MASTERCARD BEST PRACTICES FOR MOBILE POINT OF SALE ACCEPTANCE

A Guide to Enabling Acceptance on Mobile Devices

This document provides best practices for the development and deployment of Mobile Point-of-Sale (Mobile POS) acceptance solutions. These solutions allow merchants to use mobile devices as point-of-sale terminals and facilitate MasterCard and Maestro payment transactions. Here we will use the term "mobile devices" to refer to consumer-oriented, multi-purpose mobile computing platforms, including feature phones, smartphones, tablets, and PDAs.

The goal of this document is to introduce best practices to facilitate the growth of Mobile POS acceptance. This document recommends actions, practices, and product features to provide a consumer payment experience that is simple, safe, and consistent with other acceptance channels. When implemented, these best practices promote the integrity of MasterCard payments by maintaining the confidentiality of cardholder credentials and building cardholder trust.

Please note, the best practices in this document do not supersede MasterCard standards as defined in MasterCard Rules. MasterCard standards and local laws take precedence over the guidelines and provisions of this document.

33% At least a third of all POS systems will be either a tablet or smartphone within the next five years.[1]

AUDIENCE

This document is intended for all entities that develop, deploy, or use Mobile POS solutions. Audiences include:

- Acquirers, payment facilitators, hardware vendors, and software providers
- Merchants who use or are interested in using Mobile POS solutions, including those who have a direct relationship with a MasterCard acquirer
- Sub-merchants who use the services of a payment facilitator
- Issuers and others in the payment industry interested in mobile point-of-sale

1. Juniper Research study.

BACKGROUND

Today, smartphones provide users with an ever-expanding set of features and capabilities, including music, gaming, digital imaging, global positioning systems, social networking, Internet browsing, email, and text messaging, just to name a few. Smartphones are widely expected to have a significant impact on the electronic payments industry because they fill an immediate and strong need to move everyday transactions from cumbersome cash to cards and other forms of electronic payments. Doing so satisfies the payment needs of both consumers and micro-merchants.

Smartphones are widely expected to have a significant impact on the electronic payments industry because they fill an immediate and strong need to move everyday transactions from cumbersome cash to cards and other forms of electronic payments.

There are four primary types of mobile payments:

- Mobile proximity payments, such as those enabled by MasterCard mobile contactless, use the mobile device as an alternative for the card (information on MasterCard mobile contactless can be found at www.mastercard.com).
- Mobile web payments use the browser or application capabilities of the mobile device to conduct a card-not-present transaction (sometimes referred to as "mobile commerce" or "mCommerce").
- Mobile remote payments use the consumer's mobile device to initiate a transaction with a merchant who does not have the ability to process physical payment card transactions.
- Mobile POS allows a mobile device to be used as a merchant point-of-sale terminal.

Mobile devices are becoming ubiquitous around the world. According to the International Telecommunications Union (ITU, 2011), the global mobile phone market grew by 45 percent year over year from 2006 to 2011, with 5.9 billion subscriptions globally.

This document specifically addresses Mobile POS best practices. Mobile POS solutions allow merchants, including door-to-door salespeople, tradespeople, and street vendors, to easily accept MasterCard and Maestro payments via their mobile devices.

There are many potential advantages for merchants who use Mobile POS solutions versus typical purpose-built POS terminals:

- **Lower total cost of ownership**, as many Mobile POS solutions are being offered either for free or at a very low cost. Many merchants already own suitable mobile devices, so they can avoid additional costs related to purchasing, deploying, and maintaining a POS terminal.
- **Better portability and greater ease of use**, which are important factors for mobile merchants with no fixed place of business.
- **More flexible software development platforms** that can integrate with existing environments.
- **Better user interfaces** for both the merchant and consumer.

MasterCard believes that Mobile POS solutions will appeal to:

- Merchants who find the cost of purpose-built POS devices too high for profitable card acceptance, particularly small merchants who have low retail volume.
- Merchants who need an alternative to landline communications due to a lack of available infrastructure or because of the mobile nature of the merchant's business.
- Merchants who wish to enhance the retail experience by shortening lines or offering product look-ups and payment throughout the store.

