS

Page 3	Executive Summary
Page 4	Chapter 1 Introduction
Page 7	Chapter 2 How mobile wallets work
Page 9	Chapter 3 Mobile wallet advantages
Page 13	Chapter 4 Security issues
Page 16	Chapter 5 Profiles of mobile wallet providers
Page 22	References

Published by Networld Media Group

© 2015 Networld Media Group

Written by **Robin Arnfield**, contributing writer,
MobilePaymentsToday.com.

Tom Harper, president and CEO

Kathy Doyle, executive vice president and publisher

Will Hernandez, editor

Brittany Warren, custom content editor

This report provides U.S. retailers and restaurant operators with an introduction to mobile wallets, and explains why they should accept mobile proximity/point-of-sale payments through their own mobile app, through financial institution-issued mobile wallets, and through third-party mobile wallets.

The report explains the essential features of point-of-sale mobile wallets, who the key mobile wallet providers are, and how point-of-sale mobile wallet payments work. It also includes survey data on consumer adoption of point-of-sale mobile wallets.

With consumers becoming increasingly attached to their smartphones and accustomed to carrying out a very wide range of activities on these devices, bricks-and-mortar retailers and restaurants looking to the future need to be able to accept payments from mobile wallets.

Security

According to a Gallup U.S. consumer survey published in July 2015, security concerns top the list of reasons why consumers shy away from proximity mobile wallets. The report explains the following security technologies that can protect mobile payment transactions:

- Host Card Emulation/Near Field Communications, which stores mobile wallet payment account information securely in the cloud and not on the customer's mobile device;
- Tokenization, which replaces actual payment card numbers with one-time numbers;
- Point-to-point encryption, which encrypts a payment transaction from the moment the customer interacts with a POS terminal until the payment data reaches the processor;
- Mobile device identification, which ties a user's mobile wallet to his or her smartphone.



Robin Arnfield
MobilePaymentsToday.com

Robin Arnfield has been a technology journalist since 1983. His work has been published in ATM Marketplace, Mobile Payments Today, ATM & Debit News, ISO & Agent, CardLine, Bank Technology News, Cards International and Electronic Payments International. He has covered the United Kingdom, European, North American and Latin American payments markets.

Offers and loyalty rewards

The core reason why consumers will adopt proximity mobile wallets is not speedier payments, but because mobile wallets offer them the convenience of being able to store and redeem merchants' offers and loyalty rewards. "Mobile wallets are the perfect aggregator of offers," Josh Glantz, senior vice president, Mobiquity Networks, wrote in in a [Mobile Payments Today blog](#).

"The value proposition for mobile wallets has always been convenience, but, to propel consumer adoption of mobile wallets into the mainstream, the killer app needs to provide a platform for consumers to use loyalty reward offers that engage them with their favorite retailers," says Silvio Tavares, president and CEO of The CardLinX Association, which develops standards for linking loyalty reward offers to consumers' payment cards and digital wallets. "Industry collaboration is needed between wallets and retailers to enable more offers and loyalty programs to be available to consumers. The CardLinX Association enables this collaboration, creating friction-less card-linked and wallet-linked offers and loyalty benefits for consumers and retailers."

Introduction

There is disagreement in the payments industry as to how to define the term ‘mobile wallet.’ According to [Mobile Payments Today’s](#) “Mobile Wallet Comparison Guide 2015,” it is as difficult to determine a precise definition for a ‘mobile wallet’ as it is to determine the total number of mobile wallet providers. The Guide says that, in the U.S. alone, some 200 banks, retailers, telcos and other third parties claim they provide a mobile-wallet service.

“Some industry observers believe a mobile wallet can do just one thing well, while others believe it needs to be a true replacement for a physical wallet,” the Guide says.

“It’s safe to say that there is widespread agreement that a mobile wallet can be a place where consumers can store and organize coupons, loyalty programs, payment cards, tickets, car-insurance identification and whatever else can be turned into a digital item from its original paper or plastic form. Some mobile wallets tout other features such as bill payment, comparison shopping, location-aware services, person-to-person payments functionality and social-media connectivity,” the Guide says.

Types of mobile wallet

There are three types of mobile wallets that can be used at the point of sale.

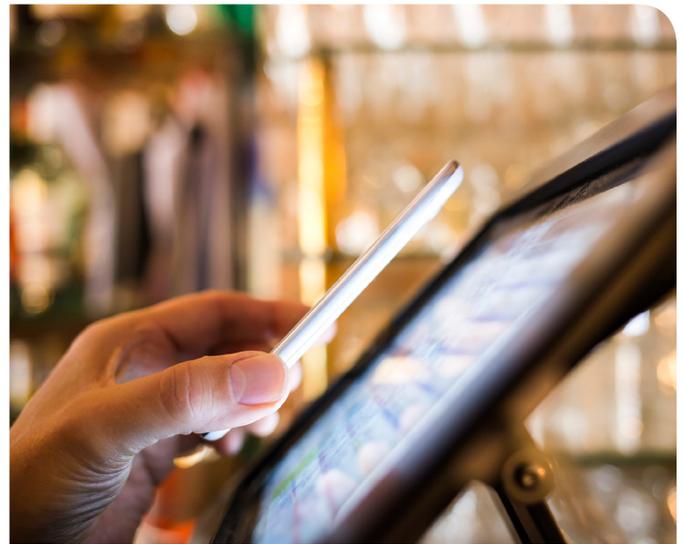
Retailers may decide to develop their own mobile app which features a mobile wallet capability.

Financial institutions (FIs) such as banks, credit card issuers and credit unions may develop a mobile wallet for use by their cardholders in retail outlets.

Intermediaries such as Apple, Google, and Samsung have developed mobile wallets that can contain cards from multiple issuers.

Smartphone ownership

To be able to use a mobile wallet, consumers need a smartphone running either Apple’s iOS operating system (Apple



Pay works only on the latest iPhones and Apple Watch at the point of sale), Google’s Android platform, or Windows Mobile. They can also download mobile wallets to certain Blackberry devices.

According to the Pew Research Internet Project, as of October 2014, 64 percent of American adults owned a smartphone, up from 35 percent in Spring 2011.

Smartphone ownership is especially high among younger Americans, as well as those with relatively high income and education levels, [Pew Research Center](#) says.

A survey conducted in December 2014 by the U.S. Federal Reserve for its “Consumers and Mobile Financial Services 2015” report, found that 87 percent of the U.S. adult population had a mobile phone, and 71 percent of mobile phones were Internet-enabled smartphones.

“The share of smartphone users who reported having made a mobile payment in the 12 months prior to the survey has increased to 28 percent, up from 24 percent in both 2013 and 2012,” the Federal Reserve says. “Among mobile payment users with smartphones, the most common type of mobile payment was bill payment through an online system or mobile app (68 percent, up from 66 percent in 2013). Over



a third (39 percent) of all mobile payment users with smartphones had made a point-of-sale payment using their mobile phone in the 12 months prior to the survey, in line with the 39 percent reporting such payments in 2013.”

