A First Data White Paper

Transforming the Customer Experience: The Promise of Mobile Wallets

By:
Christopher Cox
Vice President, First Data

Scott Sanchez
Vice President, First Data

© 2013 First Data Corporation. All trademarks, service marks and trade names referenced in this material are the property of their respective owners.
Introduction

The planets and stars of the Information Age—that is, the technologies, applications and partnerships—are now aligning to bring us into a new age of commerce. Dubbed “Universal Commerce,” it is commerce that happens anytime, anywhere, and on any type of device. It blurs the lines between in-store commerce, eCommerce and mobile commerce such that many aspects of commercial activity are seamlessly integrated into one experience. From a consumer’s perspective, shopping, payment, marketing (i.e., offers and coupons), loyalty, and money management all blend together in both offline and online experiences.

Consumers’ purchasing patterns are shifting, driven by the broad availability of self-selected, timely and relevant information. They are online, they are mobile, they go to stores, they socialize, they solicit and share opinions, they compare before they decide, they want convenience and choice, and they like incentives, rewards and value for their money. To many people, particularly Millennials who have always had the Internet and mobile phones in their lives, this isn't just a way of commerce—it's a way of life. They can’t imagine a lesser experience.

Accordingly, to become and remain relevant in a Universal Commerce world, merchants and financial institutions need to adapt quickly. It’s important that they not only recognize the digital influence on today’s commerce but also leverage it to their own benefit. A wave of innovation in mobile technology is disrupting and enabling integration across consumers’ full shopping and financial services journeys. This innovation includes smart phones and tablets combined with WiFi and 3G/4G wireless communications and millions of new mobile applications. Clearly, mobile devices are at the center of Universal Commerce, and they serve as the access points to all that is possible. (See Figure 1.)

If mobile devices are the access points to Universal Commerce, mobile wallets are the points of arrival. Leather wallets are now migrating to mobile devices, transforming the way people access and manage their financial information; pay for goods and services; make the most of offers, discounts and loyalty programs; and communicate and share good deals with their circle of friends.
Mobile wallets are a fundamental building block of Universal Commerce. They are the means for consumers to transact business and make payments electronically—anytime, anywhere. (See Figure 2.) Furthermore, mobile wallets can support exciting new functionality that could never be offered by a leather wallet—including automatic loyalty point redemptions and location-based marketing offers. Mobile wallets promise to transform much more than just payments: they provide a customizable platform for merchants and financial institutions to create richer customer experiences and deeper client engagement.

In this paper, we discuss what a mobile wallet is (i.e., what it can do), some common implementations based on available technologies, and what merchants and financial institutions should be doing now to test (or jump into) the Universal Commerce waters with mobile wallets and related services.
First, some basic definitions

We need to start with some broad definitions to clarify points made throughout this document. It’s important to note that there really aren’t industry standard definitions for these terms yet, as the roles, features and functions they portray are still evolving.

• **Mobile payment** – a payment transaction that is initiated, accepted, and/or facilitated via a mobile device, wherever a consumer happens to be. Quite often a mobile payment involves using a mobile device such as a smart phone or tablet computer, but it could just as easily involve using a kiosk, ATM or website. Payment credentials are presented at or downloaded to the point of sale (POS) and the payment transaction is processed as usual. Two of the more common utilizations of mobile devices to effectuate a mobile payment today include the following:

1. A mobile device emulates a consumer’s card and a transaction is initiated by presenting the device to the point of sale. (See Figure 3.)
2. A mobile device (usually with an attached card reader) is the merchant’s point of sale terminal and the transaction is initiated by swiping card or manually entering payment information. (See Figure 4.)

• **Mobile wallet** – an application platform or system that provides access to a variety of financial or commerce related functions or services, often (but not exclusively) via a mobile device. The most basic function of a mobile wallet system is to hold a collection of stored payment credentials, coupons, offers, etc. that can be used to initiate payment and redemption transactions. The mobile wallet also includes the application that manages all the functions and services, the payment account that goes into the application, the technology interface for storing and transmitting payment information, and a variety of additional value-added services beyond payment capabilities.

• **Service provider** – any organization that provides a service via a mobile wallet. Examples of service providers include a financial institution that issues a payment card, a merchant that offers coupons or discounts, and a mobile network operator that provides location-awareness services.

