FEDERAL RESERVE
BANK OF BOSTON™

Mobile Phone Technology: "Smarter" Than We Thought

How Technology Platforms are Securing Mobile Payments in the U.S.

Marianne Crowe and Elisa Tavilla
Federal Reserve Bank of Boston

November 16, 2012

 The authors would like to thank Sam Bass, Fergal Carroll, Darin Contini of the Payments Strategies group, Seb Taveau, CTO at Validity, and our colleagues at U.S. Treasury for their valuable contributions to the work effort, insightful ideas, and helpful comments and suggestions.

The paper can be found at: http://www.bostonfed.org/bankinfo/payment-strategies/index.htm

I. INTRODUCTION

Using a mobile phone to make payments introduces a new entry point for traditional and trusted payment methods in the U.S. It also introduces several new technologies to support mobile payments. The unfamiliarity and complexity of the mobile device and associated technologies create security concerns for consumers who want to be confident that their personally identifiable information and actionable financial information (e.g., account numbers, PINs, security codes, and passwords) are protected in storage and while being used to process a mobile payment transaction, whether that storage is on the mobile device or in the cloud. They want to be certain that their data cannot be intercepted at any time. Concerns about sensitive payment information being captured 'over the air,' or mobile phones being lost or stolen and personal data being shared inappropriately need to be addressed by stakeholders to satisfy consumers, merchants, and regulators. Data breaches or fraud resulting from a mobile payment can hinder consumer adoption. The security of each mobile technology platform will be a major contributor to its success and the ultimate broad adoption of mobile payments.

This report examines in detail how near field communication[1] (NFC) and cloud[2] technologies address security for mobile payments at the retail point-of-sale (POS). It also provides a brief overview of security for two other mobile technology platforms, QR code,[3] and direct carrier billing (DCB)[4]. Each technology manages and processes information uniquely; hence security practices and issues will vary with the technology deployed by each payments platform provider. This is inherently confusing to consumers, regulators, and possibly other mobile stakeholders.

A key concept tied to the various mobile technologies is the wallet. In this paper we distinguish between a mobile wallet and a digital wallet. A mobile wallet (e.g. for NFC), is a software application stored on

---

[1] **NFC (near field communication):** A standards-based wireless communication technology that allows data to be exchanged between devices that are a few centimeters apart. NFC-enabled mobile phones incorporate a smart chip (called a secure element) that allows the phone to store the payment application and consumer account information securely and use the information as a virtual payment card. NFC payment transactions between a mobile phone and a POS terminal use the standard ISO/IEC 14443 communication protocol currently used by EMV and U.S. contactless credit and debit cards that allows the mobile phone to simulate a physical contactless card.

[2] **Cloud** is a remote server where payment credentials are stored and used to authenticate the payment transaction, instead of on the actual mobile phone. The cloud may be managed by a merchant or payment services provider.

[3] **Quick Response (QR) code or 2D barcode** is a two-dimensional barcode which contents can be scanned and decoded quickly.

[4] **Direct Carrier Billing (DCB)** enables a consumer to use his mobile phone number to buy virtual goods and services and have them charged to his monthly mobile phone bill. Payment intermediaries partner with MNOs and merchants to handle the process of billing the mobile carrier and paying the merchant.

the physical mobile phone to manage and initiate payments. The mobile wallet accesses the payment credentials (e.g., payment cards, bank account, coupons, loyalty, transit tickets, etc.) or actionable financial information, which are stored on the mobile phone in a trusted environment known as the secure element. The consumer must have the physical phone with him to enable the payment transaction by waving or tapping the mobile phone over an NFC-enabled terminal at a retail location.

A digital wallet stores the payment information on a secure remote server, also known as the cloud. A cloud-based or digital wallet stores actionable financial information remotely from the mobile device, and sends only tokens or authorizations to the actual mobile phone to initiate and authorize the payment at the point-of-sale (POS). Wireless service, either cellular or Wi-Fi, is needed to complete the digital wallet transaction. The primary difference from the NFC mobile wallet is that sensitive financial information is stored in the cloud, not on the mobile phone.

A hybrid wallet combines features of the mobile and digital wallets. The mobile payments provider leverages the security aspects of NFC with the added protection of storing the real payment credentials in the cloud. The consumer's financial information in the cloud is linked to a mobile phone through a unique identifier in the device. Account credentials used when making POS mobile purchases are accessed from the cloud when needed, but the payment transaction is still initiated using the NFC protocol to communicate from the mobile phone to the POS terminal.

For example, Google Wallet (v. 1.5) is a hybrid mobile wallet. A virtual payment card associated with each mobile phone is stored in the secure element. The virtual card does not correspond to any specific payment card account, but is a proxy for the real card account, maintained in the cloud. For security purposes, only one real payment card account can be active at a time. Google is both the issuer of the virtual MasterCard and the merchant of record. The customer taps his NFC-enabled phone (host) at the merchant terminal and enters his PIN. The NFC controller on the mobile phone communicates the information to the merchant POS terminal. (To prevent malware, the NFC controller can detect the source of a payment request and block the request to the secure element if it is not from the host device (physical mobile phone and a PIN)). The payment authorization request first goes to the real payment card account in the cloud, and if approved, to the virtual card in the phone.

II. NFC MOBILE PAYMENTS

In the U.S., two primary mobile phone system standards are used—Global System for Mobile Communications (GSM) and Code Division Multiple Access (CDMA). The major difference between the two technologies is how they turn voice data into radio waves and how the carrier connects to the mobile phone. Other differences include the coverage area, data transfer speeds, and the type of hardware used. AT&T and T-Mobile use GSM technology, while Verizon and Sprint use CDMA in the U.S.[5] Generally, consumers are unaware of the differences between GSM or CDMA phones when making calls, sending text messages, or using other basic phone features, but there are some differences when applied to mobile payments.

NFC Mobile Payment Options

There are three NFC approaches for processing and storing sensitive consumer data in the mobile phone. Mobile payment stakeholders, including mobile network operators (MNO), financial institutions, card issuers, merchants, and payment processors, decide which option(s) to implement. Each approach is hardware-based and differs primarily on the placement of the secure element in the mobile phone.

The secure element is essentially the component within the mobile device that provides the application, the network and the user with the appropriate level of security and identity management to assure the safe delivery of a particular service. It is an encrypted smart card chip[6] that contains a dedicated microprocessor with an operating system, memory, an application environment, and security protocols, built to exacting standards and developed and delivered in controlled white room manufacturing environments. The secure element is used to safely store and execute sensitive applications, such as payment applications, on a mobile device, and store associated payment credentials and financial data.

---

[5] While Verizon and Sprint use CDMA technology in the United States, both MNOs offer mobile phone models with CDMA and GSM technology to their customers who travel to countries where only GSM networks are supported. For example, Sprint sells selected mobile phones with preinstalled SIM cards to support roaming on compatible GSM networks. Customers must contact Sprint to active the SIM card for international wireless service prior to initial use outside of the U.S.

[6] **Smart card:** Device with an embedded secure integrated circuit (or smart chip). The card connects to a reader with direct physical contact or with a remote contactless radio frequency interface. For purposes of this report, the smart card technology referenced is the SIM (subscriber identification module) used in GSM mobile phones. Smart card technology conforms to international standards (ISO/IEC 7816 and ISO/IEC 14443).

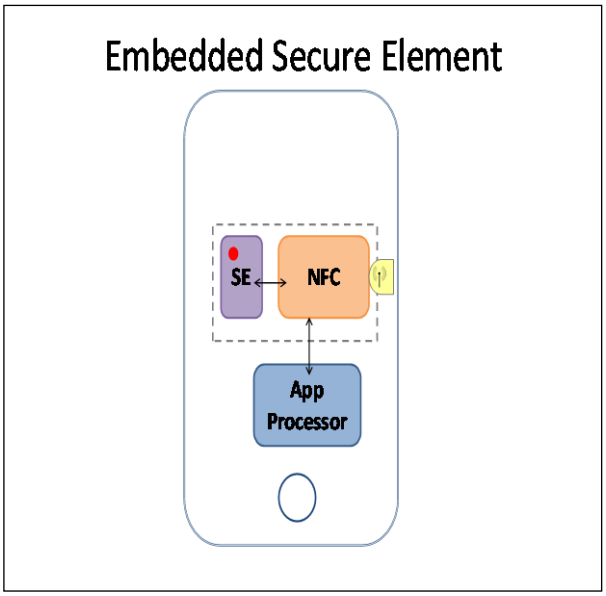
Encryption is an important component of the secure element, and plays a critical role in mitigating fraud during a mobile payment transaction by converting payment data into a form unintelligible to everyone except holders of a unique cryptographic key. **Cryptographic keys** are values that determine the output of an encryption algorithm when transforming plain text to encrypted text. The longer the key, the more difficult it is to decrypt the text in a given message. **Key rotation**[7] is the process of decrypting data with the old encryption key and re-keying the data with the new encryption key. Encryption protects consumer and transaction-level information against unauthorized access or disclosure, from the initial encryption step to the decryption step. Encryption can protect data during transmission and while at rest.