Of mobile payment users with smartphones who made point-of-sale mobile payments, 31 percent did so by scanning a barcode or QR code displayed on their phone’s screen at check out (down from 39 percent in 2013), while 22 percent used an app that didn’t require tapping their mobile phone or scanning a barcode (up from 17 percent in 2013), and 14 percent made a payment by waving or tapping their mobile phone at a POS terminal.

Smartphones are changing the way people shop, the Federal Reserve says, noting that 47 percent of smartphone users had comparison-shopped with their phone while at a retail store, and 33 percent had used their phone to scan a product’s barcode to find the best price for the item.

Of those consumers who used their phones to comparison-shop in a retail store, 69 percent had changed where they purchased a product as a result of the information they found, the Federal Reserve says.

Consumer adoption of mobile wallets

Despite a huge amount of media attention in recent years, mobile wallets have largely failed to gain mass consumer adoption. However, this began to change with the launch of Apple Pay in October 2014. According to Apple CEO Tim Cook, over one million people had registered their credit cards with the service in the first three days.

An April 2015 [survey](#) by Blackhawk Network of U.S. consumers found that 25 percent of respondents had an app incorporating mobile wallet capability on their smartphones. The survey also found that 14 percent of respondents had made a mobile payment from their smartphone or tablet, and that 18 percent of consumers had used alternative payment methods such as mobile wallets, Apple Pay or Bitcoin. Also, 68 percent of mobile payment users reported that they were using alternative payment methods more in 2015 than last year.

However, a survey published by [Gallup](#) in July 2015 said that mobile wallets are a low priority for consumers, with only 13 percent of 17,000 U.S. consumers surveyed having a wallet on their smartphone.

“Security concerns top the list of reasons why consumers shy away from proximity mobile wallets,” Will Hernandez, [Mobile Payments Today’s](#) editor, wrote. “Some 55 percent of (Gallup survey) respondents were concerned about some kind of security issue such as a hack or losing their phone. Some 21 percent of respondents don’t know enough about mobile wallets to make a decision about them.

“Some 55 percent of (Gallup survey) respondents were concerned about some kind of security issue such as a hack or losing their phone. Some 21 percent of respondents don’t know enough about mobile wallets to make a decision about them.”

— Will Hernandez, editor, *Mobile Payments Today*

Mobile wallet adoption is being hindered by lack of merchant acceptance. According to Blackhawk’s [Where it’s at: connected consumer study](#), 54 percent of consumers would likely use a mobile wallet instead of a physical wallet if it were accepted everywhere.

“Mobile wallet adoption in the online arena has been brisk since the late 1990s, and will continue to be so as more and more online volume moves towards mobile devices,” says Rick Oglesby, Head of Research at U.S.-based Double Diamond Payments Research. “The wallet streamlined the online buying experience which was very clunky at first, and the small screens and keyboard-less designs of today’s



mobile devices only serve to accentuate the need for mobile wallets online. In the offline arena, however, the need for a digital wallet is not nearly as clear-cut, and consumer behavioral patterns are far more entrenched. So consumer use of mobile wallets in offline environments will grow slowly.”

While proximity mobile wallet transactions are slow to take off, the remote mobile commerce market is booming, with Javelin Strategy and Research predicting total mobile online retail payments will grow from \$75.8 billion to \$217.4 billion between 2014 and 2019.

“For in-app sales, PayPal, Android Pay and Apple Pay are all musts, and PayPal is the leader for web-based sales,” Oglesby says.

How mobile wallets work

To obtain a mobile wallet, smartphone users need to download the app from the app store associated with their phone – for example, the Google Play Store or the Apple App Store. They then need to load their payment credentials into the wallet.

Mobile wallet payments take advantage of several features of smartphone technology, such as smartphones' built-in digital cameras, graphical representation of the wallet, GPS tracking, fingerprint scanners for authentication, and real-time connectivity to the consumer's FI, Paul Fiore, CEO of credit union mobile wallet provider CU Wallet, wrote in a blog.

There are four methods of making a point-of-sale mobile wallet payment:

- NFC
- QR codes
- Bluetooth
- Apps

NFC

In an NFC transaction, an NFC-enabled smartphone communicates via an RFID link with a contactless transmitter attached to a POS device. The cardholder pays using a card held in digital form in their mobile wallet, which is either stored in a secure element on their smartphone's SIM card, or in the cloud using a technology called Host Card Emulation (HCE).

At checkout, the consumer tells the clerk they wish to pay using their smartphone. The consumer opens their mobile wallet, selects the desired card and then taps their smartphone on the merchant's contactless POS terminal. The consumer's payment credentials are automatically retrieved from the smartphone's secure element - or from the cloud using HCE - and transmitted via NFC to the payment terminal.

Cloud-based transactions require a data connection, either through the customer's mobile data plan or through in-store Wi-Fi.



The advantage of HCE over secure element-based NFC is that, since HCE is supported by Google's Android KitKat 4.4 operating system, it can run on any NFC-enabled Android-based smartphones. By contrast, secure element-based NFC requires an agreement between the mobile wallet provider and mobile carriers, to enable customers' card credentials to be downloaded to their smartphone's secure element.

Payment apps

Several mobile payment providers such as [PayPal](#) offer apps which communicate in the cloud with retailers at the point of sale without users scanning QR codes or tapping their smartphone on a POS terminal.

PayPal's app shows users a list of retailers who accept PayPal in a particular area. The customer uses the app to check in with the merchant when in their store, tells the clerk they are using PayPal, and then pays for purchases through their PayPal account.

Bluetooth

Bluetooth Low Energy (BLE) is a protocol which enables Bluetooth 4.0-based smartphones and other mobile devices to communicate with BLE-based wireless transmitters known as Beacons. On entering a store, the consumer's mobile payment app senses a BLE Beacon, and "checks in" to alert the retailer's POS to the consumer's presence.



Bluetooth beacons are used to identify the consumer who is making the payment, and to enable the POS terminal to communicate merchant information such as the store number and location and payment due to the customer's smartphone. "However, currently the actual payment happens via another technology such as a cloud-based app," says Double Diamond Payments Research's Oglesby. At checkout, the consumer tells the clerk to post the sale to their mobile payment account, which is visible on the clerk's POS terminal. The clerk verifies the consumer's identity and completes the transaction.

According to the Mobile Payments Today white paper "The iBeacon/BLE vs NFC Debate: Now The Truth," BLE transmitters are designed to continually broadcast a discovery signal. "Any app residing within a BLE-enabled (Bluetooth 4.0) smartphone can be configured to listen for these signals," the white paper says.

In August 2015, Target announced that it is rolling out a beacon technology pilot using its mobile app in 50 stores across the U.S. to enhance the in-store consumer experience and provide customers with deals and recommendations as they browse aisles.