Currently, Mobile POS solutions are being adopted by small businesses that have never accepted card payments and that previously operated on a cash- and invoice-only basis. Additionally, retailers that already accept card payments are adopting Mobile POS solutions and integrating them into their current point-of-sale environment to enhance the retail and payment experience.

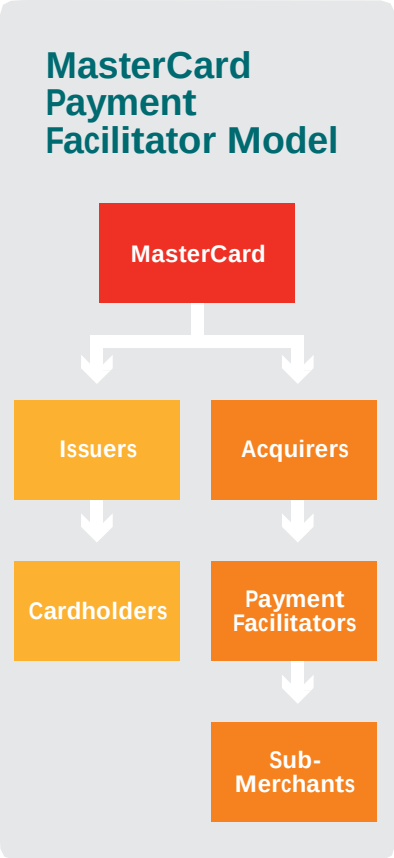
MOBILE PAYMENT FACILITATORS AND ACQUIRERS

Mobile POS solution providers may offer their products to merchants via the traditional acquiring channel. In these cases, the merchant maintains a direct relationship with a MasterCard licensed acquirer and simply uses the Mobile POS solution as an alternative to the traditional point-of-sale terminal.

Alternatively, Mobile POS solution providers may make use of the MasterCard Payment Facilitator model. In these cases, the MasterCard Payment Facilitator has a direct merchant agreement with a MasterCard licensed acquirer. The MasterCard Payment Facilitator sells services to sub-merchants and manages the settlement of funds. The sub-merchant does not have a relationship with the acquirer and interfaces directly with the payment facilitator.

To qualify as a sub-merchant, annual sales must not exceed USD 100,000 in MasterCard and Maestro combined volume. If the sub-merchant exceeds this threshold, it is required to enter into a merchant agreement directly with a MasterCard licensed acquirer.

Mobile POS solution providers that make use of the MasterCard Payment Facilitator model must be registered in the MasterCard Payment Facilitator program. This program has specific rules and requirements, including sub-merchant screening procedures, merchant agreement provisions, reporting requirements, transaction submission requirements, and requirements that ensure payment system integrity. It is also a requirement for payment facilitators to comply with all MasterCard on-boarding and merchant monitoring requirements for their sub-merchants, as defined in MasterCard standards. Payment facilitators must also comply with all local laws and regulations regarding merchants, including adequate Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements.



MOBILE POS CARD READER ACCESSORIES

Typically inexpensive and easy to deploy, Mobile POS card reader accessories attach to the audio port, USB port, or proprietary connector on mobile devices. They may also connect via Bluetooth to the mobile device. These accessories provide for magnetic stripe, EMV (Europay, MasterCard, and Visa) chip, and contactless acceptance, and are sometimes referred to as "dongles." Some Mobile POS card reader accessories are referred to as "sleeves." Mobile POS sleeves generally wrap around or encase the mobile device, and may be capable of performing magnetic stripe, EMV chip, and near field communication (NFC) contactless transactions with PIN verification.

Mobile POS card reader accessories work in conjunction with a Mobile POS payment application that resides on the mobile device. The payment application provides the merchant with an interface to the Mobile POS solution, allowing merchants to select the transaction type, enter the amount of the transaction, and enter any details required for delivery of a receipt. The payment application interfaces with the Mobile POS solution provider's back-end system, which provides payment-related functions.

INTEGRATED CONTACTLESS MOBILE POS SOLUTIONS

Integrated contactless Mobile POS solutions perform contactless transactions via an NFC antenna within the mobile device. Mobile POS contactless solutions provide for MasterCard contactless and Maestro contactless acceptance, and also facilitate acceptance where the consumer's mobile device is a replacement for the payment card.