Advantages and Disadvantages of Secure Element Placement Options

The most common secure element implementations include: a) embedded (or hard-wired) in the mobile phone, b) loaded on a SIM[8] card, and c) loaded on a microSD card. This section will examine each approach and compare the benefits and security features.

a) <u>Embedded Secure Element</u>

In the embedded NFC model, the secure element is soldered onto hardware in the mobile phone. The original equipment manufacturer (OEM) procures space on the secure element for issuing banks or other mobile payment providers, and is responsible for safely distributing the secure elements in the mobile handsets to consumers, who purchase embedded NFC mobile phones at various mobile retailers. MNOs coordinate with the handset manufacturers to ensure that authorized operating systems/applications (e.g., iOS, Android) work with the secure element.



[7] PCI DSS specifies that keys should be rotated, but does not specify the frequency of rotation. If there is concern that an encryption key has been compromised, the data should be encrypted with a new key.

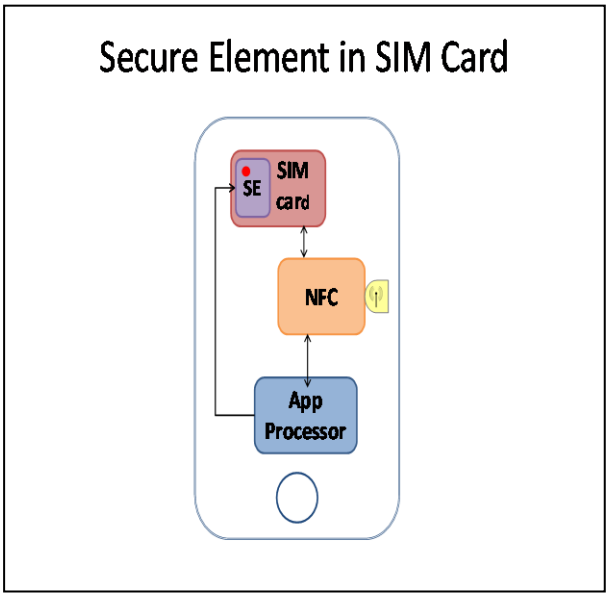
[8] As SIM card technology developed and eventually was replaced with UICC cards, the term 'SIM card' became ubiquitous and is often used interchangeably with UICC. Throughout this section, the term SIM card refers to a UICC smart card.

An embedded secure element provides a common architecture for application developers, independent of the mobile phone technology—GSM or CDMA. A larger antenna built into the handset also offers a stronger communication signal between the mobile phone and merchant terminal. And, because secure elements are built into mobile devices during the manufacturing process, they are relatively tamper-proof and less costly to produce relative to SIM and microSD options.[9]

One disadvantage of an embedded secure element is that it is not portable, making it difficult to transfer mobile payment applications and credentials between handsets. This may be inconvenient for consumers when they need to transfer credentials and applications from an old phone to a new one. However, some mobile services and operating systems enable data on the embedded chip to be transferred over-the-air (OTA) to the new phone. OTA technology transmits data using a wireless network and protects the information exchange by using a secure end-to-end communication link to the secure element. It also provides strong security by using double encryption, in which the OTA messages are encrypted with two sets of unique keys – the MNO key and the service provider key. Once the secure element is activated on the new mobile phone, a customer's payment credentials must be wiped from the old device. However this process is not a standard requirement when provisioning the mobile phone and should be addressed by the mobile payments providers. (For example, Google's mobile wallet payments strategy is built around the OTA option.)

b) Secure Element in the SIM Card

A SIM (Subscriber Identity Module) is a removable smart card used in many mobile phones. Each SIM card can hold multiple applications. GSM phones use the SIM card, while CDMA phones use their own version called CSIM (CDMA2000 SIM). For mobile payments, the SIM card performs the secure element function.



The SIM card communicates with the NFC controller in the mobile handset through a Single

[9] Industry analysts report that major manufacturers are increasing the number of shipments of embedded secure elements. Edgar, Dunn & Company, "Advanced Payments Report 2012," March 2012.

Wire Protocol (SWP).[10] Using the SIM card as a secure element is considered safe because it is personalized, remotely manageable over-the-air, and uses standard transport protocols developed by global telecom standards bodies. The MNO owns the SIM card[11] and creates secure partitions or domains[12] in the SIM for third parties (e.g., banks, retailers, and transit authorities) to rent for their mobile applications. The MNO provides each third party with a unique security key to access its domain. The keys are also known to the SIM.

One advantage to using the SIM approach is that the secure element can use information contained on the SIM (such as its unique serial number (ICCID) and the international mobile subscriber identity (IMSI)) to link to an individual consumer. This provides an additional layer of security and also simplifies the changeover process when a consumer upgrades his mobile phone, as the SIM is easily removable.[13] MNOs can also communicate with, download applications to, and manage a SIM card/secure element remotely over-the-air. If a handset is lost or stolen, it can be locked or remotely wiped to prevent any unauthorized account access.

There are some drawbacks to this approach. Because the MNO owns and controls the SIM, a mobile operating system has restricted access to the secure element in the mobile device. Furthermore, the MNO also controls which third parties or financial institutions can add payment applications or wallets, and what fees they pay to use the SIM as the secure element.

c) Secure Element in microSD card

The third option is to put the secure element in a microSD card, which is a memory card used to store data. It is designed to integrate with the mobile phone by fitting into a specially designed

---

[10] The NFC controller comprises of hardware and software that control the NFC radio signals transmitted to and from the mobile device. The NFC chip and antenna are part of the controller. Single wire protocol (SWP) is the specification which connects the SIM card and the NFC controller in the mobile phone through a single wire, which adds contactless functionality to the SIM card.

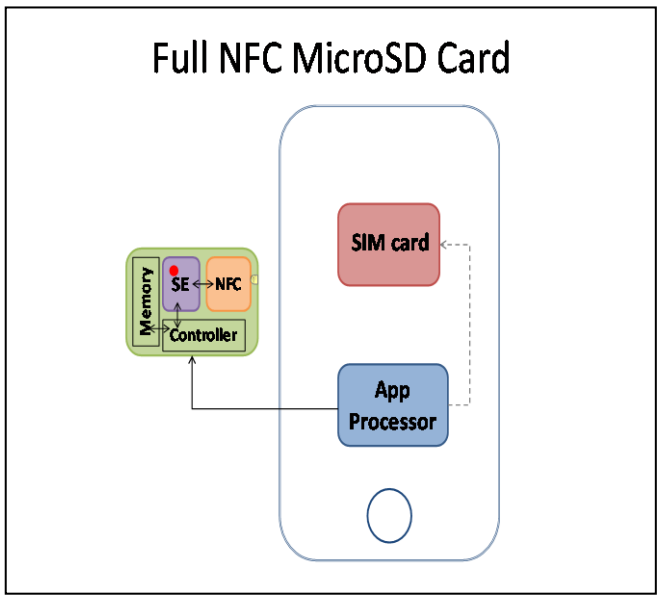
[11] For U.S. implementations the MNO owns the SIM card in handsets sold through their outlets. This may or not be true in other countries.

[12] There are three types of domains: (1) Issuer Security Domain (ISD), used by the MNO to manage the entire SIM card; (2) Controlling Authority Security Domain (CASD), managed by the TSM; and (3) Application Provider Security Domain (APSD), for each application provider. GSMA defines these as supplementary security domains (SSDs).

[13] This feature only works with GSM mobile phones today, which have removable SIM cards. Verizon's 3G mobile network uses CDMA technology, which does not require a SIM card, so this feature is not available. However, newer Verizon 4G handsets use a SIM card to access the 4G network.

slot on the device. Like embedded and SIM NFC phones, NFC-enabled microSD cards communicate with apps to enable mobile payments. The full NFC microSD card model employed in the U.S. contains the secure element, security domain, NFC chip, and antenna.