QR codes

As an alternative to NFC, some m-payment service providers such as Starbucks and LevelUp offer QR code-based systems that store payment information in the cloud instead of the handset and can be executed on any smartphone.

Starbucks' mobile wallet currently accounts for 20 percent of all its U.S. in-store transactions.

The LevelUp mobile app for iPhone and Android allows registered users to link their payment card to a unique QR code displayed within the app. To pay with LevelUp, users scan the QR code on their phone at LevelUp terminals located at LevelUp-accepting merchants. In addition, LevelUp also supports NFC and Apple's BLE-based iBeacons.

Wearables

Although it is still very early days for mobile payments via

wearable devices such as smart watches, wristband and smart glasses, a number of innovative companies are trialing the technology.

For example, Apple Pay can be used for payments with the Apple Watch which contains an NFC chip.

In August 2015, Square, the mobile payments technology vendor, launched an updated Square Cash app for the Apple Watch. The latest Square Cash release enables people to send payments to friends, family, or anyone nearby from their Apple Watch. Square Cash users can also make payments to businesses using the Apple Watch.

In August 2015, Canadian authentication technology company Nymi in collaboration with TD Bank Group and MasterCard, launched a Canadian pilot of the Nymi Band. This is an NFC-based wristband which enables consumers to make biometrically-authenticated, wearable credit card payments using their heartbeat. Other Canadian banks are expected to launch pilots of the Nymi Band during the rest of 2015.



In November 2014, RBC Royal Bank of Canada teamed up with Nymi to test the Nymi Band. RBC has also developed its own RBC Payband and RBC Paytag wearable payment devices, which it describes as "proofs of concept." The RBC wearable devices are controlled by a smartphone using Bluetooth.

According to Juniper Research, the global wearables market could be as big as \$19 billion by 2018. Currently, the largest applications for wearables are health and fitness.

Mobile wallet advantages

This chapter explains the benefits to retailers, restaurants and consumers from adopting proximity/point-of-sale mobile wallets.

Priorities for retailers and restaurants

“The most important priority for a retailer is to offer its customers its own mobile wallet that accepts tender such as gift cards, private-label cards and open-loop payment cards,” Richard Crone, CEO of Woodlands Hill, California-based mobile payments advisory firm Crone Consulting, says. “Providing a retailer-branded app containing a mobile wallet establishes a connection between the merchant and the customer, who becomes a known and registered user. The merchant can communicate with the customer both before and after the purchase, and establish a true CRM (customer relationship management) model, something most merchants don’t have.”

A loyalty card only tells the merchant that a customer has made a purchase at the point of sale in one of their stores, says Crone. “With a mobile app, the merchant can send offers to the customer, and interact with them before they come to their store, for example through the app’s shopping lists and wish-lists,” he says.

Crone says that, when a customer uses a merchant’s own mobile app to make a payment, then the merchant captures and owns the customer information. “If the customer uses a mobile wallet supplied by a third party such as Apple or a bank, then the merchant doesn’t know who is doing the purchasing,” says Crone.

The best merchant wallet is one that is subsumed into the merchant’s mobile app, so that the customer has a seamless experience, says Crone. “Merchants should take a look at Uber, the driver-hire app, which provides a seamless ordering and payment experience,” he says. “They should ‘uberize’ their mobile apps so they take out all the

friction out of mobile payments and include value-add such as personalization around the shopping service.”

“Getting payments into their own mobile app should be a priority for retailers.”

— Richard Crone, CEO of Crone Consulting

Customers should be able to add any tender into the retailer’s app including private-label store cards, gift cards, rewards cards, and card scheme-branded credit and debit cards, says Crone. “Customers want to be able to pay through offers and rewards points stored in their app using their mobile phone,” he says. “Providing this facility will be an incentive for consumers to use mobile apps, because, when they pay, their rewards points and offers will be automatically deducted from the cost of their purchase using the app from their phone.”

“Location-based retailers should be focused on providing their own mobile wallets that create account-on-file relationships with their best customers,” says Double Diamond Payments Research’s Oglesby. “However, they aren’t likely to get all of their customers to use that wallet, so the next tier of wallets to support will be the ones that are controlled by the operating systems of the major mobile devices – Apple Pay and Google’s Android Pay, for example.”

FI-issued mobile wallets

Once they have established their own mobile wallet, merchants need to be able to accept FIs’ mobile wallets, says Crone.



“Retailers should negotiate with FIs on acceptance terms to put the bank, credit union or credit card issuer’s payment app and card credentials inside the retailer’s app and to put the retailer’s app inside the FI’s app,” says Crone. “This involves the retailer and the FI negotiating over interchange fees.”

Crone recommends that retailers talk to Los Angeles-based [CU Wallet](#), a credit union service company, which has created a credit union-branded mobile wallet called CU Wallet. “Over 100 U.S. credit unions are working with CU Wallet to launch a credit union-branded mobile wallet that is accepted by merchants,” says Crone.

In addition, the largest U.S. banks are developing their own branded mobile wallets for the cardholders, and announcements are expected over the next few months, says Crone.

“Mobile wallets requires partnerships,” says Paul Fiore, CU Wallet’s CEO. “An FI wallet without retailer acceptance is no good, and merchant apps that don’t accept FI-branded mobile payments apps containing FIs’ cards won’t be consumer-friendly. In the longer term, retailers need to be able to accept open mobile wallets as well as just their own.”

Third-party mobile wallets

The third priority for retailers is to accept third-party mobile wallets such as Apple Pay, Google’s Android Pay, and Samsung Pay.

“If a retailer wants to make a sale from a mobile customer, they must accept all forms of payment including third-party wallets like Apple Pay,” says Crone. “However, retailers should remember that the one who enrolls a customer in a mobile wallet controls the data in the relationship. With a third-party app, the retailer gives up the touchpoint and the customer data. The goal of Google, Apple and Samsung, for example, is to collect data and provide customized ads and offers to their wallet-holders, and build loyalty for their wallet, not for the retailer or the bank’s wallet.”

“In the short term, merchants will work with third-party mobile wallet providers like Apple,” says Fiore. “But, in the

long term, it’s in FIs’ and merchants’ best interest to have a direct relationship with their customers and not to be disintermediated by third-party wallets.”

Benefits to consumers

A Mobile Payments Today blog by Teri Llach, chief marketing officer at Blackhawk Network, argues that it is shortsighted to position mobile wallets merely as containers for payment cards that offer speedier payments.

“We believe that most digital wallet players to date have been focused on the wrong objective – speedier payment – not on an improved mechanism for consumers to shop, spend, save and engage with their favorite retailers,” Llach says. “It’s not difficult for shoppers to pull out a debit or credit card and swipe because they always carry those cards. But shoppers don’t like to carry all their gift cards, loyalty cards and coupons because there are too many. Integrating those, as well as ID and an option for paper receipts, into a mobile wallet is when it will become game changing.”