• **Technology interface** – the means by which payment credentials are securely stored and then presented at the point of sale. For example, the Starbucks mobile app presents the credentials in the form of a 2D barcode that is read by a barcode scanner at the POS. The 2D barcode and the scanner system together form a technology interface to get the payment credentials into the transaction.
Payments: essential, but alone not sufficient for success

A basic, necessary function of a mobile wallet is to support a consumer’s ability to make mobile payments. This includes securely storing payment credentials, either on the device or in the cloud, and making them available when needed at the point of sale. However, while it is critical that a mobile wallet provides payment functionality, this capability alone is not sufficient. A mobile wallet must also enable consumers to perform other value-added activities, such as checking their payment account balance, collecting and redeeming loyalty rewards, and accepting and managing receipts for purchases made. A wallet that is owned by or closely associated with a specific financial institution also may provide mobile banking services. Regardless of the extra financial or payment services a wallet supports, by and large, the wallet is intended to enable the consumer to make payment for goods and services.

How a payment is initiated is quite dependent on the technology interface of the mobile wallet. The most common implementations in use today are discussed in the mobile wallet technology section below.

The value-added functionalities that make a mobile wallet compelling

While the notion of using a mobile phone as a payment instrument is interesting, it’s not what will drive consumers to adopt mobile wallets. Mobile wallets are much more enticing when you start to think about all the things that can only be done with a digital platform and that could never be done with a leather wallet. For example, a geolocation service on a mobile phone can determine with great accuracy where a person is at the moment. Now, combine that information with a timely offer for a nearby restaurant or shop and the wallet holder might be enticed to eat lunch at that restaurant or make a purchase in that store. The actionable intelligence of the mobile wallet system knows where the person is and what they might want at that moment. This is a fundamental aspect of Universal Commerce.

The kinds of value-added services that will drive adoption of mobile wallets include:

- **Merchant offers, coupons and discounts** – These can even be tied to the use of specific payment instruments in the mobile wallets, such as merchant funded loyalty incentives offered by a specific issuer.
- **Location-aware offers and services** – These offers are in context to a consumer’s current location, making them both time-sensitive and more relevant for the moment.
- **Loyalty program incentives and redemption** – These can be tied to a payment instrument in the wallet or to a specific merchant, or to both.
- **Mobile banking** – The consumer can have the convenience of online banking in their wallet to pay bills, look up account information, make account transfers and electronic deposits, send or receive cash electronically, and so on.
- **Comparison shopping** – Mobile applications can help a consumer compare products and prices and determine which merchant offers the best deal on a product or service.
- **Management of offers, incentives and rewards** – As more merchants and financial institutions send out offers and incentives, it will become more cumbersome for the consumer to keep track of them all, and to know when incentives are about to expire. Applications are springing up to manage these offers in a person’s mobile wallet system.
• **Ticketing** – A consumer can buy and store his tickets for air, bus, rail, ferry and other forms of public transportation, as well as for movies, concerts, sporting events and virtually anything else that requires a ticket.

• **Receipts** – A mobile wallet can store and organize customer receipts—not only for mobile transactions, but any transaction at a retailer with electronic receipt capabilities

• **Personal identity credentials** – A mobile wallet doesn’t have to be limited to commerce applications. Secure credentials in a wallet could be used for building access or other applications where personal identification is required.

More value-added services will emerge as mobile wallets grow in popularity and usage. The possibilities are almost limitless.

### Mobile Wallet Technology Options in the Market

There was a time a few years ago when “mobile wallet” was equated with “NFC,” or near field communications. Experts assumed that payment credentials would be stored in a secure element (SE) on a mobile phone and the credentials would be transmitted to a card reader through NFC technology. While this kind of implementation is growing in usage today and will remain the de facto industry standard for mobile wallet payments, it’s not the only option anymore. NFC has been slow to come to market in the U.S. because of hardware requirements for the handset and the POS device, opening the door for innovative companies to develop other ways to enable mobile payments. Nevertheless, NFC continues to represent the most promising path to widespread mobile payment adoption.

In fact, there are numerous technology interfaces that enable mobile payments today, providing merchants and consumers with a range of options to support various needs. For example, if the consumer is at a grocery store, at a farmer’s market, or at a fuel pump—the situations will help dictate what technology interface is used. The question for mobile wallet developers is how to maintain a consistent enough user experience so that consumers don’t have to relearn new ways to do things at every retailer.