In the third option, payment card data is also encrypted and stored in the secure element, but the secure element resides in the microSD card. The portability of a microSD card simplifies moving the secure element and associated payment data to any other mobile phone that has either a microSD card slot or a protective case with a microSD slot that fits over the phone (iPhone model).



Unlike the SIM and embedded secure element options, there are three ways to issue, provision and distribute an NFC-enabled microSD card to the consumer:

(1) Card-issuing financial institution provides the microSD card.
(2) Retailer provides a blank microSD card to the end consumer, similar to a prepaid card.
(3) MNO bundles the microSD with a phone or sells it independently of a phone.

Implementing an NFC-enabled microSD card solution can speed deployment of mobile contactless payment services by allowing a consumer to insert the microSD card into his existing mobile smartphone to begin making mobile payments.

Over the past few years, several U.S. banks, card networks, and transit authorities have piloted mobile payments using microSD cards to test several concepts: easier implementation, ability to enable contactless payments in consumers' mobile phones more quickly, ability to test the NFC technology without needing SIM or embedded NFC chips, and consumer interest. The pilots were relatively limited in scale, providing useful information on consumer experiences using a mobile phone for POS purchases, but also identified a number of technical problems, such as:

- Weak radio signal and interference caused by:
    - **Size and location of the antenna**. If the antenna is too small, it may result in a weaker radio signal and be subject to interference.

    - **Physical location of the microSD card slot** on the mobile phone.
    - **Material of a mobile phone's casing**. Metal casing tends to cause signal interference and weaker reception.
    - **Protective and decorative external covers**. Additional covers on a mobile device can cause signal issues and become a barrier to the radio signals.
    - **Embedded antennae.** Communication conflicts and unexpected radio interference may occur when both the mobile device and the microSD card have embedded antennae.
- Compatibility issues with mobile phones that are not equipped with microSD slots.
- MicroSD cards are typically mono-band, meaning that they can support only a single application or payment account. If consumers have multiple mobile payment and/or loyalty accounts from different sources, they may need a microSD card for each application—one from each bank, carrier, or other provider with which the customer has accounts. In contrast, a SIM card or embedded NFC chip can be segmented into multiple secure compartments to support multiple applications. While the microSD approach may be more suitable for an issuer of a single closed mobile payment application, it can be more complicated and much less convenient for the consumer.

Other consumer risks associated with a microSD card make its long-term survival doubtful.

- While consumers can transfer microSD cards from one mobile phone to another, the cards are tiny and fragile, and frequent removal and insertion into a mobile device increase the risk of loss or damage.
- Portability provides opportunity for an unauthorized person to easily gain access to the payment information on the microSD card because there is no lock or PIN to prevent anyone from opening the phone and removing it.
- Issuers must handle and protect microSD cards in the same manner as they handle plastic cards when distributed and mailed to consumers.

Finally, it is unclear whether specific standards for microSD cards exist today in the U.S., particularly to manage how microSD card slots securely communicate with user interfaces and support communication between the microSD secure element and the NFC controller on a mobile device.

Summary of benefits and challenges for NFC-type mobile payments

Benefits

According to a report from the Smart Card Alliance, "NFC-based contactless payments are considered extremely secure; there is no empirical evidence to the contrary."[14] Whether or not empirical evidence exists, using NFC technology for mobile payments offers many security benefits. (1) Payment credentials are stored in the secure element in the mobile wallet. Different passwords can be set-up to log on to the mobile device, and to activate the payment application that accesses the payment credentials in the secure element. (2) When not in use, the NFC antenna can be disabled until needed so that unauthorized users cannot access the wallet. (3) NFC is an extension of EMV[15] chip technology, with the radio interface added. When a mobile payment begins, EMV secures the payment transaction with dynamic data authentication (DDA), which uses an encryption key to generate unique, dynamic data values to authenticate the transaction when it is authorized by the card network. These values are only valid for one authentication. If a thief tries to re-use the payment account data, it will be out of sync with the number stored by the card issuer and rejected, making it harder to skim usable data and clone for counterfeiting. (In contrast, the signature used for static data authentication is the same every time.) EMV provides end-to-end security with "chip+ PIN" credit cards in most developed countries today.

Other benefits of NFC payments include eliminating the cost of plastic card provisioning, using the existing clearing and settlement channels, and providing the possibility for the transaction to be "card present" vs. "card not present" (CNP), which reduces risks associated with CNP and lowers interchange fees.

Challenges

For NFC mobile payments to succeed in the U.S., several challenges related to technology, implementation, and consumer adoption must be resolved. Few mobile phones in the U.S. are currently enabled for use with either SIM or embedded NFC secure element chips, although more handset

[14] Smart Card Alliance, "The Mobile Payments and NFC Landscape: A U.S. Perspective," September 2011, p.31.

[15] EMV is an open-standard set of specifications for smart card payments and acceptance devices developed to define a set of requirements to ensure interoperability between chip-based payment cards and terminals. EMV chip cards contain embedded microprocessors that provide strong transaction security features and other application capabilities not possible with traditional magnetic stripe cards. Today, EMVCo manages, maintains and enhances the specifications. EMVCo is owned by American Express, MasterCard, JCB, and Visa, and includes other organizations from the payments industry participating as technical and business associates. Information on the specifications and organization is available at http://www.emvco.com.

manufacturers are beginning to embed NFC chips in their mobile phones or on SIM cards as a basic component. Globally, forty-five handset manufacturers have announced plans to add NFC/SIM cards to their mobile phones[16] and Isis plans to have up to 20 Isis-ready handsets available by the end of 2012.[17] If these efforts move forward, they could begin to alleviate this barrier. More merchants must invest in upgrading their POS terminals to enable two-way NFC, a long-standing barrier to adoption. Work still needs to be done to develop an agreed upon set of technology standards for mobile phones, chips, and secure elements, and standards for provisioning and maintaining mobile payment credentials. Yet the number of cross-industry participants engaged in the mobile payment process/value chain continues to grow, further complicating business models and customer-ownership. Finally, we need to remember that many consumers are still unfamiliar with NFC technology and require not only incentives, but also education regarding its safety and security when used for mobile payments, particularly with a mobile wallet.

III. CLOUD SOLUTIONS FOR DIGITAL AND MOBILE PAYMENTS

In a cloud-based payment solution, both the consumer and the merchant must download the cloud-based application and subscribe to the service. The physical mobile phone may or may not be needed to complete the payment, depending on the solution. The mobile device becomes an extension of the POS terminal, which communicates information about the mobile payment transaction to the cloud for authentication. Consumers can access their account information in the cloud via mobile phone, e-mail address, mobile phone number, mobile browser, or mobile application. Once a cloud payment is completed, payment notification can be communicated via e-mail or SMS text messages.

Cloud Models

Cloud computing (not specific to mobile payments) is the use of shared hardware and software resources that are delivered as a service over a network (typically the Internet). Data and software are retrieved from remote servers using web-based tools and applications. Cloud computing services may be deployed using one of several models: personal cloud (user-owned content/space), private cloud (enterprise), shared

[16] GSMA announced at its Mobile Asia Congress that it has commitments from 45 MNOs worldwide to implement SIM-based NFC. http://www.nfcworld.com/2011/11/16/311363/45-mobile-operators-commit-to-nfc/

[17] Source: http://www.wired.com/gadgetlab/2012/10/isis-sets-oct-22-launch-date/)

cloud, or public cloud. Due to the openness of the public cloud (available to any customer), which by design may have inherent security risks, this paper focuses only on use of the private and shared clouds for mobile payments at POS.

In the private cloud model, a mobile payments provider assumes full control and ownership of the entire lifecycle, which provides several benefits:

- Ability for provider to implement proprietary security and ID management controls
- Quick response to regulatory changes
- Update of customer requirements in real-time
- Low merchant cost to participate
- Centralized control of the environment

Implementing a private cloud model generally requires businesses to have a large market share, an extensive customer base, and/or sufficient capital to build a large scale environment.

