

# white

**MOBILE PAYMENT  
SOLUTIONS:  
BEST PRACTICES AND  
GUIDELINES**

---

PRESENTED BY THE  
MOBILE PAYMENTS COMMITTEE  
OF THE ELECTRONIC  
TRANSACTIONS ASSOCIATION

# paper



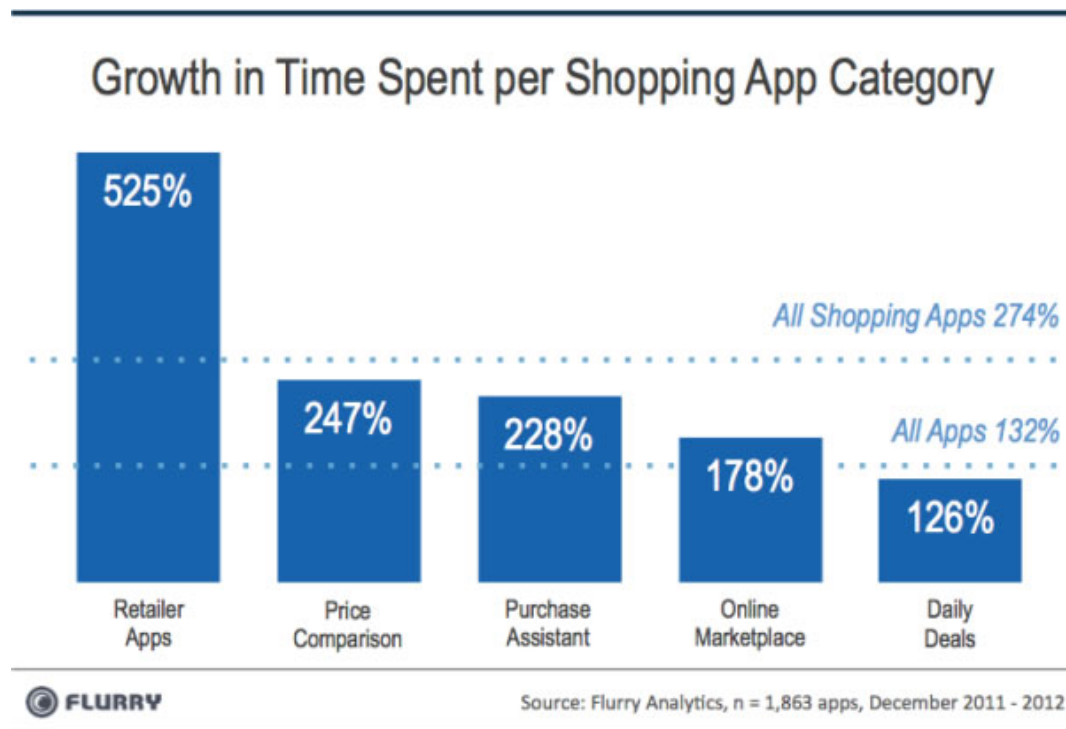
## Table of Contents

Overview .....	2
Before We Get Started .....	3
Current Status of Mobile Payments .....	5
Merchant Benefits.....	9
Understanding Merchant Risks and Costs.....	10
Mobile Payment Technologies .....	13

## Overview

With 6 billion mobile phone subscriptions globally, mobile communications is having a profound effect on people's lives, both socially and financially. In emerging countries, it provides an opportunity to access the Internet, as well as offers alternatives to cash. In developed countries, smartphones provide individuals with the ability to consolidate their payment cards, enhance security, and receive relevant offers directly on their devices. This paper will focus on the opportunities that mobile payments provide in developed countries.

Smartphones are rapidly becoming the dominant new phone type in most developed countries. As a merchant, this means that consumers are walking around your store with a little computer in their hands that allows them to compare prices, read reviews, find deals and inform their friends, all within the confines of your store. You need to be able to harness this new tool and ensure that it is working for you, not against you. If you are an online retailer, you need to leverage the power of this phenomenon to your advantage by providing a truly optimized mobile web and/or native application experience. If you are multi-channel, then you need to plan support for your mobile consumers, no matter the channel. To this point, below is a chart published by Flurry that lists the types of shopping services consumers are accessing from their mobile devices.



In order to gain real market momentum, mobile payments needs to do more than just provide a new way to initiate a payment at the register, online or through an app. They need to provide a richer shopping experience and allow both the merchant and consumer to interact more intelligently. A rich mobile commerce experience includes search, targeted offers, research, location-based offers, payments and sharing via social media.

There are many estimates on the size of the opportunity presented by mobile payments. Juniper Research predicts \$670B in transaction value by 2015, and Yankee Group believes that mobile transaction volume will be \$545B by 2015. In the US, nearly 87% of phones being sold are smartphones. Whichever prediction you believe, the fact remains that mobile is having a profound impact on consumers' purchasing experience and, as a merchant, you need to have a strategy on what to do and when to do it.

This task is not made any easier by the various mobile payment options that have been introduced and continue to be introduced on a regular basis. Further, the complexities of acceptance at both the physical and virtual POS must be addressed as part of any solution. Merchants both large and small are faced with trying to understand the effects that mobile payments will have on their businesses. What are the mobile payment solutions currently being implemented in the marketplace and how should I evaluate their potential impact on my business? What types of questions should I be asking? Where can I get unbiased answers to my questions regarding the costs and benefits of the various mobile payment options? These are the types of questions this paper will answer.