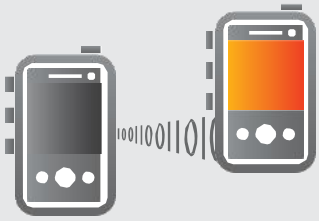
Integrated contactless Mobile POS solutions will introduce new data security challenges but are currently still in development and will not be covered directly by these best practices. Mobile POS solution providers who are building integrated contactless solutions should still become familiar with the best practices in this document so they can build solutions that provide a consistent user experience with robust data security capabilities.

Once available, Mobile POS integrated contactless solutions may be complemented with a Mobile POS card reader accessory, providing both contact and contactless payment card acceptance.

Types of Mobile POS Solution

Mobile POS solutions can utilize feature phones, smartphones, tablets, and PDAs. The feature set of the Mobile POS solution may vary according to the type of mobile device used. For example, smartphones are capable of signature capture via the touch screen, though many feature phones are not capable of signature capture without the use of an external device. Broadly speaking, there are two types of Mobile POS solutions:

1. Mobile POS card reader accessory solutions.



2. Integrated contactless Mobile POS solutions.

This document is limited to best practices for Mobile POS solutions that use Mobile POS card reader accessories. Best practices for integrated contactless Mobile POS solutions will be provided at a later date.

BEST PRACTICES

This section describes the best practices that Mobile POS solution providers should follow when developing and deploying Mobile POS solutions. Best practices are also provided for merchants and sub-merchants who use Mobile POS solutions.

1. Securing Mobile POS Payment Applications

The Mobile POS payment application allows the merchant to set up configuration details such as the merchant name, sales tax, and prompts for gratuity, and also to initiate a transaction by entering details like the transaction type and amount on the mobile device. The Mobile POS payment application interfaces with a Mobile POS solution provider or the acquiring bank's remote host system. The integrity of both the Mobile POS payment application on the mobile device and any hosted system is critically important to maintaining the security of transaction data and preventing data compromise incidents.

In accordance with MasterCard standards, merchants are required to use third-party provided payment applications that comply with the *PCI Payment Application Data Security Standard* (PA-DSS) and are listed on the PCI Security Standards Council (PCI SSC) Website, www.pcisecuritystandards.org.

UNIQUE CHALLENGE

Due to the inherent security limitations of mobile devices, the PCI SSC is not certifying Mobile POS payment applications that reside on multi-purpose, consumer mobile devices (referred to by the PCI SSC as a Mobile Payment Acceptance Application Category 3) until further guidance is developed to ensure the security of cardholder data within the mobile device. Please refer to the PCI SSC Website for more information.

BEST PRACTICES FOR MOBILE POS SOLUTION PROVIDERS

In lieu of being able to certify Mobile POS payment applications to the PCI PA-DSS requirements, Mobile POS solution providers should:

- Use industry-recognized secure coding practices when developing Mobile POS payment applications
- Ensure that software updates are provided in a secure way that prevents tampering and provides authentication of the source of the update
- Protect the application against reverting to an older version
- Have policies for handling lost and/or stolen devices and have the ability to remotely disable the Mobile POS payment application either on the remote mobile device or on the backend server

BEST PRACTICES FOR MERCHANTS

Merchants should consult their Mobile POS solution providers to understand the security their Mobile POS solution offers. Merchants whose Mobile POS solution is lost or stolen should contact their Mobile POS solution providers or acquirers immediately.

2. Securing Transaction Data Captured by a Mobile POS Card Reader Accessory

In accordance with MasterCard standards, any entity that stores, transmits, or processes cardholder data must comply with the data security requirements within the *Payment Card Industry Data Security Standard* (PCI DSS). This includes Mobile POS solution providers and merchants that use Mobile POS devices.

Additionally, in October 2011, the PCI SSC issued a new standard for building point-to-point encryption (P2PE) solutions entitled PCI *Point-to-Point Encryption Solution Requirements*. The PCI SSC is planning to certify P2PE solutions and maintain a list of certified P2PE-compliant solutions on its Website at www.pcisecuritystandards.com. Please check the PCI SSC Website for updates.