In a partnership or shared cloud model, the financial institution and the MNO provide cloud payment services that support the business functions of both the MNO and the FI. This shared model provides the following benefits:

- Allows for scalability and provisioning at a lower cost
- Ability for the MNO to enter the market with fewer regulatory limitations because of its partnership with an FI
- Ability for MNO and FI to share their client bases and increase their potential market

While use of the cloud is very new to the mobile payment channel, it has been used for Internet payments for several years. The following section highlights several vendor cloud solutions for retail payments that connect the Internet to the mobile channel.[18]

Square

In May 2011, Square launched a cloud wallet, *Pay with Square*, which utilizes geo-location technology to locate customers using the GPS function in their mobile devices. The customer's name and picture automatically appear on the merchant terminal after the customer selects the *Pay Here* button on his

[18] The minimum SSL encryption level throughout this section is 128-bit SSL 3.0

mobile app, directing the merchant to put the purchase on his tab in Square. The customer may also enable the automatic tabs function to create a *hands free* purchase, which opens a tab automatically when the customer arrives at the merchant's location, and does not require use of the mobile phone. Square stores card numbers, other payment data, and security features in the cloud, not on the mobile device. The Square software has been updated to encrypt sensitive data using industry-standard methods when stored or transmitted over public networks. Card-processing systems and applications adhere to PCI Data Security Standard (PCI-DSS), Level 1.[19]

LevelUp

LevelUp is a mobile payments platform that uses QR code technology via a downloadable mobile app that allows customers to make mobile payment transactions. To scan barcodes and accept mobile payments, a merchant must install a special LevelUp terminal. A customer links his debit or credit card to register for a LevelUp account and receives a unique QR code. The customer pays by displaying the QR code on his mobile phone in front of the merchant scanner. When the QR code is accepted, the phone vibrates and the terminal lights up. LevelUp sends an email receipt to the customer showing the merchant name and amount of purchase.[20]

LevelUp outsources to a third party cloud management system. Customer payment credentials are stored and managed by a third party vendor, Braintree.[21] All financial information is encrypted during transmission and at rest. No personal information is sold to other third parties, including businesses that work with LevelUp. The company states that it is 100% compliant with all PCI requirements.

For security purposes, LevelUp employs a triple token system. The QR code that consumers use for payment does not include credit or debit card information. It is a randomly generated token that maps to a second token on the LevelUp server, which then maps to a third token in the Braintree cloud. Only the combination of these tokens and two other authentication factors can initiate a transaction.

---

[19] Square website, September 2012. https://squareup.com/

[20] Within the LevelUp app the user can also activate a feature that allows them to receive transaction information as a push notification as well as receiving an email receipt. In September LevelUp announced plans to add NFC support to its payment terminals.

[21] Braintree offers an online platform for merchant payment processing and financial data secure storage.

PayPal In-Store Checkout

PayPal In-Store Checkout enables customers to access their PayPal accounts to pay for purchases at participating POS merchant locations. Customers must register before using PayPal at the POS. To make a POS purchase, the customer has two options. He may enter his mobile phone number or swipe a PayPal card, and then key a PIN on the merchant terminal. In either case, the physical mobile phone is not needed to complete the transaction.

PayPal stores all customer personal financial information remotely in a proprietary cloud, whether the payment is made at POS or via the Internet. No customer data is stored on the mobile phone or POS terminal. PayPal's servers are protected by a firewall and not directly connected to the Internet. PayPal uses SSL encryption to transmit personal financial information from the Internet or a merchant terminal to PayPal.

Apple iTunes

A customer registers for iTunes by creating an Apple ID and verifying his iTunes account through an e-mail link. He funds his iTunes account with a debit, credit, or prepaid gift card. If the customer links his debit or credit card, Apple places an authorization hold equal to $1.00 on the account to verify the information. To purchase digital content, the customer logs into iTunes and enters a password. The Apple ID and linked payment information are stored on proprietary Apple servers. Access to the iTunes store is done over a secure network connection using SSL encryption.

Apple recently introduced the *Passbook* feature for the latest version of iOS. Passbook is an app-based wallet to manage passes (boarding passes, movie tickets, retail coupons, loyalty cards etc.). Each pass is stored as a barcode in the relevant retailer's (e.g. Target, Starbucks) section of the app. The wallet cannot be used to make payments.[22]

V.me

V.me, Visa's digital wallet, allows a customer to store multiple Visa, MasterCard, Amex, or Discover card accounts and a home address in the cloud. A customer first registers at the V.me website. To make a V.me purchase, the customer clicks on the V.me icon on the merchant's webpage, logs into his V.me

[22] iCloud uses a minimum of 128-bit AES encryption to store data. Advanced Encryption Standard (AES) is a method for encrypting data for storage.

account using his registered e-mail address and password, and confirms the payment. V.me is currently used for internet purchases and is in an early release stage. Just few retailers accept V.me at this time and registration is by invitation only. Future plans for the service include NFC mobile payments offers based on a customer's activity, and budgeting services. V.me uses encryption to store card credentials and has multiple layers of security. Card credentials do not appear during the checkout process at the merchant website. Customers have the ability to set up real time SMS or e-mail purchasing alerts to be notified of any transactions made using their V.me account.

Benefits of cloud-based mobile payments

From the merchant's perspective, cloud-based mobile payment services may be more flexible by avoiding some POS constraints. For example, the cloud wallet decouples a purchase from the payment and can support traditional electronic and alternative payment methods that may offer less expensive payment options to the merchant. Implementation of the mobile payment solution may be easier since new POS hardware is not always required.

From the consumer's perspective there are several benefits:

- Consumer familiarity. Consumer experience with use of other mobile apps may help them transition more quickly to a cloud-based mobile payment solution than an NFC mobile solution
- Ease of use at check-out. The consumer typically inputs an account number and password, which are authenticated against his payment credentials stored in the cloud. In the push cloud model, a customer uses a token[23] stored on his mobile phone, which represents his account credentials, to initiate and complete a payment transaction
- Portability. Because the cloud model is hardware agnostic, a consumer does not need to move his data if he switches mobile devices or mobile carriers, or upgrades his phone
- Improved security. The cloud solution provides alternative security for payment credentials by not storing them on the mobile phone, unless they are stored for back-up. Also, because account credentials and sensitive data are stored in the cloud, no hardware secure element is

[23] Tokenization replaces the primary account number (PAN) with a substitute value called a token to prevent unauthorized access to the true account number. De-tokenization reverses the process and redeems the token to access the associated PAN value. The true PAN value is protected because it can only be determined if the substitute or token value is known.

needed in the mobile phone to protect payments data. Conversely, the cloud can provide secure backup storage for NFC mobile payments transaction data

- Broader availability. Cloud apps are web or browser-based (vs. native mobile apps which are developed to perform on specific mobile phone operating systems) and accessible across different device/OS platforms, enabling the apps to run on many different mobile phones.

Cloud-based mobile payment challenges[24]

Use of cloud-based mobile payment services requires both the merchant and the consumer to subscribe. While merchants do not need to implement NFC hardware and software on their terminals, merchants must work with the mobile payments providers to implement additional infrastructure to accept cloud payments at the POS, and the customer must register with each individual merchant before making a payment. Merchants should also be aware that some cloud-based transactions may be treated as card-not-present (CNP), resulting in higher transaction fees.

Cloud payments require Internet connectivity. A transaction may not work or be interrupted due to connectivity issues, particularly if access to the cloud fails and there are no back-up payment credentials stored on the mobile phone. However, the most notable problem is the lack of quick mobile Internet access. Transactions may be slow depending on how the wallet is accessed, what the connection speed is, and how much data must be entered. A payment transaction may require more time because transmission to the cloud is slower than NFC to POS. In the U.S., for example, current 3G coverage is spotty outside urban areas, leading to intermittent connectivity issues and slow speeds. Connectivity to the cloud is required at the moment a transaction is made, even more so for transit payments than retail purchases, so speed is critical. Contingency payment options, such as NFC, Wi-Fi, plastic card, or a hybrid solution using the push cloud model to store a token on the mobile phone for offline transactions, need to be established for cloud payments.

Storing payment credentials in the cloud for a digital wallet is new and relatively untested with scale. There are still many unknowns to be addressed. Because payments data can be compromised in the

---

[24] On July 10, 2012, the FFIEC Information Technology Subcommittee issued a white paper addressing the key risks of outsourced cloud computing identified in existing guidance for financial institutions to consider. See http://ithandbook.ffiec.gov/media/153119/06-28-12_-_external_cloud_computing_-_public_statement.pdf.

cloud, it is essential that: (1) payments data is not transmitted via SMS or e-mail because these platforms are not encrypted; and (2) payments to the cloud are transmitted between secure, encrypted endpoints handled either by mobile carrier data networks or merchant-provided secure Wi-Fi hotspots, and are not transmitted unencrypted over any network.