## Before We Get Started

The term *mobile payment* is being used in a wide variety of circumstances and can mean very different things to different people. In the context of this paper, we define mobile payments as the ability for a consumer to use a mobile device to initiate a payment at the point of sale and to interact with merchants for mobile offers and the tracking of loyalty points.

In addition, the Electronic Transactions Association (ETA) has compiled a comprehensive list of mobile payment terms that can be accessed at [www.electran.org/mobile](http://www.electran.org/mobile).

## *The Mobile Consumer*

Before exploring mobile payment processing, it is important to understand the mobile consumer and how technology affects their purchase experience. A helpful analogy is to review the growth of e-commerce over the last fifteen years, from a disruptive force of change to a mainstream purchasing vehicle for the majority of consumers. E-commerce empowered

consumers to browse, shop and purchase on their own terms. No longer did the consumer need to leave their home to make purchases; with just a couple clicks of the mouse and a credit card on file, the process was complete. E-commerce became an easy-to-use shopping experience with valuable benefits that motivated consumers to change their normal mode of purchase behavior. Mobile commerce has the potential to become an even larger agent of change by virtue of its ubiquity and effect on both retail and Internet commerce and the convergence of the two channels. Below are some consumer behavior drivers to consider:

- Social media -- including instant, electronic coupons and rewards -- is changing the way consumers act, react and shop with merchants
- Ease of use provided by the mobile wallet, enabling access to store cards, payment cards and alternate payment methods, in a format that mimics the online environment
- Access to information and the ability to make instant purchases through apps and the mobile web, therefore bypassing the traditional checkout process
- Young, tech-savvy consumers are comfortable sharing their purchase behavior with their friends.

For an effective mobile payment strategy, it helps to understand the mobile ecosystem as a whole. There are a number of other areas where mobile services will have a great impact on payments and, though not the focus of this paper, we wanted to provide you with a brief overview.

### *Shopping on the Mobile Device*

Shopping using a mobile application or a mobile website is technically a mobile payment. However, the mobile Internet shopping experience has progressed to the point where it is almost identical to a consumer's online, desktop experience, which has become a well-accepted, mainstream means of purchase.

### *Europay, MasterCard, Visa – EMV*

EMV is a global standard for inter-operation of integrated circuit cards and IC card capable point of sale (POS) terminals for authenticating credit and debit card transactions.

We will only mention EMV as it relates to the upgrade of existing POS terminals and how this may affect your plans for mobile enablement. We view EMV as just a new form factor for magnetic stripe that does not include a lot of the new capabilities found in mobile payment solutions. However, our recommendation is that when upgrading your POS for EMV, evaluate the requirements to support both mobile and EMV payments. If you want more information on EMV, we suggest you visit the site, <http://www.emvco.org>.

## P2P Payments

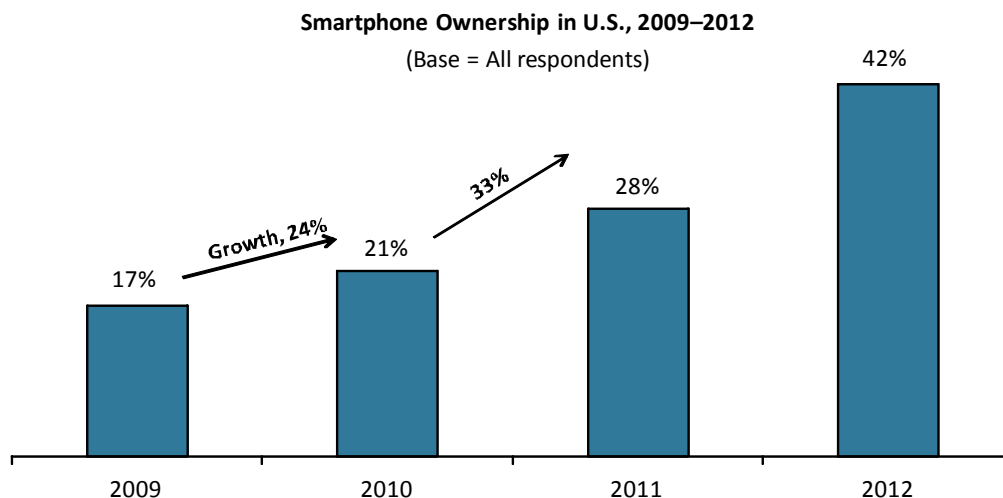
P2P (peer-to-peer payments) refers to the ability for one person to send money to another person directly from their mobile device. Many companies and banks offer these types of solutions. With P2P, consumers can initiate transactions that transfer money using existing payment rails via ACH, card networks or intra-account transfer.

## Current Status of Mobile Payments

Mobile payment is still in its infancy in the United States. Japan may be a possible roadmap, where mobile wallets have gained significant traction, with about 17% of the population (21M people) using a mobile wallet. In Japan, the mobile wallet is most frequently used for in-store payment, vending machines and transit.

Mobile payment in the US is growing rapidly. As stated in a recent FDIC report, “More than 87% of the US population now has a mobile phone and more than half of those mobile phones are smartphones. Nearly one-third of mobile phone users in 2012 have reported using mobile devices to make a purchase. Consumers spent over \$20 billion using a mobile browser or application during the year.”

One crucial factor necessary for the success of mobile payments in the US is a critical mass of smartphones in the marketplace. As can be seen in the chart below, smartphones will become the dominant phone type in 2013. As seen with the explosive growth of the Internet, it will be just a matter of time until consumers start incorporating these devices into their shopping experience.