Llach says that mobile wallets can help consumers track their rewards/loyalty points and offers and obtain seamless access to coupons, pop-up deals, rebates and rebate submission options. She argues that merchants can use in-store location technology such as beacons (See Chapter Two, Bluetooth page 7) to strengthen their relationship with customers, citing a Blackhawk survey finding that 59 percent of consumers would consider allowing retailers to know where they are in-store (via beacon technology) in exchange for exclusive values and savings.

Importance of rewards and offers

“Because they control the (mobile) device, Apple and Samsung have at least one advantage in distributing their wal-

“Mobile wallets are the perfect aggregator of offers.”

— Josh Glantz, senior vice president, Mobiquity Networks



let solution,” Josh Glantz, senior vice president, Mobiquity Networks, wrote in a [Mobile Payments Today blog](#). “Actual consumer adoption and growth, however, will depend more on the ecosystem within each. That ecosystem will have to include (and for most it already does):

- Linkable payment options (credit/debit card linking, carrier billing option, EFT, etc.);
- Card/wallet-linked offers and coupons to drive usage;
- Brand/retailer linked loyalty programs;
- Reminders (nobody likes to make a purchase only to remember later that they had an offer/coupon in their wallet!);
- Retailer adoption (this is not even close to universal yet and is a big hurdle to consumer adoption).

“Mobile wallets in the most basic sense don’t pay for products more easily or appreciably faster than cash or a credit card,” Glantz wrote. “They don’t link to your credit card loyalty program any easier than.... your credit card does. What (mobile wallet providers) should be thinking about is what the consumer wants. Going back to the list above, consumers want most of all coupons and offers. Mobile wallets are the perfect aggregator of offers. They provide a simple and elegant way to store and present those offers for ease of use. And they at least have the ability to deliver time and location-relevant reminders that an offer is available to claim or redeem.”

In a [Mobile Payments Today blog](#), Will Hernandez, the publication’s editor, said that mobile wallet providers can’t keep talking about the convenience factor with mobile payments at the point of sale. “That argument doesn’t hold weight with most consumers, regardless of the demographic,” Hernandez wrote. “One of the areas where some mobile providers fall short on convenience is with rewards. Some providers do it better than others. LevelUp and Sionic Mobile put their rewards programs front and center. The actual mobile payment is a means to an end, i.e., paying for a purchase. The problem LevelUp and Sionic Mobile face at the moment is that their reach is limited. Both continue to add more acceptance points, but they are nowhere close to being widespread.”



Card-linking

As the offers and loyalty space has become more popular, consumers have often found it cumbersome to take advantage of the variety and amount of opportunities available. Card-linking helps solve that problem by giving retailers and advertisers the ability to deliver a targeted offer or deal to consumers via their credit, debit or other payment card without having to use a paper coupon, voucher or promotion code.

Consumers simply link an offer to their card through their mobile phone, social media app, or online. When the consumer uses their card to pay in the store, they are notified of their discount or loyalty benefit through their mobile phone or e-mail nearly instantly. Thus card-linking stands at the intersection of the payments, social media, advertising, and retail industries.

“The value proposition for mobile wallets has always been convenience, but, to propel consumer adoption of mobile wallets into the mainstream, the killer app needs to provide a platform for consumers to use loyalty reward offers that engage them with their favorite retailers,” says Silvio Tavares, president and CEO of The CardLinX Association. “Industry



collaboration is needed between wallets and retailers to enable more offers and loyalty programs to be available to consumers. The CardLinx Association enables this collaboration, creating friction-less card-linked and wallet-linked offers and loyalty benefits for consumers and retailers.”

The [CardLinx Association](#) is a non-profit organization that brings together retailers, digital publishers, payment companies, banks and card-linked technology providers to develop industry standards for card-linked offers and loyalty programs. CardLinx hosts collaboration forums where small to very large retailers can meet face-to-face with the key digital commerce industry participants such as payment companies and digital publishers.

CardLinx also develops interoperability standards and services that eliminate friction for consumers and retailers. Its members include Facebook, Microsoft, Whole Foods Market, Bosch, MasterCard, Discover, American Express and First Data among others.

“Because of a lack of industry standards, it has been a technical challenge to deliver a really cool customer and merchant experience and to load merchant offers and loyalty rewards into customers’ mobile wallets,” says Tavares. “Sometimes loading offers and rewards into a mobile wallet works, and sometimes it doesn’t.”

Security issues

According to a Gallup U.S. consumer survey published in July 2015, security concerns top the list of reasons why consumers shy away from proximity mobile wallets. Some 55 percent of respondents were concerned about some kind of security issue such as a hack or losing their phone, Gallup [found](#).

“Generically, I’d say that the big security issue (with mobile wallets) is simply change,” says Double Diamond Payments Research’s Oglesby. “Whenever we change payment processes, we create new potential vulnerabilities that fraudsters will seek to exploit until they are addressed. Mobile wallets can be at least as secure as card payments, and should be more secure over time. In some ways, they already are.”

“With a smartphone-based payment, you can identify the device used for the transaction through its unique fingerprint – its Electronic Serial Number or International Mobile Equipment Identity number,” says Crone Consulting’s Richard Crone. “This means that you can tie the user to their device. In the Paydiant platform, if someone steals your mobile wallet user name and password, they wouldn’t be able to use your account as their smartphone wouldn’t match your smartphone’s unique fingerprint.”

“Retailers shouldn’t be too concerned about accepting the major wallets like Apple Pay, Android Pay and Samsung Pay,” adds Oglesby. “Each of these wallets is designed to ride the same rails as card transactions, and they actually do so with a bit more security than a physical card transaction due to their use of tokenized data and EMV compatibility.”

EMV and NFC

The U.S. payments card industry is migrating to EMV, a standard for authorizing credit and debit chip card transactions.

To be able to accept point-of-sale EMV payments, merchants must install EMV-compliant card readers in their stores, and issuers have to provide consumers with new cards containing EMV-compliant chips. The card networks have announced that, from October 2015, they will shift liability for fraudulent transactions involving EMV cards to whichever party in the transaction chain is not EMV-compliant.

Many of the EMV-compliant POS terminals currently being installed by U.S. merchants contain NFC contactless card reader technology. At the same time, smartphone manufacturers are equipping their devices with NFC technology as well as with security features such as fingerprint authentication, notes the Federal Reserve report [Consumers and Mobile Financial Services 2015](#).

“You’d be hard-pressed to find an executive in the payments industry who doesn’t believe the EMV migration in the U.S. will help make NFC mobile payments more mainstream,” Mobile Payment Today Editor Will Hernandez wrote in an [article](#) titled “US EMV transition could open door to more NFC mobile payments.” “Companies such as Ingenico and Verifone already have deployed thousands of EMV-enabled POS terminals, and the majority of those readers are equipped with contactless technology. While the merchant has the final say to switch on the technology, no one can think of a good reason why a retailer would choose to keep it off.”