Data privacy remains a key concern for payments data stored in the cloud. Cloud providers control consumer data, so they have both a legal and ethical responsibility to protect it. They need to comply with privacy laws and make sure they obtain explicit consumer permission (opt-in) before sharing consumer information with other businesses, or mining data to companies interested in monitoring consumer spending behaviors. They need to make sure their underlying payment services are secure and resilient. Collaboration between banks and merchants will help to ensure consistent support for protecting the privacy and security of the consumer data.

IV. OTHER MOBILE PAYMENT TECHNOLOGIES[25]

QR code for mobile payments at POS

Today, mobile phones with cameras can be used with barcodes to perform various functions, including mobile payments and loyalty programs. QR code use has expanded in the past year, providing incentive for consumers to use their smartphone cameras and related mobile apps to scan barcodes to access sites on the Internet, download products, find reviews and information, or pay for purchases.[26]

To initiate a POS mobile barcode payment, the customer opens a previously loaded mobile app for the selected merchant. The mobile app generates a dynamic QR code, which the customer scans at the POS terminal scanner, (which may be another mobile device enabled with a downloaded reader).
The merchant's POS system uses the consumer's account information obtained from the barcode to retrieve his payment credentials from the cloud and process the payment over the card network. The consumer's real payment credentials are not stored on the mobile phone or merchant terminal.

---

[25] While not in the scope of this paper, biometrics, such as using fingerprints to authenticate the consumer in addition to name and password, is gaining more attention as a potential method for protecting consumer data in the mobile environment and should also be explored as part of a mobile risk management initiative.
[26] "QR Codes: How Apple Passbook Changes the Merchant Equation," Javelin Strategy & Research, July 2012.

Barcodes can be susceptible to a number of security risks. Malicious QR codes can contain URLs with hidden malware, or redirect to a fake websites to commit fraud, download malware, or phish for credentials. Because of their small screens, smartphones are more prone to phishing scams which try to trick victims into entering sensitive details to a fraudulent website that looks legitimate. If the barcode implementation is not for a proprietary system, the risk of fraud increases.

There are several tools that could help minimize security risks associated with barcodes, including anti-virus and anti-malware on smartphones. For some barcode payments apps, such as the Starbucks app, customers can add passcode protection to prevent use of the app if the phone is lost or stolen. Also, a customer must enter an ID and password to reload the Starbucks account.

Direct Carrier Billing (DCB)

Direct carrier billing is not accepted at physical retail locations in the United States, but can be used to purchase digital content such a ringtones and wallpapers from online stores or make charitable donations, e.g., to the Red Cross for the Haiti earthquake, and most recently for Hurricane Sandy. AT&T, Verizon, T-Mobile and Sprint have all launched DCB services in the last several years. And acceptance of DCB payments by several large online companies, such as Google and Facebook, may increase adoption.

To make a DCB payment, the customer enters his mobile phone number during the online checkout process. The DCB service provider sends an SMS message containing a PIN code to the customer's mobile phone. The customer either enters the PIN on the checkout screen or responds to the SMS message from his mobile phone. The charge is then applied to the customer's monthly mobile phone bill.

DCB offers a simple and convenient method for consumers to pay for low value digital goods and services. Since customers already have existing relationships with their mobile carriers, they do not have to share their payment credentials with third party providers. There is also a reduced risk that the purchaser is not the account holder. To manage carrier risk, DCBs set different transaction value limits depending on the carrier. Initially set at $25, limits have increased to $100-200 based on increased consumer use.

There are risks associated with using DCB; cramming being one of the most serious. While all mobile payment methods are susceptible to fraud, cramming is unique to DCB. According to the FCC, "cramming is the practice of placing unauthorized, misleading or deceptive charges on a customer's telephone bill." Crammers rely on confusing telephone bills to trick consumers into paying for services

they did not authorize or receive, or that cost more than the consumer was led to believe.[27] A crammer charges a customer's account without the customer's full knowledge or full understanding of the transaction. The charges go through undetected because they are labeled as phone-related services (e.g., voicemail, collect calls) or they are generic recurring charges (e.g., membership, subscriptions). Consumers must proactively check their bills carefully to make sure they are not victims of cramming. The FCC recently introduced the "Truth-in-Billing" rule in order to prevent cramming. It requires MNOs to organize bills with a clear, specific layout accompanied by understandable descriptive language for describing services for which a customer is being billed.

Compared to other mobile payment methods that are cleared and settled over traditional payment networks (e.g. credit, debit, and ACH) and governed by bank regulations that limit consumer liability, DCB mobile payments do not provide the same clarity of coverage and consumer protection. Carrier-offered protections are inconsistent. Examples of differences in protections include charges related to lost or stolen devices, late fees, reporting of disputed charges, and requesting refunds. Unless mobile carriers offer protections which are on par with credit or debit card, there is a financial risk to the consumer that differs from other financial instruments covered by Reg. E or Reg. Z.

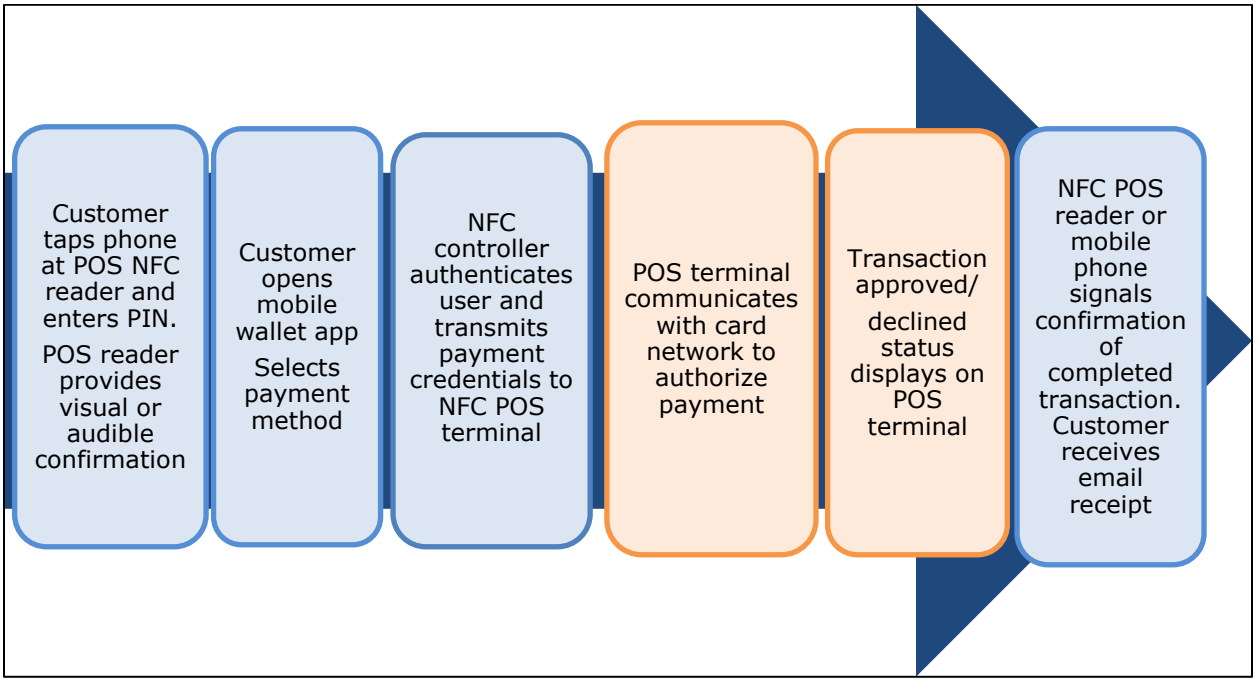
V. OVERVIEW OF MOBILE PAYMENT PROCESS FLOWS AND KEY DIFFERENCES

The different mobile payment technologies—NFC, cloud, and barcode—all enable consumers to make payments at the POS. At a high-level, the process flows for each platform share similarities as well as some key difference, particularly in how a payment is initiated, the storage location of a consumer's payment credentials, content of data that is transmitted, and how a consumer's payment credentials are identified. In all instances, the customer is required to enter one or multiple passwords to access his mobile wallet application and/or unlock his mobile phone.

