MOBILE PAYMENT ACCEPTANCE SOLUTIONS

VISA

VISA SECURITY BEST PRACTICES
VERSION 3.0

Visa Security Best Practices for Mobile Payment Acceptance Solutions, Version 3.0

Since Visa's first release of this best practices document in 2011, we have seen a rapid increase in mobile acceptance deployments around the world. Visa is publishing an updated version of this document as we continue to identify best practices to safeguard cardholder and account data when using mobile acceptance solutions.

Visa is always looking for ways to accelerate the introduction of innovative payment solutions around the world while maintaining trust and security. During the Mobile World Congress 2013, Visa announced the launch of the Visa Ready Program. In this version of the best practices, Visa recommends participation in the Visa Ready Program.

The Visa Ready Program paves the way for non-traditional payment partners, such as mobile device manufacturers, technology partners, wallet providers, and mobile network operators to easily navigate the complexities of the payments ecosystem more effectively. The program provides innovators a path for the certification of devices, software and solutions used to initiate or accept Visa payments, as well as guidance and best practices to access the power of the Visa network. With the Visa Ready Program symbol, acquirers and merchants will be able to identify solution providers that meet the applicable requirements.

Scope

This document applies to the providers of mobile acceptance solutions acquirers and their payment service providers (PSPs), as well as merchants that use these solutions to accept Visa payments.

A PSP, commonly called a "master merchant" or "payment facilitator," is an entity that contracts with an acquirer to provide payment-related services to sponsored merchants. Some mobile acceptance solution providers (hereafter referred to as "vendors") are PSPs that sell their solutions directly to merchants, whereas others only provide their platforms as white label solutions for acquirers or PSPs to be the ones to market solutions to merchants. Acquirers, PSPs and solution providers should review the "Best Practices for Acquirers & Payment Service Providers (PSPs)" section of this document for applicable best practices.

Visa's definition of a merchant or sponsored merchant is any person that enters into an agreement with an acquirer or PSP for the acceptance of Visa cards for purposes of originating payment transactions under any Visa marks.

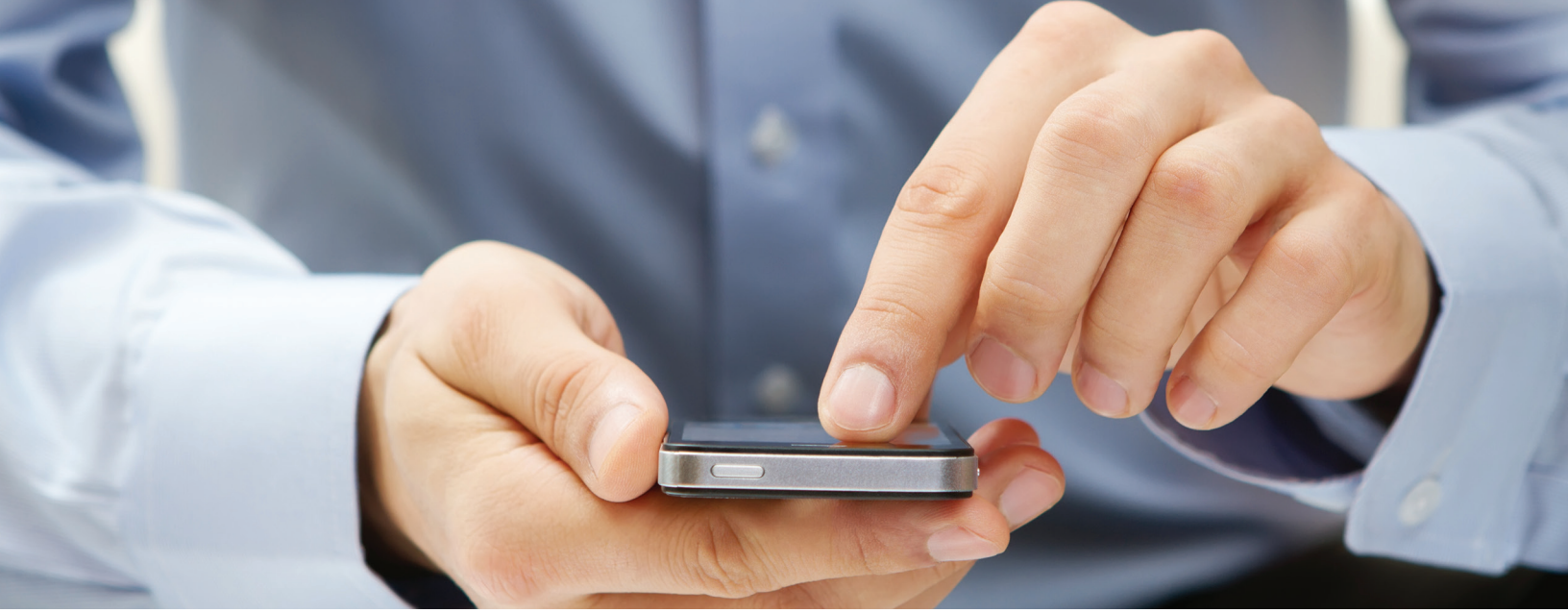
Beyond these best practices, solution providers, merchants and acquirers must follow all Visa requirements for magnetic stripe, chip and contactless acceptance (where supported). The mobile payment solution should also adhere to the principles set out in the Payment Card Industry Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), PIN Transaction Security Standard (PCI-PTS) and the PCI Point-to-Point Encryption Standard. Because the industry is moving towards chip globally, Visa also encourages solution providers to establish and implement their own EMV roadmap in the near future.