“Security-minded consumers may have more confidence making a mobile payment from a device that uses multiple layers of security, complies with EMV standards, and/or offers

new or additional features,” the Federal Reserve report says. “The changes in the marketplace may ultimately better protect customers’ data by reducing the amount of data accessed and stored by merchants.”



Tokenization

Tokenization is a key security technology which mobile wallet service providers need to deploy. It involves a one-time number being used to represent an actual credit or debit card number in a payment transaction. This token can only be detokenized – turned back into an actual card number - by the tokenization service provider. The cardholder's primary account number (PAN) is only stored on the tokenization service provider's system.

There are three types of tokenization.

First, website tokenization occurs when a customer enters their full PAN on a merchant's website, but the merchant never sees the PAN as it is immediately tokenized by the processor in a software vault.

Second, POS terminal tokenization occurs when the cardholder's PAN is tokenized as soon as the card is swiped or tapped against a POS terminal.

Third, network tokenization involves a card network such as Visa or MasterCard or a mobile wallet service provider tokenizing a cardholder's PAN and the token being stored securely on the user's mobile device or in an HCE cloud-based software vault.

"While Android Pay stores card details in the cloud using HCE, Apple Pay uses a secure element to store card details on the phone, but tokenizes the card numbers," says Crone Consulting's Richard Crone. "If you store card numbers on the phone, they are vulnerable even if they are tokenized."

If the token isn't encrypted, it could be intercepted and used fraudulently until the issuer realizes that there is fraud involving that token, Crone argues.

"It's more secure to store the card details on the cloud and not give the card credentials to the merchant," says Crone. "For example, Paydiant's approach, as adopted by MCX, is to store card details in the cloud and never disclose card credentials to merchants. Paydiant in fact tokenizes the transaction session versus just tokenizing the card account number. With session tokenisation, the merchant doesn't get to see the card number."

Sorting card credentials in the cloud takes the fraud risk out of PCI DSS compliance scope for merchants, because they never get to see the customer's card details, says Crone.

However, Crone warns that tokenization schemes prevent merchants from identifying their customers by their card numbers. "Merchants carry out big data analysis of their customer's credit and debit card numbers, so they can capture sales information about them," he says. "If a customer pays with a tokenized method such as Apple Pay, this means the merchant won't be able to capture data on them. Third-party wallet providers like Apple won't share customer data with merchants, so the retailer won't know who their customer is. The only way merchants can get data about customers making mobile purchases is if customers use the merchants' own apps."

Point-to-point encryption

Point-to-point encryption (P2PE) involves encrypting transaction data from the point of interaction with the merchant's POS device until the data reaches the P2PE solution provider's secure decryption environment.

"Tokenization works very well in combination with P2PE," says Benoit Boudier, vice president of International Sales at Ingenico Mobile Solutions. "You encrypt the transaction message including the cardholder's token and then send it to the acquirer and the card network in encrypted form."

It is best practice to use a P2PE solution that is compliant with the security standards specified by the Payment Card Industry Security Standards Council.

The PCI SSC is an open forum which develops and manages the PCI DSS (Payment Card Industry Data Security Standard) and related payment card data security standards such as the Payment Application Data Security Standard (PA-DSS), which assesses ATM and POS applications to ensure they support PCI DSS compliance. Merchants, processors, card issuers, technology vendors and any organization hosting cardholder information are required to comply with these standards, whose purpose is to safeguard cardholder data and sensitive authentication data by eliminating security vulnerabilities at any point



in the payment card infrastructure. The standards cover POS, e-commerce and ATM transactions.

The PCI SSC's PCI P2PE standard provides a specification for the use of strong encryption to achieve point-to-point encryption, where clear-text card data is removed from the payments environment.

By using a PCI-compliant P2PE solution, merchants can potentially reduce their PCI compliance obligations.

Profiles of mobile wallet providers

The mobile wallet market has recently seen several of the major players acquire smaller rivals. For example, Samsung bought LoopPay, while PayPal acquired Paydiant, and Google acquired Softcard's assets.

FI support

It is vitally important for third-party wallet providers to sign agreements with FIs and credit card issuers so that the FIs allow their customers' cards to be loaded into their mobile wallets.

"Apple Pay, Android Pay and Samsung Pay are likely to have support from the FIs via the FIs' relationships with the payment networks, which in turn have relationships with the mobile wallet providers," says Double Diamond Payments Research's Oglesby. "Also, PayPal supports all FIs through its accounts-on-file and ACH approaches, so, in terms of FI coverage, these mobile wallet providers are all on fairly equal footing."

Apple Pay

Apple launched its Apple Pay NFC-based mobile payment service in October 2014 for the iPhone 6 and the Apple Watch (<https://www.apple.com/iphone-6/apple-pay/>). Users can also make Apple Pay purchases within participating apps on the iPhone 6, iPad Air 2, and iPad mini 3.

Apple has signed up a significant number of U.S. FIs and iPhone 6 users for Apple Pay and, according to Juniper Research, has helped increase adoption of contactless payments over the past year.

In a January 2015 earnings call, Apple CEO Tim Cook said Apple Pay accounted for two out of every three dollars of contactless payments on American Express, Visa and MasterCard's U.S. card payments networks. Cook has also said that Apple Pay is on course to be accepted at 1.5 million locations in the U.S. by the end of 2015.

In June 2015, Apple announced that it had included support for loyalty cards and store cards in Apple Pay.

Apple Pay's security features include Apple's Touch ID fingerprint authentication sensor, storage of payment credentials in Apple Passbook, and the secure element chip built into the iPhone 6 and the Apple Watch for NFC payments at the point of sale.

To pay with Apple Pay, iPhone 6 users hold their iPhone near the merchant's contactless card reader with their finger on Touch ID.

Apple Pay assigns a unique Device Account Number to each registered payment card, which is encrypted and stored in the iPhone 6's secure element. Using tokenization technology (see Chapter 4, Tokenization, page 14), these Device Account Numbers are used instead of their associated payment card number, along with a one-time security code. This means users don't reveal their name, card number, expiration date or card security code to cashiers when making in-store payments.

Actual payment card numbers aren't stored on Apple servers, nor are they shared with merchants or transmitted with payments, Apple says. Users can add payment cards to Apple's Passbook from their iTunes account or by using the iPhone 6's camera to capture card information.

If an iPhone 6 is lost or stolen, the Find My iPhone feature can be used to put the device in Lost Mode so nothing is accessible, or the iPhone can be wiped clean completely.

According to Mobile Payments Today, in the U.S. Apple earns 15 cents on every \$100 spent using Apple Pay.

Android Pay

In May 2015, Google announced Android Pay, with American Express, Discover, MasterCard, Visa, FIs such as U.S.



Bank, PNC Bank, and Bank of America, and retailers such as McDonald's, Panera, Whole Foods, and Uber announcing support for the HCE-based [mobile payment system](#).