A consumer initiates an NFC-enabled mobile payment by tapping or waving his phone on an NFC-enabled contactless reader at the POS. The consumer's payment credentials (e.g., credit or debit card account number) are encrypted and stored in the secure element on the phone. Using NFC communication protocols, the mobile phone communicates the consumer's payment credentials to the merchant's POS system.

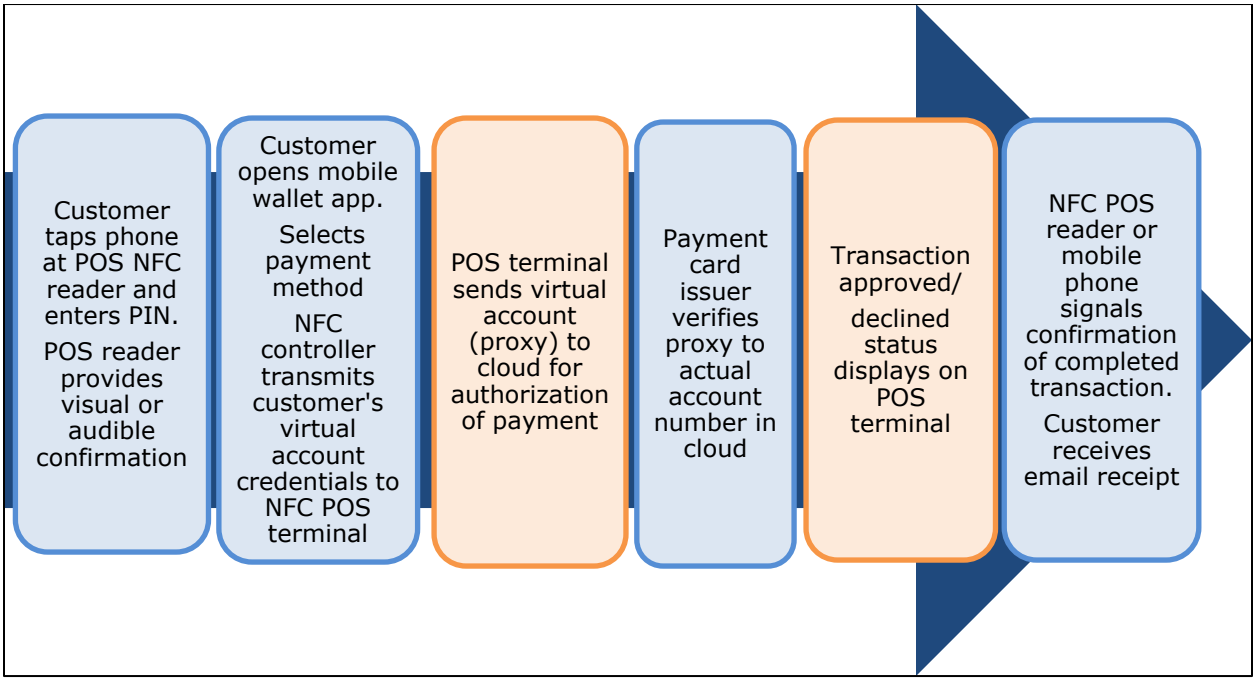
[27] http://www.fcc.gov/guides/cramming-unauthorized-misleading-or-deceptive-charges-placed-your-telephone-bill

NFC Contactless Model



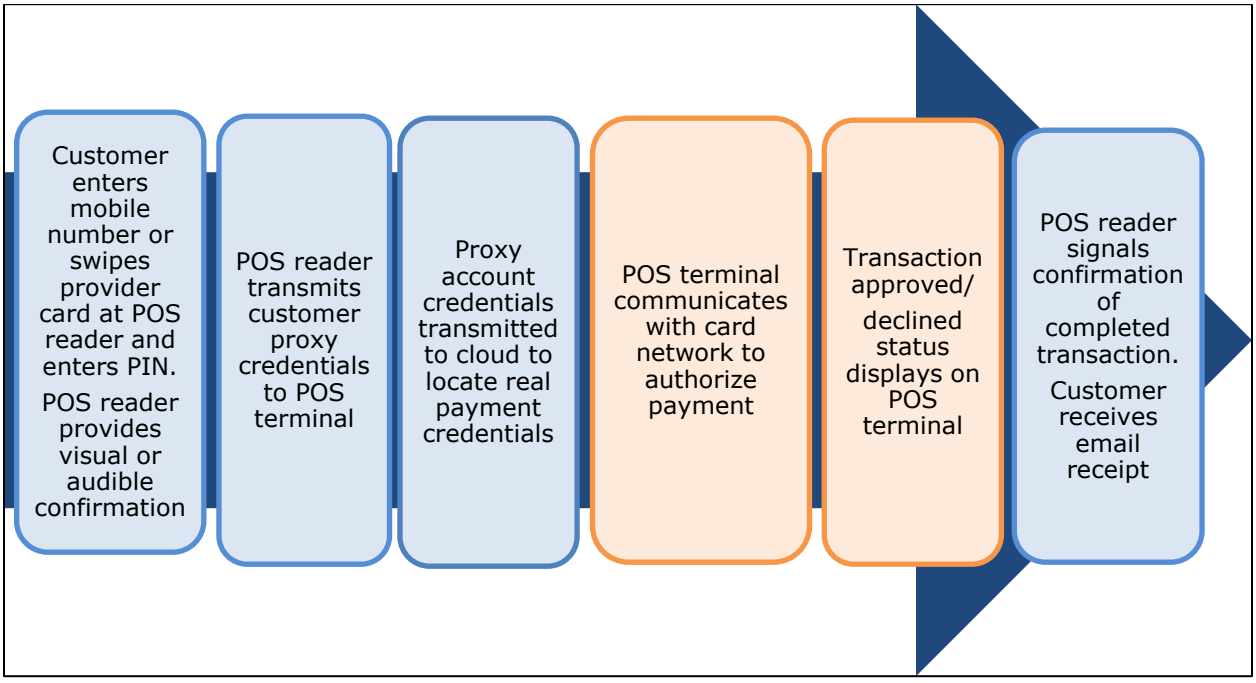
Initiating a hybrid NFC-cloud mobile payment is the same process as an NFC-only payment, but the payment credentials are not stored locally on the mobile phone. Instead, a virtual account number or proxy is stored in the secure element and used in communication from the mobile phone to merchant's POS system, which is then used to identify the customer's real payment credentials which are encrypted and stored remotely on servers (the cloud). Neither the merchant nor the mobile phone's operating system has the real payment card information.

Hybrid Cloud Model



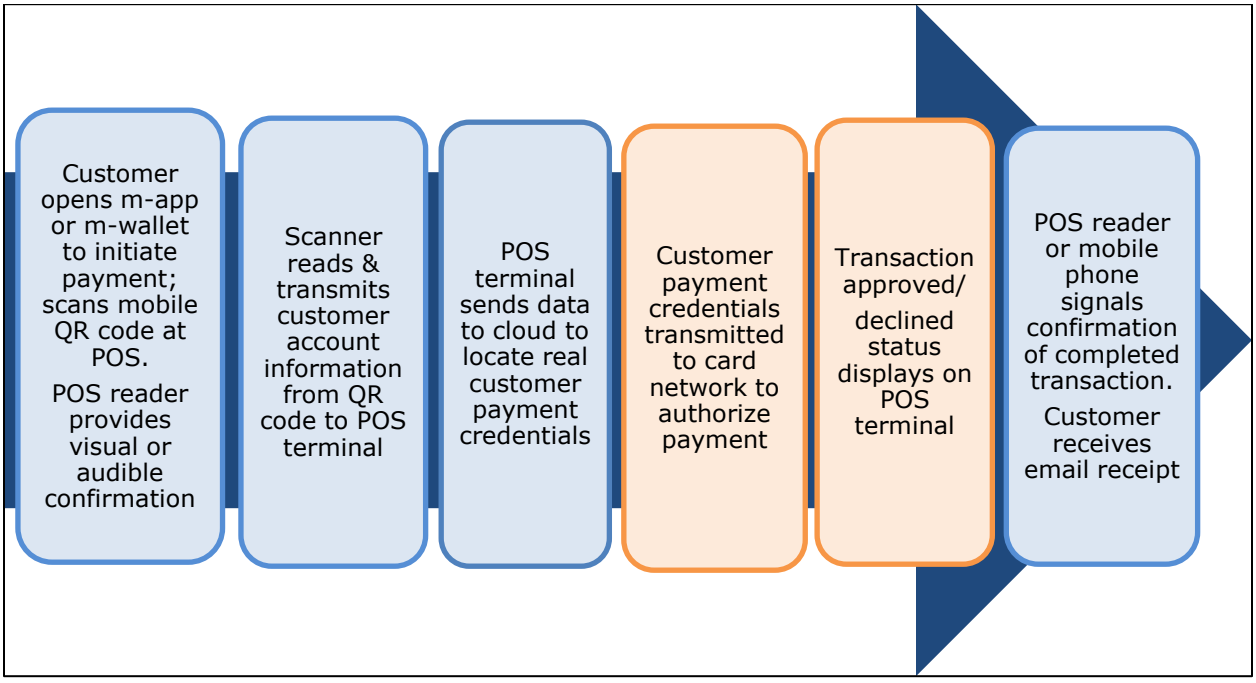
A consumer initiates a true cloud payment by entering his mobile phone number at the POS or swiping a proprietary card. The physical mobile phone is not required to complete the transaction. Similarly to NFC-cloud payments, a virtual account number is communicated to the merchant's terminal, which is used to retrieve the consumer's payment credentials stored in the cloud.