Mercator Advisory Group

There have been a number of mobile payment deployments nationwide, and they range from closed-loop mobile applications to complete mobile wallets. These services can reside on the device, operate in the cloud, or utilize some combination.

Closed-loop applications are developed by a merchant for use by their customers to manage reward points, pay for their purchases, and redeem offers. One success story is the Starbucks mobile application that allows consumers to pay at the register by scanning a barcode on their phone and automatically accumulate their loyalty points. The Starbucks example highlights our previous assertion that a mobile deployment has to provide more than just a different method of initiating a transaction – it needs to provide consumers with added benefits like easier tracking of rewards points or targeted offers that save them money. As you evaluate the success of the various programs on the market, consider whether the success of these programs is unique to a particular business model or whether it is applicable to a wide variety of retail settings and retailers.

There have been a number of mobile wallets that have been deployed or announced. Our definition of a mobile wallet is an electronic account/storage locker accessible from a mobile device that can be used to store user payment information such as existing credit and debit cards and transfer value. A mobile wallet can store the user's credentials and payment mechanisms either on the device itself or in the cloud. Examples of mobile wallets include:

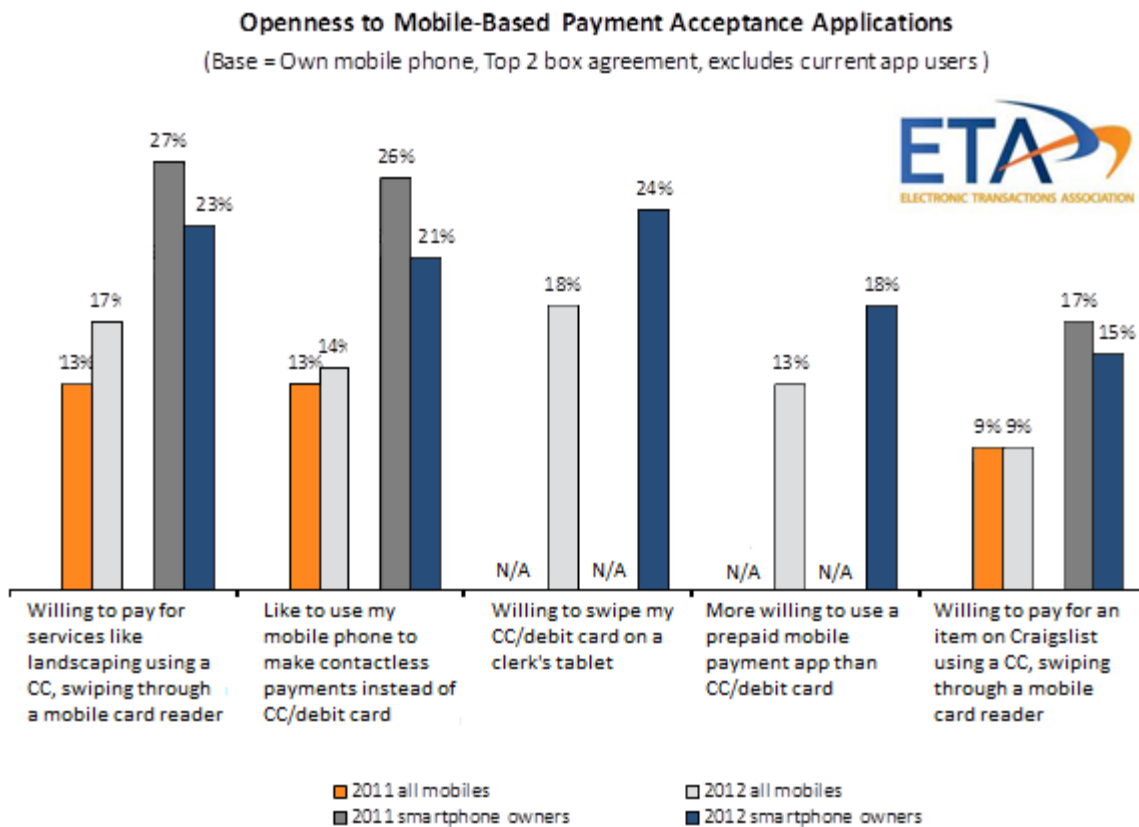
- Isis – A joint venture between AT&T, Verizon and T-Mobile, with partnerships with Discover, Visa, MasterCard and American Express. Isis has announced agreements with three card issuing banks – Chase, Capital One and Barclaycard - for loading funds into the Isis wallet.
- Google Wallet – Launched in September 2011, Google Wallet currently partners with MasterCard, Citi and Sprint. They launched the service using NFC (near field communication) but have since migrated to a cloud solution, and consumers can now utilize payment cards from any issuer or card brand.
- MasterCard – In addition to its partnership with Google Wallet and Isis, MasterCard has made enhancements to existing PayPass service to support mobile payments.
- Visa – In addition to its partnerships with Google Wallet and Isis, Visa has also launched an open mobile wallet for both Visa and non-Visa accounts and supports NFC-based payments. Visa has also launched the V.me service that will allow for single click checkout for online stores.
- PayPal Mobile Wallet – PayPal is supporting a wide range of potential payment forms, including cards and cloud based solutions.
- MCX – A consortium of large national chains including Walmart and Target that has announced their own mobile payment system called Mobile Customer Exchange (MCX). Few details have been provided for MCX at this time.