Smart phones have overtaken feature phones in popularity as more than half of all American mobile customers today own a smart phone. What’s more, at the end of 2011, there were 331.6 million wireless subscriber connections in the U.S. This vast number represents a huge array of device types, brands, models and configurations. With so much handset diversity, it’s difficult for mobile wallet developers to know what kind of device or hardware configuration a consumer will use for their mobile wallet platform. Accordingly, it is vital that they worry less about the individual technology, and instead focus on creating a compelling value proposition for consumers. Developers should plan to support the most likely device configuration scenarios and leading mobile wallet technology interfaces—and avoid counting on a single hardware standard to emerge.

In the forthcoming sections, we look at three logical scenarios that are already addressed by mobile wallet solutions and that have some level of momentum in the marketplace. The list is by no means comprehensive, but we have chosen to focus on today’s dominant scenarios:

1. The consumer has a device with both a secure element for storing the payment credentials and an NFC connection for sending the payment information from the phone to the POS reader.
2. The consumer has a device with an NFC connection, but no secure element for storing payment credentials.
3. The consumer’s device has neither a secure element nor an NFC connection.
Note that the technology interface part of the wallet is largely independent of the payment part of the wallet. The interface solutions discussed below can work with practically any payment type: credit, debit, prepaid, corporate card, closed loop or open loop cards—any of them can be made to work with a mobile wallet. What’s more, the technology interface is simply the means to store and transmit payment credentials. It is separate from but closely integrated with a wallet application (software) that manages the features and functions available to the consumer; for example, making payments, managing offers, tracking rewards, and so on.

**NFC-based solutions—with a secure element to store credentials**

Two or three years ago, this technology configuration was considered the minimum to support a mobile wallet system, largely because it most closely replicates the current plastic card environment. A secure element inside the phone stores the payment credentials, thus providing card emulation.

The phone is also equipped with an NFC chip and a radio frequency antenna. When the user presents the phone at a POS or acceptance device that has an NFC reader, the payment credentials are securely transmitted from phone to reader. The phone acts just like a card so this is considered a card present transaction.

The initial release of the Google Wallet in 2011 is perhaps the best known example of this technology interface. Because of the hardware dependency of the NFC and SE chips, wallets based on this kind of configuration are often driven by the owner of the handset or the MNO that supports the handset.

**The underlying technologies**

**Near field communication (NFC)** is a set of standards for smartphones and similar devices to establish radio communication with each other by touching them together or bringing them into close proximity, usually no more than a few centimeters. NFC standards cover communications protocols and data exchange formats, and are based on existing radio frequency identification (RFID) standards. NFC builds upon RFID systems by allowing two-way communication between endpoints, where earlier systems such as contactless smart cards were one-way only. This two-way communication supports a host of value-added capabilities, such as direct transmission of sales receipt information from the point of sale to the handset.

An NFC-based mobile wallet system requires an NFC chip in both the handset (or similar device) and on the card reader to transfer data from the phone to the point of sale. While relatively few merchants have NFC readers today, more and more are adopting this technology every day. In addition, most POS readers that are designed to support contactless EMV also support NFC. As merchants upgrade their POS readers in the coming months and years to support EMV, they will be able to support NFC transactions as well.

**A secure element (SE)** is a secure storage area of a mobile handset that is used to store the payment account information for a mobile wallet. The SE is completely separate from the storage area of the phone that holds contact information, photographs and other user-generated data. There are currently three SE implementations: a chip embedded in the mobile phone, SIM (subscriber identification module) based, and SD (secure digital) card based.
To maintain security, a trusted service manager (TSM) is the only entity that is permitted to have write access to the secure element in order to provision and maintain account information. A financial institution that wants to get its cards into a mobile wallet that utilizes a secure element must work through the TSM provider. Account provisioning is done real time over the air, making it possible to provision an account onto a mobile wallet in just minutes.

The pros and cons of NFC-based wallets with an onboard secure element

The scenario of a mobile wallet system that utilizes a technology interface based on both NFC and a secure element has its positive aspects and its drawbacks.

On the plus side:

- **Continuity** – This solution most closely replicates the existing model for card provisioning and security.
- **Security** – This is one of the most secure options for mobile wallets because of the secure element. In addition, NFC is widely viewed as a secure means of communicating sensitive information at the POS.
- **Proven** – With Google Wallet live in the market for some time, the technology interface and the processes behind them have demonstrated usability, stability and security. At this writing, millions of cards have been provisioned to consumers' mobile wallets.
- **Ease of use** – For the consumer, an NFC interface requires less effort to simply wave the device in front of a reader (compared to a QR code that must be lined up with a reader).
- **Extensible** – This type of solution is well suited to support multiple service providers in the mobile wallet. For example, it’s possible to provision numerous financial institutions’ products in one wallet. However, unless a financial institution owns the wallet, it doesn’t control the secure element and it may find it difficult to get permission to put its cards in the wallet.
- **Simplicity** – Consumers don’t need to learn anything new: “Tap and pay” is intuitive and works just like a credit card does today.