Mobile POS solutions that are compliant with the PCI point-to-point encryption solution requirements are considered compliant with the *MasterCard Wireless POS Terminals and Internet/ Stand-Alone IP Enabled POS Terminal Security Standards*.

UNIQUE CHALLENGE

Due to the open architecture of mobile devices and their susceptibility to malware, unencrypted cardholder data can be compromised. Furthermore, due to limitations with the security features of mobile devices, merchants who use Mobile POS solutions will find it challenging to comply with the requirements of the PCI DSS. There are also risks associated with fraudsters maliciously using legitimate or counterfeit Mobile POS solutions to perform malicious attacks on the core payment system network.

BEST PRACTICES FOR MOBILE POS SOLUTION PROVIDERS

Mobile POS solution providers are strongly advised to build Mobile POS solutions that utilize *Payment Card Industry PIN Transaction Security (*P2PE) in accordance with the *PCI Point-to-Point Encryption Solution Requirements*. It is recommended that transaction data be encrypted within the Mobile POS card reader accessory and that the enciphered data is transmitted via the mobile device to the Mobile POS solution provider or acquirer's remote host.

Compliant P2PE solutions will help minimize the risk of account data compromise. Mobile POS solution providers are recommended to build or use card reader accessories that are compliant with the PCI PTS standard. This will facilitate the certification of the Mobile POS solution against the *PCI Point-to-Point Encryption Solution Requirements*. The Mobile POS solution should also provide cryptographic authentication of the Mobile POS card reader accessory to ensure that data can only originate from legitimate merchants using genuine Mobile POS solutions. The data received from the Mobile POS solution should be validated to ensure its authenticity.

BEST PRACTICES FOR MERCHANTS

Merchants are strongly advised to use Mobile POS solutions that utilize P2PE solutions in accordance with the *PCI Point-to-Point Encryption Solution Requirements*.

3. Securing Personal Account Numbers (PAN)

There are various situations where a merchant may handle the cardholder's MasterCard account number, sometimes referred to as the personal account number or PAN.

In cases where a magnetic stripe read fails, the fallback mechanism may be a "key-entered" transaction where the merchant manually enters the cardholder's PAN using the keypad of the mobile device. Key-entered transactions are considered less secure than contact (magnetic stripe or EMV chip) or contactless payments.

In accordance with MasterCard standards, merchants may store a cardholder's name, expiration date, service code, and PAN after authorization to facilitate dispute resolution. If a PAN is stored, whether on the mobile device or on a hosted system, it must be protected in accordance with the requirements of the PCI DSS.

UNIQUE CHALLENGE

Mobile devices may be susceptible to key-logging software or malware, and as a result, data entered on the keypad may be at risk. The mobile device has limited capabilities to secure PANs that are key-entered on the touch screen or mobile device keypad or to store PANs securely for dispute resolution purposes.

BEST PRACTICES FOR MOBILE POS SOLUTION PROVIDERS

A PAN should not be retained on the mobile device. If a Mobile POS solution provider allows PANs to be key-entered, the Mobile POS solution should employ encryption of the PAN for transmission purposes.

BEST PRACTICES FOR MERCHANTS

Merchants should be aware that key-entering PAN data is less secure than a contact (magnetic stripe or EMV chip) or contactless transaction. Merchants should consult their Mobile POS solution providers and acquirers to better understand the risks associated with key-entered transactions and to ensure that the solution is properly securing PANs.

4. EMV Chip Transactions

The use of magnetic stripe is still prevalent globally, and as a result, data elements such as the PAN and PIN must continue to be treated as sensitive data, especially since PAN can be used to facilitate card-not-present fraud. In the future, as EMV becomes ubiquitous globally, the sensitivity of these data elements may decrease. However, EMV migrations are still ongoing in various markets around the world, and the use of magnetic stripe will continue for years to come.

The core requirements for EMV terminals and acquirer host processing of chip transactions are contained in the *MasterCard M/Chip Requirements*, downloadable by MasterCard customers from MasterCard Connect at www.mastercardconnect.com.