- Apple’s Passbook – A wallet designed to work on Apple hardware. At this time, Passbook is only used to store coupons or tickets, but it is assumed within the industry that it will at some point also offer payment capabilities.

In addition, there are some new and innovative mobile payment solutions:

- Carrier Billing – Companies like BilltoMobile, Payvia, Paypal and Boku provide the ability to charge a transaction to a user’s mobile phone bill.
- Tabbed-Out – Allows customer to interact directly with a POS system and never have to go to the register.
- Level-Up – POS system that uses a smartphone to read a 2-D barcode for purchase.

Below is a survey by Mercator Advisory Group, describing the types of goods or services that US consumers would purchase using their mobile devices.





## Merchant Benefits

As a merchant, the benefits of mobile payment acceptance will vary depending on your type of business and consumer demographics, but here are some of the benefits to expect when deploying a mobile payment system.

1. **Consumer Data** – Many mobile payment services also include online transaction reports. These reports can provide a better understanding of your consumer’s behavior and information on how to better service their needs. For example, you could use this data to ensure that the favorite products of your best customers are always in stock, or that you deliver targeted, promotional offers for products that consumers desire.
2. **Consumer Control** – Mobile payments empower your customers and allow them to pay with their preferred method and funding mechanism, while easily controlling all of their loyalty and reward points in a single place.
3. **Flexibility at the Register** – There are mobile payment solutions that allow consumers to check out directly from their mobile device and never have to go to your register. Mobile technologies allow consumers to make purchases utilizing their devices anytime, anywhere. Merchants can enable consumers to shop utilizing mobile browsers or apps while at home or in the store. When ready to complete the purchase, the consumer simply executes the transaction. The merchant’s systems receive notification and the goods are ready for pickup at the customer service counter. This can also be coupled with a mobile checkout or tablet based POS system that allows the merchant to interact with the consumer and complete the sale on the show floor.
4. **Speed of Checkout** – If a merchant participates in a daily deal program or offers specials via coupons, these can all be automatically administered by the consumer utilizing their mobile device. Scanning a QR code for a payment tied to an offer can be significantly quicker than keying the offer into a computer, then processing the payment.
5. **Enhanced Security** — Mobile devices provide more security than standard mag stripe credit cards. Phones can be locked with a password; all mobile payment applications can be set to require a password, and phones can be configured to have all of their data wiped remotely.

## Understanding Merchant Risks and Costs

Like any service that consists of transferring money, there is the possibility for fraud and deception. It is safe to assume that, as mobile payments become more popular for consumers, criminals will start to target mobile payments. Fortunately, many of the lessons learned with the rollout of e-commerce translate directly to mobile.

### **Risks**

Here is some information contained in the recent FDIC Supervisory Insights paper published December 2012. To view the complete report, please go to <http://www.fdic.gov/regulations/examinations/supervisory/insights/siwin12/mobile.html>

“Mobile payments present the same types of risks to financial institutions associated with many traditional banking-related products, including Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) compliance, fraud, credit/liquidity, operations/IT, reputation, and vendor management.

“The regulatory expectations for managing mobile payments are generally consistent with those associated with other financial services delivered through more traditional channels. No safe harbors or carve-outs from coverage for mobile payments exist. Thus, mobile payments providers must determine how to comply with existing legal requirements when the application to mobile payments may not be readily apparent.”

“To date, no federal laws or regulations specifically govern mobile payments. However, to the extent a mobile payment uses an existing payment method, such as ACH or EFT, the laws and regulations that apply to that method also apply to the mobile payment. For example, a mobile payment funded by a user’s credit card will be covered by the laws and regulations governing traditional credit card payments.”

In addition, industry associations are creating their own best practices for mobile payments.

- ETA Mobile Payments Best Practices and Guidelines document can be viewed at [www.electran.org/mobile](http://www.electran.org/mobile).
- Payment Card Industry “PCI Mobile Payment Acceptance Security Guidelines for Developers” and “PCI Mobile Payment Acceptance Security Guidelines for Merchants as End-Users” documents can be viewed at [https://www.pcisecuritystandards.org/documents/Mobile\\_Payment\\_Security\\_Guidelines\\_Developers\\_v1.pdf](https://www.pcisecuritystandards.org/documents/Mobile_Payment_Security_Guidelines_Developers_v1.pdf) and [https://www.pcisecuritystandards.org/documents/Mobile\\_Payment\\_Security\\_Guidelines\\_Merchants\\_v1.pdf](https://www.pcisecuritystandards.org/documents/Mobile_Payment_Security_Guidelines_Merchants_v1.pdf)
- CTIA “Best Practices and Guidelines for Mobile Financial Services” can be viewed at [http://files.ctia.org/pdf/CTIA\\_MFS\\_Guidelines\\_BP\\_Final\\_1\\_14\\_09.pdf](http://files.ctia.org/pdf/CTIA_MFS_Guidelines_BP_Final_1_14_09.pdf)

We suggest that you take some time to become familiar with these best practices and ensure that whatever mobile payment solution you select will follow these guidelines.