Google's earlier point-of-sale mobile payment system Google Wallet lives on as a dedicated person-to-person transfer mobile app for both Android and iOS devices, [Mobile Payments Today](#) says. Google says that [Google Wallet](#)-holders can spend the money in their accounts using a Google Wallet prepaid MasterCard in stores, or transfer the funds to their bank account.

"With select retailers, your loyalty programs and special offers will be automatically applied at checkout (through Android Pay), [Google says](#). "For example, when you tap to buy a Coke at a vending machine, your MyCokeRewards will be automatically applied. With Android Pay the contactless terminal not only receives your payment info, but also your loyalty programs and offers."

When using Android Pay to make a point-of-sale purchase, Android Pay won't send the customer's actual credit or debit card number with their payment. Instead, Android Pay will use tokenization to generate a virtual account number representing the customer's account information, Google says.

In February 2015, Google bought [Softcard](#), the mobile wallet joint venture between AT&T, T-Mobile and Verizon Wireless which was previously called Isis.

Google [said](#) on September 10, 2015 that it had begun to roll out Android Pay in the U.S. "Android Pay works with all NFC-enabled Android devices (running KitKat 4.4+), on any mobile carrier, at every tap and pay-ready location across the U.S.," Pali Bhat, director of product management for Android Pay, said. "Android Pay will support credit and debit cards from the four major payment networks: American Express, Discover, MasterCard and Visa"

Android Pay will come pre-installed on new AT&T, Verizon and T-Mobile smartphones thanks to Google's Softcard acquisition.

Michelle Evans, senior consumer finance analyst at Euromonitor International, told [Mobile Payments Today](#) that Android Pay will leverage NFC technology [and HCE sup-

port], and enable merchants to accept mobile payments in-store from participating consumers, as well as enable merchants to embed Android Pay directly into their mobile apps. Android Pay also will support fingerprint readers for users to authenticate payments at checkout in the same vein as Apple Pay, Evans said.

CU Wallet

As of August 2015, four U.S. credit unions are piloting CU Wallet with their employees.

"We provide two different version of the CU Wallet software to reflect the two approaches adopted by our clients," says CU Wallet's Fiore. "The first version is for FIs which already have mobile banking apps and don't want to confuse their members by providing a separate mobile wallet on the app store. So, for this type of client, we provide an integrated mobile wallet that integrates with their existing mobile banking provider."

As an alternative, CU Wallet provides a standalone mobile wallet app that is separate from mobile banking. "This is for credit unions which who don't want a monolithic app that does everything," says Fiore. "So this version isn't integrated with the credit union's mobile banking provider."

However, whichever version of CU Wallet a credit union installs, the wallet will use the same password and user name as the FI's mobile banking app. "In both approaches, our app is integrated with the credit union's core banking system and hooks back to their member information database," says Fiore. "This means that, both in an integrated app and a stand-alone app, the member can see their last 10 or so credit card transactions without logging out."

Fiore says CU Wallet encourages credit unions to make their mobile wallets open, so that members can add gift cards, credit and debit cards from any issuer, PayPal and even Bitcoin into CU Wallet. "Our wallet incorporates a merchant offers network provided by Relevant Solutions," he says. This integration gives CU Wallet member credit unions the ability to deliver promotions and offers from over 750 national merchants, as well as local retailers directly to their members.



CU Wallet's software is provided by [Paydiant](#) and offers QR code-based payments.

"CU Wallet will go to market with QR codes, since QR currently works with the largest number of merchant POS systems," says a CU Wallet spokesperson. "However, our Paydiant back-end solution also supports NFC and BLE."

"Paydiant can handle QR codes in two ways," says Fiore. "Either the merchant has a QR code scanner at their POS terminal which scans the QR code on the customer's smartphone, or the customer's smartphone camera scans a merchant's QR code."

"CU Wallet's interface can be easily adjusted to support all merchant device-pairing technologies, including QR codes, NFC, HCE, and BLE," CU Wallet says in a product information sheet.

The disadvantage of CU Wallet from a retailer's point of view is that merchants need to support Paydiant on their POS terminals to accept CU Wallet. "For example, Subway's 27,000 locations accept Subway's Paydiant-based mobile wallet, and this means Subway could accept any FI-issued mobile wallet that is based on Paydiant," says Fiore.

Fiore says that ultimately mobile payments will migrate to open systems and merchants won't need to have Paydiant software to accept CU Wallet. "The payments industry is moving towards POS hardware that is open and will accept all kinds of payment methods such as smartphones with NFC and QR code-based mobile wallets," he says.

LevelUp

[LevelUp](#) says its mobile wallet supports NFC, QR codes, and BLE, and is available on Apple, Android and Windows smartphones, smart watches, Apple Passbook and Google Wallet. Users link one or more payment cards to their LevelUp account, which then generates a QR code for display on their smartphone's screen.

To make a payment from a card linked to their LevelUp account, users either tap their NFC-enabled smartphone against the LevelUp scanner or scan their LevelUp QR

code on the LevelUp scanner's screen. They will then receive a digital receipt seconds later.

LevelUp says its system is accepted at over 14,000 U.S. merchants.

The LevelUp scanner can either be installed on a stand-alone basis and connect with a LevelUp smartphone, or it can be integrated with the merchant's existing POS system. For more information on which POS vendors' systems can be integrated with the LevelUp scanner, see <http://setup.thelevelup.com/integrated?locale=en>.

LevelUp offers merchants a loyalty and rewards platform that enables them to capture and analyse data about their customers using campaign analytics software and then provide them with rewards programs. "Because LevelUp is the method of payment, (rewards) redemption is always seamless as customers simply pay to accrue and redeem rewards," LevelUp says.

A [white-label](#) version of LevelUp is available, which offers merchants a custom mobile payments app and loyalty program.

In May 2015, LevelUp and Olo launched what they claim is the restaurant industry's first turnkey mobile commerce solution with built-in ordering, loyalty and payment in one user experience. The fully-branded app removes the complexity of integrating solutions and brings together fast, fluid mobile ordering with customer offers and rewards, said Michael Hagan, LevelUp's chief strategy officer. Consumers can order and pay ahead, earn rewards, or pay in-store all within the same application, available for both Apple iOS and Google Android devices.

Since May 2015, LevelUp has allowed its users who are Sprint subscribers to charge in-store purchases to their Sprint mobile phone bill thanks to a partnership with direct carrier billing company Danal.

MasterCard MasterPass

[MasterCard MasterPass](#) provides a single sign-in for remote mobile and online purchases at merchant websites that accept the MasterCard-branded digital wallet.



While it can be used for in-app purchases, MasterPass is not intended for use at the point-of-sale, and doesn't involve downloading an app to a smartphone.

MCX

Merchant Customer Exchange (MCX) is an alliance between the largest U.S. retailers and restaurant companies, including WalMart, Target, and Best Buy. Its goal is to bring down the cost of card acceptance in its members' stores through the use of the CurrentC mobile wallet.