But the drawbacks include:

- **Infrastructure complexity** – This solution has greater infrastructure requirements than some other forms of mobile wallets. What’s more, this type of solution requires an ecosystem of companies to deliver it—mobile network operators, financial institutions, card associations, a trusted service manager, etc. Many of these parties are not accustomed to working together.
- **Scarcity** – Few handsets today are equipped with NFC, and even fewer have a secure element. The numbers are growing, however. NFC is expected to be more commonly embedded in smartphones by 2014. On the merchant side, few merchants have deployed NFC readers to date, but the upcoming move to EMV is likely to increase deployment of readers that also support NFC.
- **Control** – One entity controls access to the secure element, which can create a choke point or bottleneck in the ecosystem.
- **Confusion** – Consumers may become confused and/or frustrated that not all handsets and carriers can support a particular mobile wallet.
NFC-based solutions—
storing credentials in the cloud

The number of handsets on the market today that have a secure element is relatively small (although it is growing). Therefore, we must consider the case where a phone has NFC capabilities but no secure element that financial institutions have easy access to. (There may, in fact, be an SE on the phone controlled by a proprietary solution.) In this scenario, we have to think about a payment solution or redemption method in which the consumer’s credentials are stored somewhere in the cloud instead of in a secure element locally on the phone. The credentials are transmitted to a virtual card in the phone as needed and delivered to the POS reader via the NFC connection.

This solution hasn’t been implemented widely yet. The new version of the Google Wallet released in August 2012 is among the first wallets to implement credential storage in the cloud. Google’s approach allows consumers to link any Visa, Discover, American Express or MasterCard to their mobile wallet, greatly expanding payment choices and convenience for consumers. Financial institutions also benefit as they find it easier to get their cards into the mobile wallet.

The underlying technologies
This scenario depends on NFC technology as described above. Even though the credentials aren’t stored in a secure element on the phone, the credentials are delivered from the cloud to the phone at the time of a purchase, and the NFC connection securely transmits the credentials to the point of sale.

Payment credentials are stored in a secure cloud-based vault. In the case of Google Wallet, Google stores each card’s details on a server it controls. Consumers link their preferred card to a virtual MasterCard. To an end user, it would appear that the cards are directly available on the phone, without having to pass through a separate account. When a purchase is made with the cloud-based wallet, Google acts as the merchant of record. It presents only the virtual card number to brick and mortar retailers. However, issuers still receive the transaction data from Google Wallet purchases.

Pros and cons of NFC-based wallets with credentials in the cloud
The positive and negative attributes of using NFC, as described above, still apply for this scenario. That said, the additional benefits of storing credentials in the cloud instead of on a secure element include:

- **Choice** – Cardholders as well as financial institutions might find it easier to get their cards into this wallet. There is no secure element that is tightly controlled by a mobile network operator or other entity that is restricting access.
- **Addressable Market** – There is a broader addressable market for a solution that doesn’t depend on a limited quantity component (i.e., the secure element). There are currently many more phones without a secure element than there are phones with one.

The downside to this technology interface includes:

- **Untested** – The practice of storing payment credentials in the cloud has been done for years by Apple, PayPal and Amazon for eCommerce purposes—however, it is largely untested as a mobile wallet solution. This is not to say it’s not a viable and valid process, but this method needs to build a longer term history with success before it can be considered mainstream.
- **Connectivity** – A good Internet connection (via WiFi or 3G/4G) is required to deliver credentials from the cloud to the phone at the point of sale. The connection may be slow or simply unavailable in some locations.
The promise of NFC-based wallets will take some time to be realized given the POS and handset requirements. Many companies are developing innovative approaches to mobile wallets that can be more readily adopted because they do not require NFC for communications or a secure element to store the account credentials.

One type of technology interface that is attaining good traction is based on scanning a 2D barcode, often called a Quick Response or QR code. 2D barcodes, which look like odd black and white jigsaw puzzles, can be encoded to contain information that enables mobile payments.