Some of the guidelines that should be implemented include but are not limited to:

- Authentication
  - Authenticate user identity with username/password combined with risk based authentication techniques such as velocity checks, etc.
- Disclosure of Material Terms of Purchase
  - Provide users with clear terms for each purchase, including a description of the product, taxes, surcharges and any other fees. Complete terms can be offered as a link to external document or may be part of the physical or electronic receipt.
- User Authorization
  - A checkbox that includes express authorization for a transaction, a confirmation screen and a transaction cancellation option.
  - Separate and specific opt-in for any services regarding location tracking or receiving additional offers.
- Receipts, Order Status and Account Information
  - Receipts for mobile purchases should be provided via email, SMS message or via a website.
  - If deploying a mobile app or mobile website for your consumers, provide users with information about their order including the order status, completed transactions, refunds and cancellations.
- Privacy Policies
  - When utilizing location based schemes or technologies that share data between loyalty providers, it is important to have clear legal privacy policies designed to protect consumer information. For further information on privacy policies, please review the ETA Best Practices and Guidelines document, which can be found at [www.electran.org/mobile](http://www.electran.org/mobile).

## **Costs**

The costs for a mobile deployment will vary depending on the existing capabilities of your POS system, but here are some of the expenses you can expect.

1. Hardware Upgrade – It will be necessary to upgrade your POS in order to accept mobile payments. We will go into more detail on these options in the Mobile Technology section of the paper.
  - a. New EMV/Contactless Terminal – A terminal with contactless and EMV capabilities will cost between \$250 - \$600.
  - b. Adding Contactless NFC Readers - If you are utilizing a traditional credit card terminal, it may be as simple as adding a contactless card reader to process EMV

applications. A contactless reader will cost between \$50 - \$150 and requires a terminal application that supports a contactless reader. Consult your merchant services provider for specific costs and compatibility. There may be additional costs associated with adding a contact reader to an integrated POS system. Because there are different “flavors” of NFC, please clarify the capabilities of the NFC reader before purchase.

c. Scanners

- i. Laser vs. Optical – To accept bar code based mobile payments, it may be possible to use existing hardware. However, most scanners today use laser technology, which has difficulty reading a barcode on a mobile device due to glare. Optical scanners are recommended when scanning barcodes on a device. If you do not have a compatible scanner or need a scanner, the prices range from \$100 - \$750 depending on capabilities. As a starting point, we suggest visiting the Scansource website for more details at <http://www.scansource.com>.

2. POS Software Upgrade

To accept mobile payments, it will be necessary to make changes to your POS systems. In some cases, it may be as simple as adding a contactless card reader. In other instances, you may need to upgrade your barcode scanner, add new tender types, change receipt verbiage, integrate with your ordering systems, or implement customer facing devices. Fortunately many POS software providers are currently in the process or have already rolled out mobile payment processing capabilities. We suggest that you speak to the company currently providing your POS systems to inquire as to their mobile payment support capabilities. When doing so, make sure to inquire as to their NFC and mobile wallet capabilities (i.e., which wallets they support), and operational changes required in order to roll out their mobile payments program. We also recommend as part of any upgrade discussion, you evaluate the support requirements for EMV processing.

In addition, there are some new mobile payments solutions that provide an online dashboard for reviewing your mobile payment transactions.

## Questions to Consider Before Deploying Mobile Payments

Before you deploy any type of mobile payment solution, there are a few key questions you should consider.

*Are your consumers tech-savvy and how many of them own a smartphone?*

Our definition of a smartphone is a mobile phone built on a mobile operating system, with more advanced computing capability and connectivity than a feature phone. In order to take advantage of mobile payments, people will need to have a smartphone, so it would be beneficial to have a ballpark estimate of the percentage of your consumers owning a smartphone. There is no fixed percentage that will tip the scale one way or the other as the benefits of mobile payments will vary greatly from business to business. This is a decision that you as a business owner will need to make based on your knowledge of your customer base, their acceptance of new technologies, and their receptiveness to targeted, mobile offers.

*Will your consumers increase their spending in your store with an easy-to-use loyalty program or with targeted mobile offers?*

One of the major benefits of a mobile payments solution is the ability to learn more about your customers' buying habits and, in turn, be able to better service their needs. This could be in the form of targeted mobile promotions that will entice your customers to visit your store more frequently to save money on products that they have purchased in the past or inform them of related products to increase the breadth of their purchasing.

*What are the current capabilities of your POS system?*

This information will help to determine the cost and amount of work required to fully support mobile payments. If your POS is already connected to your back-end applications like inventory and ordering, this will reduce the amount of work needed for integrating offers into your mobile deployment. If your POS is already securely connected to the Internet, it may be possible to also support enabling consumers to pay via the cloud and exploit the convergence of online to offline. Also, if you already have optical scanners, they can likely be used to immediately start redeeming 2D / QR barcodes without additional hardware costs.

A barcode is an optical machine-readable representation of data relating to the object to which it is attached. 2D barcodes are two dimensional and are sometimes referred to as Quick Response (QR) codes. Examples of a 2D barcode are below:



### *How will information on the consumers' mobile purchases be stored and protected?*

Make sure you understand how the mobile payments company you will be working with protects and secures your customer's information. For more information on the rules and guidelines to follow, refer to the ETA's Mobile Payments Best Practices and Guidelines document at [www.electran.org/mobile](http://www.electran.org/mobile). In addition, you should ensure your provider is validated as PCI compliant. You can refer to the PCI Best Practices document at <http://www.pcisecuritystandards.org>.

Some mobile payments applications allow you to determine your customer's location based on the GPS chip in their mobile device. This technology can provide a way to deliver offers to your customers when they are in the vicinity of your store. As a general rule, this type of targeted marketing should only be deployed with the opt-in permission from your customers.