Acquirers and PSPs must continue to follow the requirements outlined in the *Visa International Operating Regulations* and adopt the guidelines established in other related ancillary documents. In particular, acquirers and PSPs must adhere to Visa Operating Regulations due diligence requirements when onboarding and monitoring their merchants, and they must be in compliance with all local laws and regulations regarding merchants, including adequate Know Your Customer (KYC) and anti-money laundering due diligence requirements.

Definitions

Consumer Mobile Device: Any consumer electronic handheld device (e.g., smart phone, tablet or PDA) that is **not** solely designed for payment acceptance and has the ability to wirelessly communicate account data (via GSM, GPRS, CDMA, etc.) for transaction processing.

Mobile Payment Acceptance Solution: This consists of a (i) mobile payment application; (ii) consumer mobile device; and (iii) hardware accessory capable of reading account data if account data is electronically read from a payment card. Solutions that do not electronically read account data may not be permitted by Visa in all territories or may be subject to certain restrictions. Solution providers **must** review local Visa Operating Regulations before providing mobile payment acceptance solutions to Visa-accepting merchants.



Best Practices for Mobile Payment Acceptance Solution Vendors

SECURITY GOALS

1	Design and implement secure Mobile Payment Acceptance Solutions
2	Ensure the secure use of Mobile Payment Acceptance Solutions
3	Limit exposure of account data that could be used to commit fraud

GOAL	BEST PRACTICES
Design and implement secure Mobile Payment Acceptance Solutions	1. **Provide payment acceptance applications and any associated updates with a known chain of trust.** A vendor should be able to provide assurance that the code within a payment application has not been tampered with or altered without authorization. 2. **Obtain Visa Ready certification.** The Visa Ready Program enables mobile POS (mPOS) providers to quickly bring compliant solutions to market by defining mPOS requirements. The program defines device, application and processing requirements for device manufacturers, software developers, merchants and acquirers to participate in the Visa Ready Program. Non-traditional payment partners, such as mobile device manufacturers, technology partners, wallet providers, and mobile network operators, can easily understand Visa's requirements and have a clear path for the certification of devices. The Visa Ready Program also makes it easier for financial institutions and merchants to adopt new, innovative payment methods that are fully approved by Visa and to help them drive growth by expanding the use and acceptance of electronic payments globally. The program provides a list of mPOS solutions that comply with best practices and mandatory requirements and therefore makes it easier for institutions to select compliant solutions. In order to access the Visa Ready Program requirements, please register on the Visa Ready Program for mPOS page at www.visa.com. 3. **Validate against PA-DSS standards.** Validating the mobile application against PA-DSS requirements will ensure that the application is developed according to software development best practices. Validation of an application against PA-DSS is highly recommended. For the Visa Ready Program, PA-DSS validation is mandatory if the payment application accepts manual key entry of the 16-digit Primary Account Number (PAN).