MCX was founded in 2012 with the aim of providing a mobile payment system that would give participating merchants a way to integrate "a wide range of consumer offers, promotions and retail programs." The system is intended to bypass the card networks and eliminate the need to pay credit card interchange, thus lowering merchants' card acceptance costs, Mobile Payments Today says.

To achieve this goal, MCX plans to only offer acceptance in CurrentC of low-cost payment methods such as private-label store credit and debit cards, gift cards, and direct access to checking accounts (also referred to as decoupled debit). To encourage consumers to use CurrentC, MCX will incorporate merchants' loyalty programs directly into CurrentC, making it easier for consumers to earn rewards points and receive offers.

"CurrentC lets you select personalized and tailored offers based on your location and purchase history, and, when you check out using the CurrentC mobile wallet, it will automatically deduct the offer and show you the discount on your bill," says Crone Consulting's Richard Crone

Crone says that, while initially CurrentC will not be open to bank/card network-branded payment cards, various parties such as CU Wallet are attempting to get MCX to accept open-loop cards. "What MCX should do is to incentivise CurrentC users to pay with lower-cost payment cards through rewards and offers," he says. "If it doesn't become open and just stays with store cards, it will be dead on arrival."

In September 2015, MCX was due to launch a public pilot of CurrentC in Columbus, Ohio, following a trial with vari-

ous merchants and their employees. However, MCX said CurrentC will not be rolled out until 2016.

Based on Paydiant's platform, CurrentC uses QR codes, with all payment transactions occurring in the cloud.

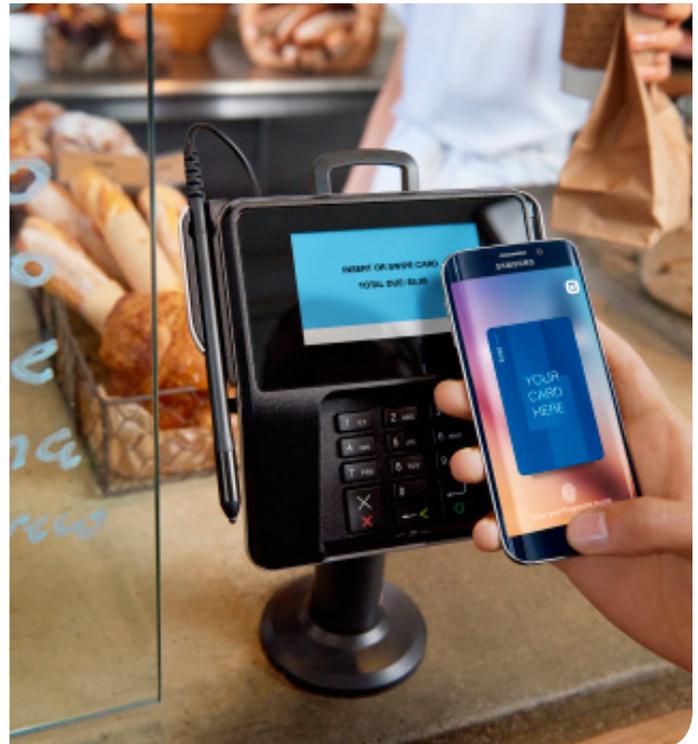
PayPal/Paydiant

In February 2015, PayPal acquired white-label mobile wallet provider Paydiant, giving it a foothold in the point-of-sale mobile payments market in which PayPal had struggled to gain traction.

Paydiant clients' current mobile wallet deployments are QR code-based, but Paydiant is agnostic as to payment acceptance methods and will support BLE and NFC, says CU Wallet's Fiore.

PayPal launched a point-of-sale version of the PayPal Wallet in 2012, but failed to gain large user numbers.

"PayPal has an opportunity to be a real catalyst in mobile payments with its huge customer and merchant base,"





says Crone Consulting's Richard Crone. "Following the Paydiant deal, PayPal has three approaches to mobile wallets. PayPal has its own PayPal-branded mobile wallet which supports all ways of making a payment, and it also supports retail-branded wallets and bank-branded wallets through Paydiant."

One of the first fruits of PayPal's Paydiant acquisition is that Paydiant customer Subway agreed in July 2015 to incorporate PayPal as a payment option within the Subway App which was developed by Paydiant and released in early 2015. This means that PayPal will be accepted at 27,000 Subway locations across the U.S.

"To pay in-store or as part of a mobile order, Subway guests will simply select the PayPal option, enabling them to utilize any smartphone or operating system (Android or iOS) to conduct their transaction," Paydiant said in a news release. "PayPal will also be integrated as a payment choice for online orders on order.subway.com. We're also enabling PayPal's One Touch™ checkout experience – the faster, easier way to pay - for eligible consumers checking out online and on mobile. With One Touch, consumers who have opted-in can pay in a single touch without having to type in their PayPal usernames or passwords after initial log-in for six months."

Apart from Subway, other Paydiant mobile wallet clients include Barclaycard, Capital One, Harris Tweeter supermarkets, Orange Leaf, and MCX.

Paydiant says it doesn't store any payment card data on a customer's smartphone, instead securely storing sensitive cardholder data in the cloud in a PCI Level 1-compliant, SAS70 certified data center. PCI Level 1 is the highest level of compliance with the Payment Card Industry Security Standards Council's PCI DSS standard (see Chapter 4, page 14).

Samsung Pay

Samsung Pay will launch in the U.S. on September 28 after debuting in Korea. The mobile wallet will be preloaded on select Galaxy S6 Edge+ and Galaxy Note 5 smart-



phones. A free software upgrade will be rolled out from mid-August to enable Samsung Pay on customers' Galaxy S6 and S6 edge devices in the U.S. and Korea. Users will be able to pay for purchases by waving their phones near a card reader in a store and scanning their fingerprint on the phone.

Samsung Pay is partly based on technology which Samsung acquired when it bought LoopPay in February 2015. It will use NFC to communicate with NFC-based POS devices, but also will use LoopPay's Magnetic Secure Transmission technology which enables users to make a payment by holding their smart phone near a traditional magnetic-stripe card swipe reader.

This feature will give Samsung Pay an advantage over Apple Pay which requires POS devices to be equipped with NFC technology.

"With Magnetic Secure Transmission and NFC technologies, Samsung Pay works with most existing POS terminals," Samsung said in a press release. "That means it's the only mobile payment service that works virtually anywhere you can swipe your credit card or debit card."

Samsung says it anticipates working with payment networks such as American Express, Discover, MasterCard



and Visa, major banks including Bank of America, Chase, and U.S. Bank, and key financial partners including First Data, private-label card issuer Synchrony Financial and TSYS to extend Samsung Pay to the U.S.

AT&T, Sprint, T-Mobile, and U.S. Cellular are listed on Samsung Pay's promotional pre-launch [website](#) as supporting Samsung Pay on their smartphones. However, Verizon isn't listed, and, according to [ZD Net](#), is still evaluating the new payment system. The Samsung Pay promotional website also lists Amex, MasterCard, Visa, Bank of America and U.S. Bank as supporting the system.