## **Mobile Payment Technologies**

If you determine that accepting mobile payments is a possible fit for your business strategy, below is a listing of the major mobile payments technologies currently on the market.

<b>TYPE</b>	<b>Initiation Method</b>	<b>POS Needs</b>	<b>Processing Method</b>
<b>EMV</b>	Standard for chip cards and acceptance of cards at the POS, including terminals for authenticating credit and debit card transactions.	POS terminal capable of reading EMV specified RFID signal.	Consumer inserts chip or EMV-capable contactless card into the POS reader. Process flows as normal credit or debit card transaction, with a deeper level of security and authentication than mag-stripe.
<b>NFC or Contactless</b>	Short-range wireless RFID technology using secure authentication and credentials on the mobile device to transmit card information to the POS.	POS terminal capable of reading RFID and software capable of processing the NFC transaction in the POS or credit card terminal.	NFC as it exists today is a "tap-and-go" process. Once read, the transaction processes as a regular credit or debit card.
<b>Image-based, Barcode or Cloud-based</b>	Consumers utilize a mobile wallet or application on the mobile device to securely access their account data. Once authenticated, a barcode or other image is presented on the mobile, which the merchant uses to process the transaction. In a cloud example, the necessary info to process is conveyed over the air to the POS.	Optical image scanner capable of reading 2-D barcodes, depending on the wallet being accepted. For cloud based, a POS system capable of securely being connected to the Internet.	POS system is enabled to scan the barcode as a tender type. Transaction settlement is typically between the wallet provider and the merchant. For cloud based, the POS accepts the card info and processes it through its existing connections.
<b>Carrier Billing</b>	The ability to purchase goods	New hardware is not	Process is between the carrier billing

	and services and have them charged directly to a user's mobile bill or account.	required, but a relationship with a carrier billing provider is necessary.	system and the merchant's host environment. Today, this is not used in retail nor for physical goods.
--	---	--	---

### ***NFC – How it Works***

NFC (Near Field Communications) is also referred to as contactless because the device does not actually make contact with the acceptance device to be read. Common applications for NFC include transit passes and security access cards. MasterCard's PayPass and Visa's PayWave cards also utilize NFC technology. In general, NFC is a protocol that allows for the secure transmission of data, utilizing Radio Frequency ID between two complementary devices that are in close proximity. For NFC payments, this means the secure transmission of card or payment data from the mobile to a contactless reader attached to the POS. As with a building card, PayPass card or transit card, NFC technology allows the consumer to "tap and go" at the POS when using an NFC enabled device.

In the US, the initial foray into NFC initiated mobile payments is with Isis, a consortium of the major telecom providers and card brands. In addition to Isis, the Google Wallet utilizes NFC for payment processing in a similar manner. This current rollout follows the same processes as the contactless cards first introduced into the market in 2002. There are other payment programs where NFC is used as the communication method, with the card or payment data taking an alternate route for the payment. With the Isis and Google Wallet NFC models, merchants can accept mobile payments from consumers using downloaded applications on NFC enabled mobile devices. For merchants, the process is nearly identical to processing a contactless Visa or MasterCard.

In order for consumers to use NFC, they will need an NFC enabled mobile device, a downloaded payment application and an associated payment card for processing transactions. Through a process with the various constituents in the payment stream (e.g. card issuers, payment platforms, service providers), the application is activated for use in processing NFC payments. This process includes establishing credentials and authentication mechanisms designed to prevent fraud.

When a consumer elects to make a payment utilizing the wallet, they simply open the application, authenticate themselves via password, select the card type, and the device is ready to "tap and go" when the terminal or POS prompts the consumer. At this point, the merchant's contactless reader establishes a secure connection with the mobile device, and once authenticated, receives the transaction information and the process flows as a traditional payment card.

It will be necessary to upgrade your terminal or POS in order to accept NFC payments. Once your equipment is upgraded, which may require an update to your software and an NFC

capable reader, you should also be able to process both mobile-based NFC payments and the millions of contactless credit and debit cards already issued by Visa and MasterCard.

Below is an example of an NFC transaction:



### ***Barcodes – How they Work***

At this time, barcode payments are the most deployed mobile proximity payments service in the US. The customer registers for an account with the barcode system, creates a username and password, and designates funding sources. This payment information can be stored on the retailer's own server or can be stored on a third-party server in the cloud.

You will need to select a mobile barcode provider, install their software into your system, and install optical scanners for best results in scanning from a mobile device. Your customers will also need to download a mobile application onto their mobile device in order to use the service.

The advantage to a barcode payment solution is that it provides the features and convenience of mobile payments without a major investment in hardware. One disadvantage to barcode solutions is that consumers may need to download many different applications for use at their favorite stores. As mentioned previously, a 2-D barcode reader will cost between \$50 - \$150.



Below are several examples of barcode scanners:



Cloud Based QR code processing is a service that allows a consumer to access their cloud based or local mobile wallet connected to a mobile web site or a native application and initiate both ordering and payment to a physical POS system. An example of this is where a consumer opens a tab at a restaurant on their device, shows their server a code and proceeds with ordering without having to hand their card to the server or requiring specialized portable terminals. When they are done, the customer can close their tab without having to wait for the server, apply their chosen gratuity, and leave the establishment.