Cloud Model



To make a QR code payment the consumer opens a mobile application to retrieve and display the barcode for the specific merchant on his mobile phone, and then scans the QR code at the POS scanner. The merchant's POS system uses the consumer's account information associated with the barcode to retrieve his payment credentials from the cloud to process the payment over the card network. Like other cloud-based payment systems, the consumer's real payment credentials (e.g., credit and debit card account number) are never stored on the mobile phone or merchant terminal.

QR Code Model



In all cases, the merchant online authorization process begins after the consumer's payment credentials have been properly identified. The payment and settlement processes are the same processes used when the consumer pays with a traditional credit or debit payment card. When the transaction is complete, the consumer is alerted either via his mobile device or the POS reader, and receives an emailed receipt.

VI. CONSUMER RISKS AND MITIGATION OPPORTUNITIES

Because mobile payment transactions involve numerous participants, a physical device, a new payment channel, and unique mobile applications, there are multiple points of risk in the process. Securing the mobile technology platform or solution is only one component in the risk management process. Interestingly, the weakest link in the mobile payments security chain may be the consumer rather than the technology or hardware. Many consumers fail to take even the simplest precautions, such as protecting their mobile phones with passwords. Consumer education about how to protect the mobile phone, especially when used for financial transactions, is essential. However, mobile payment providers should continue to implement tools that protect both hardware and software to minimize the potential for human

error. A 2012 Javelin report[28] on identity fraud found 33% higher incidence of fraud among smartphone users than in the general public. It suggested that poor user security practices, e.g., a smartphone owner not using a password to protect the phone (almost 66% do not) or saving log-on credentials on the device, may be partially responsible for this difference. Saving log-on credentials, also known as 'Remember Me,' is much riskier when these credentials are linked or authorized to access payment apps.

The most well-known causes of mobile security breaches include:

- **Insufficient controls on a mobile device** that allow negligent, accidental, or malicious mobile user behavior, (including a lost/stolen phone, frivolous app downloading, and jail-breaking (iOS) or rooting (Android) a device). Jail-breaking Apple iOS phones or rooting Google's Android OS phones allows third party apps that are not certified or approved by Apple or Google to run on a mobile device and modify the mobile phone to gain access to and control of the operating system.[29] Downloading any uncertified or unknown source applications increases the risk of the app containing malicious code (malware) or viruses, which enable unauthorized 'back door' access to account credentials and lead to loss of sensitive information, stolen credentials, fraudulent transactions, and compromised data. *Mobile spoofing* uses a malicious app to fraudulently misrepresent a legitimate brand and obtain sensitive personal information. This can lead to identity theft, stolen confidential information, and potential financial loss to consumers and banks. If fraudsters gain access to the customer's personal financial information through mobile malware or spoofing, they can use the data to access online bank accounts or purchase goods and services in a card-not-present Internet environment. While this is a major security concern, with proper education and support from the mobile payments providers, customers can take precautions to protect their mobile devices and payment information.
- **Inadequate mobile payment provider fraud controls**. Poor monitoring, detection and prevention tools can also cause undetected or unauthorized access to financial data and unauthorized transactions, leading to fraud losses. Many security software vendors are

[28] "2012 Identity Fraud Industry Report: Social Media and Mobile Forming the New Fraud Frontier," Javelin Strategy & Research, February 2012.

[29] Jail-breaking or rooting a mobile phone enables the user to exploit vulnerabilities in the iOS or Android operating system to gain administrative or root-level access to the device and undermine the OS security infrastructure. These apps can perform other functions such as 'unlocking the mobile device to work with a different carrier, enable user interface changes, use the phone as a mobile hotspot, and expose the customer to harmful apps that contain viruses, worms and other malware. These actions will void customer warranties as the handset manufacturers and carriers do not support jail-breaking and rooting, although according to the American Copyright Office these actions are legal. See http://www.wired.com/threatlevel/2010/07/feds-ok-iphone-jailbreaking/

developing mobile fraud tools, but a comparative analysis needs to be done to assess their abilities to address mobile payments security holistically.

Mobile stakeholder cooperation is key to enhancing mobile payments security

Mobile stakeholders, including FIs, mobile carriers, regulators, card networks (debit, credit, and prepaid), mobile payment and solution providers, and merchants need to share responsibility and work cooperatively to enhance mobile payments security and protect consumer privacy. This requires a combination of best practices and robust standards, along with the appropriate tools, such as:

- Developing a standard, technology-agnostic certification process to safely provision mobile phones and wallets. The process should include certifying mobile wallets before they are loaded into the secure element on the phone and certifying all payments-related vendor applications prior to being accessible in an app store and loaded to the mobile wallet. Certification and testing can help to ensure that data are encrypted during transmission and while stored, and that financial applications are virus- and malware-free before they are available in an app store. Use of end-to-end encryption should be a standard for protecting any mobile payment transaction stored on the phone, remotely on a file server, and when data are in transit over the wireless network, including bank account and card numbers and passwords.[30]
- Developing a cohesive, coordinated approach for the consumer to conduct mobile payments, regardless of the choice of handset, carrier, mobile wallet, or technology.
- Developing guidelines to help consumers mitigate mobile risks, identify mandatory and opt-in security features, and include full disclosure on the risks of various options and how to resolve any problems. Consumer guidelines could address topics such as:
    - Mobile apps: A consumer should only download applications or other software from reputable sources. If the consumer is uncertain about the source, he should be instructed to contact his financial institution or other mobile service provider. He should never click on unknown links in a mobile web browser and should install mobile malware detection and antivirus software on a mobile device, which can detect malware on the phone, in a mobile application or on a mobile webpage. Finally, consumers should understand the importance of

[30] Customer authentication determines whether a person attempting to access his account information is who he says he is. Means of authentication can be passwords, personal security questions, digital certificates, and multi-factor authentication, which uses two or more factors to identify a consumer (e.g., password, personal security questions, pictures, or biometrics).

checking app update notifications regularly in the app store and accepting app update push notifications for available certified fixes to protect against known vulnerabilities and limit risk.

- Jail-breaking: Consumers should never compromise their mobile phones by jail-breaking (iPhone) or rooting (Android). While usability might be enhanced, it increases the risk that the mobile phone will be vulnerable to attacks because altered devices are specifically targeted by malware. Using a jail-broken or rooted mobile phone also violates the policies of the mobile carriers, who may deny any accountability for a problem or breach from a compromised phone. When possible, FIs, and mobile payment providers should consider disabling these features from their mobile apps.[31]
- Mobile wallet: The mobile payment/wallet provider should ensure that the consumer does several things: (1) protects the mobile phone in the same way as a physical wallet by never leaving it unattended and keeping it in a secure location at all times; (2) creates strong passwords/PINs to protect the mobile device and any financial applications on the phone; (3) uses a different PIN for wallet access; (4) enables auto device time-out to automatically lock the phone when not in use to help prevent unauthorized users from gaining access to sensitive data; and (5) enables the mobile phone's remote device lock and wipe features to allow data to be erased and the mobile phone to be locked from a remote location if it is lost, misplaced, or stolen.[32] The consumer should be instructed to immediately report the loss to the mobile carrier and/or financial institution. Lastly, a consumer should work with his mobile carrier or provider to securely remove all data from his mobile phone before disposing of it.
- Alerts: Mobile payment providers should encourage customers to set up real-time alerts through their card issuing or primary bank to receive email or text notifications of suspicious account activity, purchases that exceed preset dollar limits per transaction or per day, and other available risk management options. Alerts can provide consumers and FIs with information to help them detect mobile fraud, identify and assess the cause of a breach, and avoid future compromises and fraudulent account activity. Alerts can empower consumers to take immediate action and engage them in sharing in the responsibility for preventing fraud and identify theft.