UNIQUE CHALLENGE

Due to open architecture and the remote nature of mobile devices, there are important considerations to be made concerning transaction authorization, card authentication, transaction performance, and the security of the payment system public keys.

BEST PRACTICES FOR MOBILE POS SOLUTION PROVIDERS

The EMV level 2 kernel can be located on the mobile device, on the remote server, or split between both. Depending on the architecture, the location or locations chosen may negatively affect performance. Mobile POS solution providers should ensure that the architecture of their EMV solutions maintain transaction performance and do not introduce significant latency, and therefore create a poor cardholder and merchant experience.

Mobile POS solutions should be configured for online-only authorization. This affords the issuer better fraud management protection in this new acceptance environment. In instances where there is no available network connection, transactions should not be authorized offline.

As all transactions will be authorized online, the issuer will perform online card authentication method (CAM). Mobile POS solutions that support EMV mode contactless transactions must support the offline card authentication method (CAM) as per MasterCard's contactless rules and requirements. Offline CAM may be performed at the remote server, the mobile device, or both; however, the transaction performance must be maintained. If the mobile device is not capable of maintaining the integrity of the payment system public keys, then offline CAM cannot be supported on the mobile device. The Mobile POS solution provider must ensure that bogus keys cannot be inserted with malicious intent, and therefore Mobile POS solution providers should consider designs where the server verifies that the keys are correctly stored on the Mobile POS card reader accessory or the mobile device on a periodic basis.

As a reminder: EMV Level 2 Kernel is certified by EMV, and a Letter of Approval is issued that lists all the approved terminal configurations. The EMV L2 Kernel must have an approved configuration that matches the mobile POS features. This is crucial because the terminal understands its capabilities by invoking a particular approved configuration and not by hard coding the capabilities. EMV Kernels can be approved with multiple configurations.

BEST PRACTICES FOR MERCHANTS

When accepting EMV chip transactions, merchants are advised to only use Mobile POS solutions that have been approved by EMVCo (EMV Type Approval) and the MasterCard Terminal Integration Process (M-TIP).

5. Display of the MasterCard Acceptance Mark

Accurate and consistent use of the MasterCard acceptance mark provides cardholders with a clear indication that MasterCard-branded products are accepted and establishes expectations for a payment experience that is similar to all other MasterCard-branded transactions.

UNIQUE CHALLENGE

Displaying the MasterCard acceptance mark is a requirement for all merchants that accept MasterCard transactions. However, many merchants using Mobile POS solutions will not operate a storefront, stand, or kiosk. Therefore, the only opportunity to display the MasterCard acceptance mark may be on the mobile device, the Mobile POS card reader accessory, or the Mobile POS payment application.

Displaying the MasterCard acceptance mark on Mobile POS solutions may be challenging due to limited real estate on the mobile device itself, the mobile device display, or on the Mobile POS card reader accessory.

BEST PRACTICES FOR MOBILE POS SOLUTION PROVIDERS

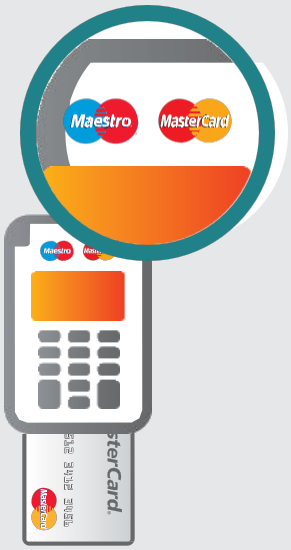
Mobile POS solution providers should provide MasterCard acceptance decals to merchants and provide instructions on how to display the decals where possible.

Where possible, the Mobile POS solution provider should make provisions to display the MasterCard acceptance mark on the mobile device (via the app) or on the Mobile POS card reader accessory. In instances where MasterCard branding is displayed with other brands on a POS terminal, the MasterCard branding must appear at visual parity with the other brand(s) displayed. To achieve parity with all other brand marks displayed, the acceptance mark must be at least as prominent and appear in at least the same frequency, size, and color treatment as the largest other acceptance mark displayed. For more information, visit www.mastercardbrandcenter.com/us/howtouse/amu_home.shtml

BEST PRACTICES FOR MERCHANTS

For merchants that operate a storefront, stand, or kiosk, MasterCard standards and guidelines apply to the display of the MasterCard and Maestro acceptance marks, even if the merchant utilizes a Mobile POS device. Guidelines for the display of the MasterCard and Maestro acceptance marks can be found on the MasterCard merchant Website at www.mastercardmerchant.com.