## **Carrier Billing**

This service allows a consumer to charge a purchase directly to their wireless phone account. The charge appears on the user's monthly phone bill. This service can reduce the friction from mobile purchases by eliminating the need to enter a lot of data onto a small screen. The user simply provides their mobile number to initiate the transaction. At this time, carrier billing is restricted to non-physical goods like virtual currency, online subscriptions and online dating services.

Below is an example of a carrier billing transaction from a desktop browser and a mobile browser.



## **Understanding the Wallet**

The mobile wallet is a mechanism whereby the mobile device has access to a variety of payment vehicles (ACH, debit, credit, prepaid, gift) via an application accessed through the mobile device. The mobile application provides a secure mechanism for access to the wallet along with various authentication mechanisms which must be validated prior to making the final payment. With some wallets, the payment information is contained on the mobile device, while other wallets utilize the cloud or remote systems for authentication, communication and payment processing.

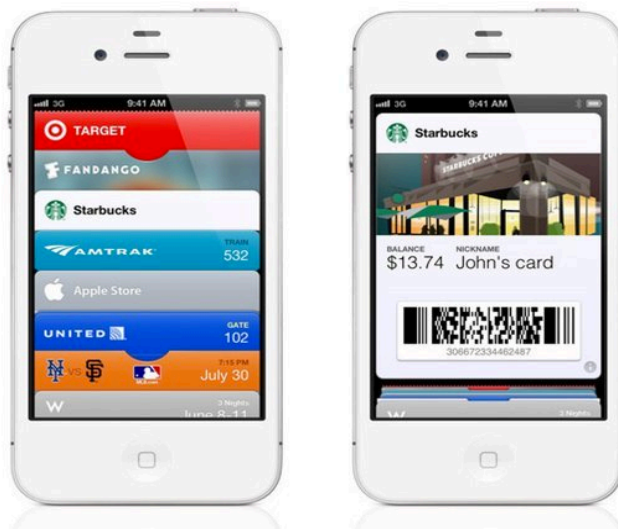
In addition to accessing payment vehicles, the wallets can access loyalty programs, coupons, instant rewards and daily deal promotions, all of which can be redeemed via the mobile device at the POS. While the NFC payment schemes are classified as a wallet, this section focuses on the various non-NFC based wallets and how these wallets can also be used to process payment transactions.

## Mobile Wallet Transaction Components

A mobile wallet typically utilizes the following components when processing transactions.

- The mobile application used by the consumer, which can be a pure third-party wallet such as Google Wallet, Apple Passbook, PayPal, or any other wallet used by the consumer. A wallet may also be part of a proprietary store application.
- A mobile wallet allows for initiation of payment at the POS by providing the consumer with access to a funding account and settlement to the merchant.
  - Consumers may utilize a wallet to access payment methods established with the wallet provider, including, but not limited to, their credit card, debit card, checking account, store credit or a prepaid account.
  - Carrier billing is an option with some wallets, with the transaction being billed to the consumer as a line item on their monthly cell phone bill.
  - The wallet provider is responsible for initiating the charge to the consumer.
  - The payment vehicle may be in the form of a prepaid daily deal redemption, such as Groupon or Living Social, and the payment mechanism may include other discounts or offers in the form of a coupon.
- Payment validation, authorization and redemption functions are performed by the wallet provider in concert with the POS and the funding mechanism.
- A payment token, or redemption identifier, is used by the consumer in place of a payment card, check or cash when paying for goods and services. These redemption identifiers are usually one of the following:
  - Barcode: The POS scans the barcode, validates the barcode with the wallet provider, and closes the transaction for payment on the wallet host.
  - QR Code: Works the same as a barcode, however, the physical characteristics of the code are different.
  - Alphanumeric Code: Displayed on the mobile for entry by the cashier into the POS.
- A settlement infrastructure is part of any mobile wallet based scheme. The settlement infrastructure obtains funds from the consumer's payment vehicle for payment to the merchant. The settlement infrastructure provides merchants with the ability to receive payment for validated funds and manage consumer disputes. For practical purposes, the settlement infrastructure provider is typically the wallet provider, but may also be the merchant services provider.

### *Example of a Mobile Wallet*



### **Paying with a Mobile Wallet**

Once a user has selected a mobile wallet, they then must load their payment information into the wallet. This process is similar to loading payment information to online accounts. For instance, if a consumer already has a wallet available for online purchases, the consumer can often activate that exact same wallet on their mobile device. The consumer may select a default payment card, or the wallet provider may steer the user to the cheapest payment method based on a particular transaction. When the consumer loads the wallet application on their mobile device, an authentication process takes place between the mobile device, the application and the wallet stored on remote servers. At this time, credentials are established, and the wallet is ready for retail payments.

When paying with a mobile wallet, the consumer opens the wallet application and enters a PIN to authenticate the user and transaction. Once opened, the consumer selects the payment method, and a barcode is displayed on the mobile device. Keep in mind, for the wallet to work, the consumer must have Internet access.

Below is the step-by-step process for a mobile payment:

- Upon entering all of the goods and obtaining a total, the cashier asks for payment.