---

[31] One way to mitigate jail-breaking would be for MNOs and other reputable distribution channels to begin to offer more interoperable mobile handsets across various mobile carriers and vendors.

[32] Apple's free 'Find my iPhone' app lets users locate a missing device, remotely lock it and then wipe it. Kelli B. Grant, 'Keeping Prying Eyes off Your Phone,' Smartmoney.com February 21, 2012.

- Wi-Fi use: Since public Wi-Fi networks may be unsecure, consumers should be educated to understand the risks of using them to conduct personal financial activity (e.g., paying bills, providing credit card information, transferring funds, etc.).

VII. CONCLUSION

The primary purpose of this paper was to identify and describe different mobile payment technology platforms and provide a high level comparison of the security of each alternative, without showing a bias to any one particular option. While the mobile technologies covered may be relatively proven for other purposes, they are still considered nascent for mobile payments. Each has different strengths and weaknesses depending on the venues in which they are used; in other words, not all mobile technologies are optimum for all payment-related purposes. NFC with the secure element provides extensive and mature security features suitable for POS; however, all technologies need continuous improvement as they are integrated into the mobile payment system, particularly as they impact consumer use. Because consumers tend to apply the minimum protections, security providers need to anticipate problems and incorporate automated risk mitigation tools where feasible, leveraging the ability of mobile phones to share real-time data, such as location and customer-entered authentication, regardless of the technology platform. For example, use of a mobile network and geo-location can indicate whether a mobile transaction was conducted in the same place as the phone itself.

Many parties are involved in supporting the multi-faceted mobile payments ecosystem. Private and government sectors, and banks and non-banks must collaborate to mitigate related security and fraud problems. Together they need to identify potential vulnerabilities, share applicable data, conduct security analysis of weak points in the mobile process, and determine who is responsible for fixing them. Then they will have the tools to develop reliable controls, education plans and standards that may be needed.[33] This is a complex task that will not be achieved in silos, or by just one entity, but only through collaborative efforts, which will be a win-win for all mobile stakeholders, especially the consumer.

[33] Achieving enhanced fraud and security capabilities is not simple. For example, telecommunication laws limit the ability of mobile carriers to share or use security-enhancing information, such as location, which is limited by CPNI (Customer Proprietary Network Information) rules, without a customer's explicit consent. And, even if that data could be shared, FIs must assess their own ability to use that information in a cross-channel payments process to best mitigate fraud.

APPENDIX I. EXAMPLES OF MOBILE SECURITY VENDORS

ABnote provides a TSM service which has received certification from both MasterCard and Visa.

AuthenTec is a provider of mobile and network security products that help protect individuals and organizations through secure networking, content and data protection, access control and strong fingerprint security. Solutions include mobile applications for VPN, device encryption and DRM, and security toolkits and semiconductor IP. They also offer tools that help people manage their digital identities and enhance the fingerprint sensor user experience at work and home. Their smart sensors enable fingerprint security to be added to PCs, peripherals, phones and other products. AuthenTec was acquired by Apple in July, 2012.

Authentify provides phone-based out-of-band authentication services for many large online business enterprises, allowing them to quickly and cost-effectively perform real-time, multi-factor user authentication during an Internet session and protect against man-in-the-middle and man-in-the-browser attacks used to steal login credentials or hijack online sessions. The OOB service enables banks and other financial services firms to make certain the legitimate account holder is the user initiating an online transaction. 2CHK is a unique feature that is an 'always on' out-of-band authentication service that maintains a secure second channel to Authentify's authentication service. The bank or ecommerce provider can use this second channel and the 2CHK app to securely show customers the actual transaction details generated on one device (e.g. a PC) and let them approve or reject them on the second device (e.g. a mobile phone).

CorFire offers CorTSM, a TSM service platform that acts as a bridge between financial institutions, MNOs, and other players to allow mobile payments to be carried out successfully. It received MasterCard GVCP security compliance certification as well as meeting PCI DSS, Triple DES, and Global Platform standards/regulations.

Confident Technologies provides web, mobile and multi-factor authentication tools. Its mobile authentication tools are mostly image-based. As a replacement for the traditional CAPTCHA (e.g., an image of obscured text, that must be copied into a box to verify an actual human user), the correct image must be selected from a set of 12. This has a wide range of uses, including app security, transaction authorization, persistent login, or BYOD.

Entersekt Technologies provides 'emCert' for mobile devices, which limits the chances of man-in-the-middle type attacks by providing a secure encrypted channel between the user and enterprise. It also provides end user identification tools. Banks use Entersekt's Interactive Transaction Authentication (ITA) to provide customer authentication to their banking services when accessing accounts via web, mobile, VPN, and other channels. ITA uses a secure channel.

MobileIron develops mobile device management software to secure and manage mobile apps, content, and devices for global companies. Innovations include multi-OS mobile device management, mobile application management, and BYOD privacy controls.

Sequent Software splits TSM services into two discrete roles: Credential Management and Secure Element Management. It concentrates solely on secure element management through its PaaS offering Sequent Secure Element Management.

ThreatMetrix is an industry solution that integrates malware detection and device identification technologies in a single, unified platform with shared, centralized intelligence that works to minimize the risk in online transactions.

Trusteer provides a standalone app or a SDK (software development kit) which developers can use to embed Trusteer Mobile into their application.

Validity is a leader in Natural ID™ authentication, providing secure, cost-effective fingerprint sensor solutions for mobile payment transactions and cloud-based services. Passwords and PINs can be ineffective at meeting the needs of end users and service providers as they're either too easy to hack or too hard to remember. Natural ID provides a simple and effective way to optimize usability while providing strong security, authenticating users by their unique human characteristics such as fingerprint, voice, and face.

viaForensics is a digital security firm that focuses on computer forensics, mobile forensics, and mobile app security for iOS and Android, enterprise security, and forensics training. It offers a suite of services for mobile and enterprise security.

Voltage Security specializes in data encryption with a dedicated section on transaction security. It provides end-to-end encryption and tokenization for transactions from the point of capture to authorization, settlement and beyond. Two of its products, Identity-Based Encryption and Format Preserving Encryption, combine to enable this. It also offers cloud data encryption technology.

Webroot is a security software company with a wide range of online security products for home and office. Webroot protects corporate networks and allows consumers to download music, store digital files, bank, shop, surf and search – safely. Mobile security products are available for both Android and iOS.

APPENDIX II. COMPARISON OF MOBILE PAYMENT TECHNOLOGIES[34]

		ADVANTAGES / DISADVANTAGES	ISSUER / OWNER / CONTROLLER OF NFC SECURE ELEMENT
NFC Non-Removable Secure Element	Embedded	• OS platform-independent • Additional hardware costs (e.g., onboard embedded-chip integration costs) • Might cause issues when user upgrades a handset	Chipset, platform & handset manufacturer
NFC Removable Secure Element	SIM / UICC	• OS platform-independent • No additional hardware costs • No issues with handset upgrades	Mobile operators
	microSD card	• OS platform-independent • Additional hardware costs for micro SD card • Needs SD card slot • No issues with handset upgrades	Handset manufacturers, mobile operators, financial institutions, retailers
Cloud		• Leverages existing payment terminals • No special consumer device needed • Strong link to online channels • Limited capability to enable value-added features (e.g.,loyalty, rewards, etc.) • Potential trust issues	
QR Code		• Leverages existing POS systems • Works on most devices and operating systems • Low upfront and ongoing costs • Weaker security • Lack of standards • Not broadly recognized as a payment method	

[34] Adapted from 'Strategy Analytics Insight,' July 24 2012, and 'NFC Mobile Payment: Opportunities, Threats and Future Outlook,' VDC Research white paper for M for Mobile, August 2012. www.mformobile.com/paymentsusa/