MasterCard Acceptance Marks on Mobile POS



6. Merchant Confirmation

The cardholder has a certain degree of confidence that they are dealing with a legitimate MasterCard merchant when there is a storefront, a MasterCard or Maestro acceptance mark, and other factors that provide a degree of comfort and familiarity.

UNIQUE CHALLENGE

Many merchants who use Mobile POS solutions may be mobile and not operate a storefront. As a result, consumers may question whether those merchants are in fact legitimate MasterCard merchants. Growth in the Mobile POS channel is dependent upon consumer trust and, ideally, consumers should have the ability to verify that a merchant is legitimate.

BEST PRACTICES FOR MOBILE POS SOLUTION PROVIDERS

Mobile POS solution providers should provide the ability for cardholders to confirm that a merchant is a legitimate customer of their solution. This can be accomplished with identification cards, serial numbers, a publicly available Website with a list of registered merchants, or through other automated technologies that permit a cardholder to quickly confirm the validity of a merchant. It should be noted that while the above measures will help confirm merchant validity, these measures are not expected to provide absolute assurance.

7. Cardholder Verification Methods

Depending on the MasterCard payment product or the country of the transaction, there are two types of cardholder verification methods (CVM): personal identification number (PIN) and signature.

In certain transaction scenarios, a CVM may not be required. For example, in the processing of quick payment services (QPS) transactions and contactless transactions below the MasterCard contactless chargeback protection amount or Maestro contactless ceiling limit, no signature or PIN is required.

7a. PIN CVM

The security of the cardholder's PIN is critical for preventing fraud, and therefore PIN entry must only be conducted on PIN-entry terminals that are certified as compliant with the *Payment Card Industry PIN Transaction Security (PCI PTS)* requirements. In accordance with MasterCard standards, the PCI requirements need to be met for PIN entry.

EMV offers various options for PIN verification, including online, offline plaintext, and enciphered PIN. For contactless transactions, offline PIN is not supported. With the growth of mobile as a cardholder device, however, an additional option is now available: on-device cardholder verification. For additional information, consult the *PayPass–M/Chip Reader Card Application Interface Specification v3.0, also available as EMV Kernel C-2*. These documents can be found at www.mastercard.com/contactless and www.emvco.com, respectively.

To be clear, cardholder PINs must never be entered into the merchant's mobile device unless the mobile device can be certified to the PCI PTS.

As a reminder: POS terminals must support offline PIN (both plaintext and enciphered offline PIN) and online PIN.

UNIQUE CHALLENGE

Currently, the keypads or touch screens on mobile devices are not capable of complying with the PCI PTS requirements. In the future, mobile device manufacturers intend to use technologies that can better secure the keypad, but these technologies are still in the early stages of development. It is not yet known if mobile device keypads will ever be appropriate for PIN capture.

BEST PRACTICES FOR MOBILE POS SOLUTION PROVIDERS

When considering the development of a PIN-capable Mobile POS solution, ensure that compliance with the PCI PTS requirements can be achieved.

BEST PRACTICES FOR MERCHANTS

Merchants must not capture cardholder PINs on their mobile devices or any other device that is not PCI PTS compliant. Merchants interested in PIN acceptance should consult their acquirers or Mobile POS solution providers and consider Mobile POS sleeves and other external devices that are certified to the PCI PTS standard.

7b. SIGNATURE CVM

The capture of a cardholder signature is important to ensure that merchants have second presentment chargeback rights.

UNIQUE CHALLENGE

Various commercially deployed Mobile POS solutions capture the cardholder's signature via the touch screen on the mobile device. However, the capture of a signature in certain mobile devices may not be possible.

BEST PRACTICES FOR MOBILE POS SOLUTION PROVIDERS

Mobile POS solutions that use a mobile device with a touch screen for signature capture should ensure that the signature panel displays pertinent transaction information, including the merchant name and the transaction amount in the original transaction currency. There should be adequate space provided for the cardholder's signature.