An example of a mobile wallet based on 2D barcode technology is the Starbucks mobile application. In this particular implementation, a customer is able to load their Starbucks prepaid account into a custom mobile application. To pay for a purchase, the customer opens the Starbucks mobile app, touches the screen to display the barcode on the phone, and presents the screen to be scanned by the counter clerk using a barcode scanner. The rest of the payment process works exactly as if the customer had presented the actual plastic prepaid card. The Starbucks mobile wallet also manages the customer’s Starbucks card and balance, facilitates redemption of earned rewards, enables quick reloads of the card, tracks the customer’s rewards program status and history, and allows the customer to send a friend an eGift.

The underlying technologies
Solutions based on 2D barcodes can be deployed in numerous ways, including these two most common implementations:
1. Merchant generates and displays a barcode that consumers can scan with their mobile phone cameras.
2. Consumer’s phone generates a barcode that the merchant reads using its POS scanner.

Regardless of the implementation, the same basic technologies are needed:

A **2D barcode** or **QR code** is a matrix barcode consisting of black modules (square dots) arranged in a square pattern on a white background. The pattern encodes numeric, alphanumeric or binary data, which can be “read” by a scanner or digital camera. It is quick, easy and very inexpensive to generate a QR code. Depending on how the barcode is generated, it can hold more than 7,000 characters. Sometimes, the data in the barcode is an unencrypted representation of the card number—however, the information in the barcode can be encrypted for security purposes, and card numbers can be tokenized or replaced with virtual card numbers.

**Barcode reader software** uses input from the scanner or camera to convert the dots into information that can be used to facilitate the transaction. Reader software is built into barcode scanners that merchants commonly use at checkout, and mobile phone owners can download a reader app for free.
Pros and cons of 2D barcode-based solutions

The positive aspects of this technology interface include:

- **Ease of implementation** – It’s relatively quick and inexpensive for a merchant to implement a mobile wallet solution based on this technology. QR codes are based on industry standards and they cost practically nothing to create. Merchants can utilize regular barcode scanners at the point of sale as the QR code readers.

- **Simplicity** – Consumers find this type of solution relatively easy to use, although it is important to properly align the QR code with the scanner or camera. Consumers are accustomed to seeing QR codes in action, and increasingly know what to do with them.

- **Addressable market** – Since no NFC chip is required on the phone, the addressable market for this technology interface is quite large. It can work on practically any phone that can run mobile apps.

But there are drawbacks as well:

- **Security** – Unfortunately, in many current non-payment implementations of QR codes, security can be a drawback. QR codes can be vulnerable to website redirection and more susceptible to fraud. Consequently, they may not be suited to high value transactions unless proper encryption and tokenization is implemented.

- **Inconsistency** – There currently exists no standardization for payments via QR codes, resulting in unpredictable technical specifications and an inconsistent user experience.

- **Usability** – Using QR codes at the point of sale is not as easy or seamless as “tap and pay”: consumers and merchants are both required to perform more work in order to complete a transaction.

Planning a mobile wallet solution to fit your Universal Commerce enablement needs

Consumers are in the driver’s seat where mobile wallets are concerned. They will choose which one(s) to use and their decisions are typically based on convenience, ease of use, and most of all, the benefits they’ll reap from using a particular wallet or payment type. From a consumer’s perspective, it’s not the flashy new payment process of using a mobile phone but the value-added services that make the wallet worthwhile.

For merchants and financial institutions, the value of mobile wallets is the fact that they are platforms for engaging customers in a variety of ways, many of which didn’t exist before. In fact, mobile wallets can be said to lie at the very heart of Universal Commerce.

Because there are so many seemingly viable implementation options in the market, it’s not yet clear which type(s) of mobile wallet will enjoy the greatest long term success. More than likely, there will be a consolidation of the market in the years ahead, bringing us down from the 120+ wallets of today to a few solid sets of technologies and mobile wallet systems. Nevertheless, now is the time for merchants and financial institutions to be testing the waters and planning a solution (or two) to gain experience and remain relevant.
Getting started for financial institutions

Financial institutions need to start planning how to mobile enable their card portfolio. Issuers can take steps now to prepare, for example, by getting contactless BINs that might be part of this situation, or by establishing relationships with mobile wallet owners.

A critical step is to try some of these wallets to gain some valuable experience. Those banks that come late to the game risk being dis-intermediated. The competitive threat from new entrants is real, and consumers have shown a willingness to consider alternatives to their primary banks to provide mobile wallets and even core banking services."