GOAL	BEST PRACTICES
Ensure the secure use of Mobile Payment Acceptance Solutions	4. **Provide the ability to disable the Mobile Payment Acceptance Solution.** As a security precaution, the entity processing transactions on behalf of the merchant should be able to disable payment acceptance. For example, if a device were lost or stolen, the Mobile Payment Acceptance Solution should be disabled. 5. **Provide the ability to limit access to the Mobile Payment Acceptance Solution.** Ensure that only authorized users have physical/logical access to the payment functionality of the solution by providing the ability to lock the mobile acceptance solution interface on the Consumer Mobile Device with a passcode, password or security pattern when the device is not in use. The mobile acceptance app should be configurable to auto-lock after several minutes of inactivity. If permitted by the mobile acceptance application, each user should have a unique passcode to access the payment application. 6. **Provide the ability to track use and key activities within the Mobile Payment Acceptance Solution.** Event logs captured by the Mobile Payment Acceptance Solution should automatically be transferred to a centralized back-end system where they can be analyzed for unusual or suspicious activity. Also, consider analyzing information that originates from the Consumer Mobile Device such as the device ID or geo-location, where available to supplement fraud detection engines.
Limit exposure of account data that could be used to commit fraud	7. **Provide the ability to encrypt all public transmission of account data.** To maintain confidentiality and the integrity of account data, it must be encrypted during transmission over wireless and/or public networks. All account data that originates from a Mobile Payment Acceptance Solution and is sent to any other termination point must be encrypted in accordance with industry-accepted encryption standards using industry-accepted algorithms and appropriate key sizes. 8. **Ensure that account data electronically read from a payment card is protected against fraudulent capture and use by unauthorized applications in a Consumer Mobile Device.** Visa recognizes encryption at the electronic reader (e.g., card reader or a PIN entry device) as a mature technology to meet this best practice. This is especially important when a merchant has limited or no direct control over the security of the environment in which the Consumer Mobile Device is deployed. 9. **Provide the ability to truncate or tokenize the PAN after authorization to facilitate cardholder identification by the merchant.** For more information, refer to *Visa Best Practices for Tokenization* and *Visa Best Practices for Primary Account Number Storage and Truncation*. For more details on these topics, go to the Data Security News & Resources page at www.visa.com.

GOAL	BEST PRACTICES
Limit exposure of account data that could be used to commit fraud [continued]	10. Protect stored PAN data and/or sensitive authentication data. If a Consumer Mobile Device is temporarily unable to transmit account data to the acquirer, solution provider or PSP due to a poor network connection or other reasons, account data must be encrypted or otherwise protected until it can be securely sent to the acquirer or PSP. Any PANs that are retained after authorization (e.g., in logs), must be truncated or tokenized (refer to best practice No. 9). After authorization, sensitive authentication data must be deleted from the merchant acceptance solution (even if encrypted). The solution should not include any debug functionality that might allow unauthorized access to account data by the merchant or others. Any other personal information and/or personally identifiable information captured either as a part or a consequence of the payment process must be protected in accordance with any applicable local/regional laws, government regulations or other legal requirements. 11. Provide security for Account on File Systems. In select mobile acceptance solutions, account data may be captured and retained in a central system where this retained data can subsequently be used to authorize new transactions. In some cases, a cardholder can make payments using the data stored on a central system through the use of credentials such as a password or tokens such as QR (quick response) codes to pay at the point of sale. When registering new card details, the solution should include steps to establish the legitimacy of the enrolling card/cardholder. The registration process should include the use of Verified by Visa and address verification checks; but the process should not be performed on the merchant's Consumer Mobile Device. When accepting payments, the solution should clearly provide a means to capture the cardholder's intent to make a payment for a specific amount. Tokens should be time bound and revocable. If possible, the solution vendor should take steps to limit the value of the stolen tokens. For example, a parking garage token could be linked to the license plate of the cardholder's registered vehicle. The process of registering additional benefactors for tokens should be similar to registering new card details with the solution. For account-on-file solutions, the CVV2 must never be retained after initial authorization. When making account on file based payments, solutions vendors should consider subscribing to Visa Account Updater (if the vendor's operating market supports the solution) to avoid disruptions in customer relationships due to Visa account information changes.