Samsung Pay uses tokenization, Samsung KNOX, and fingerprint authentication to provide secure payments and reduce the security risks inherent to plastic cards.

According to [TechRepublic](#), KNOX is a containerization system that separates business and personal data to add a layer of security not available on standard Android devices.

Sionic Mobile

Atlanta, Georgia-based [Sionic Mobile](#) has developed the ION mCommerce platform which delivers mobile promotions, payments and rewards, along with two cloud-based free apps, ION Loyalty for merchants and ION Rewards for consumers. After downloading ION Rewards, a consumer needs to link a credit or debit card to the app.

ION rewards users are rewarded instantly with two percent cashback every time they pay with their smartphones at the nearly 100,000 retailers and restaurants in the U.S. that use the ION platform. They can redeem their ION rewards at any ION-accepting merchant.

Sionic Mobile charges merchants a one percent fee when users pay with an ION app plus a funds transfer fee which is paid to its payment processing partners.

The company says its Sionic Mobile platform requires no integration with POS systems and can typically be set up in under an hour.

Visa Checkout

[Visa Checkout](#) provides a single sign-in for remote mobile and online purchases at merchant websites that accept the Visa-branded digital wallet.

While Visa Checkout can be used for in-app purchases, it is not intended for use at the point-of-sale, and doesn't involve downloading an app to a smartphone.

About the sponsor:

The non-profit CardLinx Association is the leading association for the card-linked industry. Card-linking is the practice of associating deals, offers, and loyalty rewards with a consumer's choice of payments card and digital wallet, eliminating the need for paper coupons or promotion codes. CardLinx brings together leading merchants, digital publishers, payment networks, and banks, including MasterCard, Discover, Microsoft, Facebook, PayPal, and First Data, to develop industry standards that eliminate friction for consumers and merchants. It also provides forums where small to very large retailers can meet face to face with digital commerce industry participants. CardLinx members serve or represent over 6 million merchants, have issued over 1.9 billion payment cards, and serve consumers with over 200 million card-enabled accounts and over 700 million active daily users. For more information, visit [cardlinx.org](#).

REFERENCES

Mobile Payments Today
www.mobilepaymentstoday.com

“NRA releases mobile payments guide for restaurateurs”
Mobile Payments Today
<http://www.mobilepaymentstoday.com/news/nra-releases-mobile-payments-guide-for-restaurateurs/>

“No surprise: Gallup finds mobile wallets low priority for consumers” by Will Hernandez
<http://www.mobilepaymentstoday.com/blogs/no-surprise-gallup-finds-mobile-wallets-low-priority-for-consumers/>

“Major mobile wallet providers not distinguishing themselves” by Will Hernandez
<http://www.mobilepaymentstoday.com/blogs/major-mobile-wallet-providers-not-distinguishing-themselves/>

“Uber and lessons for the mobile wallet” by Mark Ranta
<http://www.mobilepaymentstoday.com/blogs/uber-and-lessons-for-the-mobile-wallet/>

“Digital wallets: how merchants can use the platform to draw in consumers” by Teri Llach
<http://www.mobilepaymentstoday.com/articles/digital-wallets-the-rise-of-promising-platforms-and-whats-needed-to-break-through-with-consumers/>

“Mobile Banking and Payments Security: What banks and payment service providers need to know to keep their customers safe,” by Robin Arnfield
Network Media Group
<http://www.networldmediagroup.com/inc/sde-tail/12036/18751>

“Mobile Payments State of the Industry 2015 - Omnibus Edition”
Network Media Group
<http://www.networldmediagroup.com/inc/sde-tail/12036/19754>
<http://www.atmmarketplace.com/news/new-industry-report-examines-consumer-habits-preferences-in-mobile-banking-payments/>

Mobile Payments Today white papers
<http://www.mobilepaymentstoday.com/whitepapers/>

“mPOS 101: What merchants need to know about mobile point-of-sale technology” By Robin Arnfield
Mobile Payments Today
www.mobilepaymentstoday.com/whitepapers/mpos-101/

Mobile Payments Security 101 by Robin Arnfield
<http://www.mobilepaymentstoday.com/whitepapers/mobile-payments-security-101/>

A look at the PCI guidelines for mobile POS
Mobile Payments Today white paper sponsored by Moki
<http://www.mobilepaymentstoday.com/whitepapers/a-look-at-the-pci-guidelines-for-mobile-pos/>

“There’s more to mobile payments than payments: Engaging Your Customers in the Age of the New Mobile Wallet”
Webinar and slidedeck sponsored by LevelUp
<http://www.mobilepaymentstoday.com/whitepapers/theres-more-to-mobile-payments-than-payments-engaging-your-customers-in-the-age-of-the-new-mobile-wallet/>

Mobile Payments Today directory of suppliers
<http://www.mobilepaymentstoday.com/companies/directory/companies-by-category/>

“Mobile Wallet Comparison Guide, 2015 edition”
Network Media Group
<http://www.networldmediagroup.com/inc/sde-tail/12036/20723>

“End-to-end Security in an Open and Mobile World”
Ingenico white paper
<http://ingenico.us/wp-content/uploads/2012/07/Ingenico-End-to-End-Security-in-an-Open-and-Mobile-World-EN.pdf>

Payment Card Industry Security Standards Council (PCI SSC) documents page
https://www.pcisecuritystandards.org/security_standards/documents.php



The LexisNexis® 2014 True Cost of Fraud(SM) Mobile Study
LexisNexis Risk Solutions and Javelin Strategy Solutions
and Research

<http://www.lexisnexis.com/risk/insights/true-cost-fraud-mobile.aspx>

PCI SSC Tokenization Product Security Guidelines

https://www.pcisecuritystandards.org/security_standards/documents.php

“The iBeacon/BLE vs NFC Debate: Now The Truth”
Mobile Payments Today white paper sponsored by Pyrim
Technologies

<http://www.mobilepaymentstoday.com/whitepapers/the-ibeaconble-vs-nfc-debate-now-the-truth/>

Visa Digital Solutions

http://usa.visa.com/clients-partners/technology-and-innovation/visa-digital-solutions/index.jsp?ep=v_sym_digitalsolutions

“Mobile Payment Acceptance Solutions Visa Security Best
Practices Version 3.0”

Visa

<http://usa.visa.com/download/merchants/bulletin-mobile-best-practices.pdf>

“Don’t Buy the Apple Pay Adoption Surveys” by John Misasi

https://www.linkedin.com/pulse/dont-buy-apple-pay-adoption-surveys-michael-misasi?trk=hb_ntf_MEGAPHONE_ARTICLE_POST

“Bluetooth Low Energy, Beacons and Retail”

By Erik Vlugt, Verifone

<http://www.verifone.com/media/3603729/bluetooth-low-energy-beacons-retail-wp.pdf>