As much as the focus is on mobile, it’s more important to think about mobile wallets in the holistic context of Universal Commerce. Yes, mobile commerce is a key part of the strategy, but so is eCommerce and physical commerce. Thus, financial institutions need to think about a multichannel banking experience for their customers. Consumers have expectations to interact with their banks and banking services whether they are on the go with a smartphone or tablet, sitting at a personal computer, walking into a branch, or visiting an ATM. It’s imperative for financial institutions to deliver a rich set of products and services regardless of the customer interface.

The richness of the mobile products and services, in particular, needs to go beyond the staid activities of checking an account balance, making an account transfer, paying a bill, or locating a branch or ATM. Financial institutions need to move into the realm of the value-added services that mobile wallets enable, such as merchant offers and enhanced loyalty programs. What’s more, banks can offer new services to track and manage customers’ offers, incentives, receipts and spending reports. Surveys indicate these types of services are what consumers really care about. This presents an opportunity for financial institutions to form the partnerships, develop a loyalty strategy, and create the value-added services that will place their cards and payment methods at the top of their customers’ wallets and deepen their engagement with customers.

Getting started for merchants

In order to make this simple for consumers, merchants need to be able to accept multiple technology interfaces. Merchants that are on a path to update their POS equipment for EMV or other reasons should make sure the new customer-facing equipment can support a variety of technology interactions, from EMV to NFC to QR code.

Merchants need to think about how to mobilize their current programs. If they have a loyalty program, prepaid card, or a private label credit card, they need to consider how to take these pieces and put them on a path to be used in various mobile wallet systems—whether in a merchant’s own wallet or in one of the aggregator’s wallets.

Merchants should be planning how to offer the value-added services that will be the real drivers for mobile wallets. Offers, discounts, loyalty incentives, merchant-funded offers delivered through aggregators, receipt management, location-aware services—all of them will be important drivers to bring consumers to a merchant’s venues, whether they be physical stores, a website, or a mobile application. These services also provide merchants with innovative new opportunities for deepening and enriching their customer relationships.
It’s also important to consider how to enhance security in this new era of uCommerce. We know that with any new payment mechanism or payment method, there’s the perception and the reality of security concerns. A lot of the technologies going into mobile wallets are going to make payments more secure than the magstripe cards available today. Consumers, however, may have the idea that payments tied to a phone aren’t secure. It will take consumer education to build their confidence in the security of mobile wallets. Beyond perception versus reality, merchants need to consider what additional technologies or processes to layer on top of the built-in mobile wallet security to watch for fraudulent transactions, and to better understand their customers’ behaviors.

### Conclusion

Mobile wallet systems are gaining momentum in the marketplace. They are at the very heart of Universal Commerce, and merchants and financial institutions alike need to consider how to utilize mobile wallet systems to engage new and existing customers in a variety of ways.

The adoption of mobile wallets will be driven by interesting value-added services that go beyond mobile payments. The top value-added services are the offers that drive traffic to merchants’ venues, as well as rewards for specific customer behaviors. Consumers want a convenient, fully integrated shopping experience no matter where they are or what time of day it is.

It’s still unclear which mobile wallet systems will have a long term impact on the marketplace. It is certain, however, that the emphasis right now should be placed on creating an optimal user experience with a compelling value proposition, instead of trying to predict which technologies and specifications will become standard. Financial institutions and merchants need to be positioned to win in multiple ways, so it’s important to start developing a strategy now, forming relationships with partners and vendors, and perhaps testing the waters with existing mobile wallet solutions. This early experience will give a leg up on competitors who wait for more clarity before jumping into the market.

---

### What’s in it for merchants

The benefits to merchants of participating in mobile wallets include:
- Generate additional revenue through mobile payment acceptance
- Attract new customers with mobile targeted couponing
- Drive increased loyalty through mobile enabled reward programs
- Potentially reduce payment acceptance costs by steering customers’ selection of payment cards in a mobile wallet.
- Increased knowledge about your premium customers with access to rich mobile customer information
- Enhance campaign analytics and ROI with mobile marketing platform
- Allow offers to be shared via NFC and Social (creating viral effect)
The Global Leader in Electronic Commerce

Around the world every day, First Data makes payment transactions secure, fast and easy for merchants, financial institutions and their customers. We leverage our unparalleled product portfolio and expertise to deliver processing solutions that drive customer revenue and profitability. Whether the payment is by debit or credit, gift card, check or mobile phone, online or at the point of sale, First Data helps you maximize value for your business.

For more information, contact your First Data Representative or visit firstdata.com