- A mobile payments enabled POS typically asks for the tender type. This is evolving to include the typical payment types such as cash, check, debit, credit, along with the wallet providers, such as Google Wallet, PayPal, Apple Passbook, etc.
- When the consumer shows the barcode, the cashier scans the barcode displayed on the consumer's mobile device.
- The merchant's POS communicates with the wallet provider to initiate the transaction by sending a message that includes the merchant information, payment amount and other elements required by the wallet provider. This process is similar to sending a credit card authorization request.
- The wallet provider may also send an SMS or e-mail message to the consumer indicating transaction processing has been completed.
- The wallet provider settles with the card brands, ACH networks or other funding mechanism chosen by the consumer.
- At the end of the day, a settlement process occurs between the merchant and the wallet provider to balance the funds due.
- The wallet provider pays merchants on a pre-determined schedule.

### **Ordering with the Mobile Wallet**

The example above is for a retail transaction. Alternatively, when ordering from a mobile wallet, the user initiates the order and payment from an application, or perhaps a mobile browser, accessing the Internet through the mobile device. This transaction typically requires the consumer to pick up the goods or services at the retailer location or have them delivered. As with the wallet initiated transaction mentioned above, this transaction is completed when the consumer presents a bar or QR code to the cashier to scan and the necessary information is communicated over the air to the POS.

A twist to this scheme involves geo-fencing, or the utilization of GPS, to identify the consumer's location and the ability for a merchant to deliver offers or prepare pre-purchased merchandise for pickup. SquareUP is launching such a service, and Starbucks and Google have rolled out this type of offering to a large fast food chain. The advantage to the consumer is that they can place their order while still at work or in the parking lot, rather than waiting in line. A coffee drinker can set a recurring order for the same drink any time they walk into a store.

The advantage to the merchant is that it can prepare orders in advance, or if using geo-fencing technology, place orders in the queue as soon as the consumer walks in the door. The consumer simply approaches the POS, indicates they have an order for pickup, then utilizing their mobile wallet, scan their QR barcode and complete the exchange. Geo-fencing works only when the consumer enables their device for GPS tracking.

Ordering through mobile devices requires significant technology changes within the merchant's POS and operational infrastructure. These changes may include:

- The ability to scan a QR or barcode from a mobile device, which may require an upgrade to 2D or 3D scanners depending upon the consumer application in use.
- The POS may need to be programmed to identify the transaction as a completely different tender type. While the transaction may ultimately be drawn from a Visa or MasterCard, the merchant may be paid by Google, PayPal or an entity other than their merchant services provider. Accounting, dispute, and other finance controls may need to be implemented for proper support.
- Merchants that provide same day store pickup when ordering online may already have the infrastructure in place to support an application that allows consumers to order through a mobile application. Merchants without an online ordering system will need to implement the infrastructure to support store pickup. This may include modifications to their inventory management, order processing and other systems.
- When using a geo-fencing type of application, the merchant's POS systems will require deeper integration with the mobile application ecosystem in that the order will be delivered from the cloud, rather than a cashier entering the information into the POS. Further, customer service and consumer training are paramount to a successful implementation of this type of service.

## Mobile Devices for Payment Acceptance

There are various factors you should consider when evaluating a mobile payment acceptance solution. These factors include transaction volume, scalability and costs for both hardware and software.

Mobile card readers (dongles) range from small swipe devices that plug into a smartphone's headphone jack to larger, wrap-around units referred to as sleds or sleeves. These larger devices are more expensive but offer capabilities for encrypted PIN pads and printers.

For smaller merchants or tradespeople, a simple payments acceptance application with a plug-in dongle may be the answer. These solutions use a consumer device such as an iPad or Android tablet as the POS terminal, which can greatly reduce deployment costs. Proprietary devices, such as a traditional wireless credit card terminal, are often significantly more expensive than a tablet or smartphone. With these consumer device solutions, the apps and dongle are typically free or offered at a minimal fee, as the costs are incorporated into the payment processing fees.

Typically these applications provide little or no integration into your back-end inventory and financial applications. However, they usually provide a web dashboard to enable viewing transaction history.

Larger merchants and national chains will benefit from having a mobile payments solution fully integrated into back-end systems for inventory tracking, replenishment and other critical data mining functions.

A typical mobile payment acceptance program includes the following:

- A card swipe dongle connected to the mobile device via the audio port, data port or Bluetooth.
  - SPECIAL NOTE – Most dongles encrypt the card data in the card reader itself, rendering the card data inaccessible to any systems other than the authorization platform. To ensure maximum protection of consumer data, verify that the card swipe device being utilized is an encrypted reader.
  - For information on card data security standards for mobile devices, you may visit the PCI Security Standards Council website at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org) or the ETA website at [www.electran.org](http://www.electran.org).
- An application downloaded directly from the service provider or through the online store such as Apple's App Store or Google Play.
- Transactional reporting available through the application or through a web interface at the back office.
- E-mail receipts containing digital signatures of the customer captured on the screen.
- Secure logon and user IDs, protecting rogue use of the application.
- The applications typically communicate directly to the authorization processors using the cellular data networks or through WiFi. However, there are applications and services designed to send the data to corporate hosts or in-store POS applications. Companies such as NCR and IBM offer these types of services.

In general, accepting payments on mobile devices is proven and works well. However, utilizing mobile devices to accept payment does come with a few risks, including:

- Access to and reliability of the cellular or Wi-Fi network.
- Durability of the card readers attached to the mobile device.
- Sensitivity of the device reader, which may or may not work across different mobile devices, especially with the various Android operating systems.
- Managing security and anti-virus programs on a mobile device is more difficult than managing a PC.
- Customer reluctance to provide an e-mail address for receipt purposes.
- Broad privacy policies of some payments providers may not be acceptable for your organization.