BEST PRACTICES FOR MERCHANTS

If the Mobile POS solution is not capable of capturing an electronic signature, the merchant should capture the signature on a handwritten paper receipt to retain second presentment chargeback rights.

8. Receipts

All receipts, whether printed, digital, or handwritten, must comply with MasterCard standards (located at www.mastercardmerchant.com) and satisfy the requirements of all applicable local laws.

UNIQUE CHALLENGE

Merchants who use Mobile POS solutions must have the ability to provide cardholders with a receipt; however, most Mobile POS solutions do not have the capability to print a receipt. Some of the more sophisticated Mobile POS solutions might have access to an external printer via a Bluetooth connection; however, this adds to the cost and complexity of the Mobile POS solution.

BEST PRACTICES FOR MOBILE POS SOLUTION PROVIDERS

The Mobile POS solution should be able to send receipts via email and/or text message. The content of the email or text message receipt must conform to the receipt requirements as described in MasterCard standards. As a reminder, MasterCard requires retailers to truncate the PAN on printed, handwritten, or digital receipts. PAN truncation blocks out all but the last four digits of an account number (for example, XXXX-XXXX-XXXX-1234). Each receipt must clearly identify the transaction as a retail sale, credit, or cash disbursement. Refer to the Sample Receipt image at right to see the information that must be included on the receipt.

The receipt must not reflect:

- The PIN, any part of the PIN, or any fill characters representing the PIN
- The Card Validation Code (CVC 2)
- Expiration date

BEST PRACTICES FOR MERCHANTS

It is acceptable to provide a receipt via email or text message only if the cardholder consents to receive electronic disclosure. Merchants should be mindful of consumer privacy and associated laws and regulations regarding data privacy, and only use a cardholder's email address or mobile phone number for the specific purpose of providing the cardholder with a receipt for each individual transaction. In instances where email or text messaging is not an option, merchants should be prepared to provide a handwritten receipt that conforms to all of the sales receipt requirements described in MasterCard standards.

For additional information about MasterCard Mobile Point-of-Sale Best Practices, please contact mobilepos@mastercard.com

Sample Receipt

Merchant Name

Doing Business As
Merchant Address
Date and Time

A description and the price of each product and service purchased, including applicable taxes, in detail sufficient to identify the transaction

SALE

Card no. XXXX-XXXX-XXXX-1234
Card Type: MasterCard

Base Amount (CUR): ____
Tip (CUR) optional: ____
Total Amount (CUR): ____

All authorization numbers must be entered on the receipt (except on credit receipts)
****Customer Receipt****

GLOSSARY OF TERMS

These terms are to be used solely for this document

Acquirer
A member who maintains the merchant relationship and acquires the data relating to a transaction from the merchant or card acceptor.

Cardholder Verification Method (CVM)
A system or technology used to verify the authenticity of the cardholder. Examples include signature, personal identification number (PIN), a chip (integrated circuit), Universal Cardholder Authentication Field™ (UCAF), and biometrics methodologies.

EMV Chip Card
A credit or debit card containing a computer chip with memory and interactive capabilities, used to identify and store additional data about the cardholder, cardholder account, or both. Also called an integrated circuit card. Previously referred to as a smart card.

EMV Specifications
A global standard established by EMVCo LLC for credit and debit payment cards based on chip card technology. EMVCo LLC was formed in 1999 by Europay, MasterCard, and Visa to manage, maintain, and enhance the EMV® Integrated Circuit Card Specifications for Payment Systems. Go to www.emvco.com to obtain the latest version available.

EMVCo LLC
An organization formed in February 1999 by Europay, MasterCard, and Visa to manage, maintain, and enhance the EMV® Integrated Circuit Card Specifications for Payment Systems. With the acquisition of Europay by MasterCard in 2002, JCB joined the organization in 2004, and American Express became its fourth member in 2009.

EMVCo is currently operated by American Express, JCB, MasterCard, and Visa. EMVCo's primary role is to ensure interoperability and acceptance of payment system integrated circuit cards on a worldwide basis. EMVCo also maintains type approval processes for terminal compliance testing and common core definitions and common payment application card compliance testing. These testing processes ensure that a single terminal and card approval process is developed at a level that will allow cross-payment system interoperability through compliance with the EMV specifications. Go to www.emvco.com for more information.

Feature Phone
A mobile phone that at the time of manufacture is not considered to be a smartphone, but nevertheless has additional functions over and above standard mobile services. It addresses the market for customers who don't want the features of smartphones, and also typically allows a lower price point.

Integrated Contactless Mobile POS Solution
A Mobile POS solution that performs contactless transactions via a near field communications (NFC) antenna embedded within the mobile device.

MasterCard Acceptance Mark
MasterCard has established and enforced a common set of standards to ensure consistent, efficient, and secure use of its payment card network. MasterCard offers a wide range of payment solutions through the MasterCard brand, and the MasterCard acceptance mark ensures consistency at the point of sale and online. Merchants use the acceptance marks to help cardholders understand where MasterCard products are accepted.

Merchant
A commercial entity or person that, pursuant to a Merchant Agreement, is authorized to accept cards when properly presented.

Mobile Device
Consumer-oriented, multi-purpose, mobile computing platforms including feature phones, smartphones, tablets, and PDAs.

Mobile Contactless (NFC)
Contactless payment integrated into the mobile phone.

Mobile Point of Sale (Mobile POS)
A point-of-sale terminal that makes use of a mobile device.

Mobile POS Card Reader Accessory
Typically inexpensive and easy to deploy, Mobile POS card reader accessories attach to the audio port, USB port, or proprietary connector on mobile devices. They may also connect via Bluetooth to the mobile device. These accessories provide for magnetic stripe, EMV chip card, and contactless acceptance, and are sometimes referred to as "dongles."

Mobile POS Solution
A product or offering that uses mobile devices, payment application software, or card reader accessories to facilitate the acceptance of MasterCard transactions.

Mobile POS Solution Provider
A vendor that offers Mobile POS solutions to MasterCard merchants. Mobile POS solution providers may be MasterCard acquirers or independent vendors.

Near Field Communications (NFC)
Based on existing radio-frequency identification (RFID) standards such as ISO14443, NFC standards cover communications protocols and data exchange formats.

Payment Card Industry PIN Transaction Security (PCI PTS)
The *Payment Card Industry PIN Transaction Security (PCI PTS)* requirements are used primarily by ATM and point-of-sale equipment manufacturers to secure cardholder data at the physical point of interaction.

Payment Card Industry Security Standards Council (PCI SSC)
The governing organization and open forum responsible for the development, management, education, and awareness of PCI Security Standards, including the *Data Security Standard* (PCI DSS), the *Payment Application Data Security Standard* (PA DSS), and *PIN Transaction Security* (PCI PTS) *Standard*, among others. Additional information on PCI security can be found at www.mastercard.com/pci360 or www.pcisecuritystandardscouncil.org.

Payment Facilitator
A merchant registered by an acquirer to facilitate transactions on behalf of sub-merchants.

Personal Identification Number (PIN)
A four- to 12-character alphanumeric code that enables an issuer to authenticate the cardholder to approve an ATM or terminal transaction occurring at a point-of-interaction (POI) device.

Point-to-Point Encryption (P2PE)
A method or protocol for encrypting data so it can be transmitted securely between two points.

POS Terminal
An attended or unattended device located in or at a merchant's premises or otherwise used by or on behalf of a merchant to facilitate a transaction.

Primary Account Number (PAN)
The number that is embossed, encoded, or both, on a MasterCard® card to identify the issuer and the particular cardholder account. The PAN consists of a major industry identifier, issuer identifier, individual account identifier, and check digit.

Smartphone
A mobile phone built on a mobile computing platform with more advanced computing ability and connectivity than a feature phone.

Sub-Merchant
A merchant that has an agreement with a payment facilitator and is authorized to accept cards when properly presented.

Tablet
A tablet computer, or a tablet, is a mobile computer that's larger than a mobile phone or personal digital assistant, has an integrated, flat touch screen, and is primarily operated by touching the screen rather than using a physical keyboard.