Best Practices for Merchants

SECURITY GOALS

1	Ensure the secure use of Mobile Payment Acceptance Solutions
2	Limit the exposure of account data that may be used to commit fraud
3	Prevent software attacks on Consumer Mobile Devices

GOAL	BEST PRACTICES
Ensure the secure use of Mobile Payment Acceptance Solutions	1. **Only use Mobile Payment Acceptance Solutions as originally intended by an acquiring bank and solution provider.** To prevent unintended consequences from the misuse of a mobile acceptance solution, ensure that the solution is used in a manner consistent with the guidance provided by an acquiring bank, PSP or solution provider, and that any software downloaded onto the Consumer Mobile Device comes from a trusted source.
Limit the exposure of account data that may be used to commit fraud	2. **Limit access to the Mobile Payment Acceptance Solution.** Ensure that only authorized users (i.e., designated employees) have physical/logical access to the payment functionality of the solution. Merchants are encouraged to use a passcode, password or security pattern to lock their Consumer Mobile Device when not in use. The Consumer Mobile Device should be configured to auto-lock after a number of minutes of inactivity. If permitted by the mobile acceptance application, each user should have a unique passcode to access the payment application. 3. **Immediately report the loss or theft of a Consumer Mobile Device and/or hardware accessory.** Contact the acquiring bank or PSP immediately to report the loss or theft of a Consumer Mobile Device and/or hardware accessory to help ensure the prompt implementation of any necessary actions. For more recommendations, refer to Visa *What To Do If Compromised—Visa Inc. Fraud Control and Investigations Procedures, Version 3.0.* This guide is intended for Visa clients (i.e., acquirers and issuers), merchants, agents and third-party service providers. It includes step-by-step instructions on how to respond to a security incident and specific time frames for the delivery of information or reports outlining actions taken by Visa, its clients and agents. 4. **Safeguard the cardholder signature.** If the mobile application requires the cardholders to sign in to the mobile screen, the signature should be protected in the same manner as a PAN, which is outlined by the PCI-DSS standard.
Prevent software attacks on Consumer Mobile Devices	5. **Install software only from trusted sources.** Merchants should not circumvent any security measures on the Consumer Mobile Device. To avoid introducing a new attack vector onto a Consumer Mobile Device, install only trusted software that is necessary to support business operations and to facilitate payment. 6. **Protect the Consumer Mobile Device from malware.** Establish sufficient security controls to protect a Consumer Mobile Device from malware and other software threats. For example, install and regularly update the latest anti-malware software (if available). Merchants should also regularly update the firmware of their device and install any application updates whenever a new update becomes available. Merchants that deliberately choose to subvert the native security controls of a Consumer Mobile Device by "jailbreaking" or "rooting" the device increase the risk of malware infection.

Best Practices for Acquirers & Payment Service Providers (PSPs)

SECURITY GOALS

1	Design and deploy robust Mobile Payment Acceptance Solutions
2	Design and implement appropriate controls when onboarding merchants
3	Ensure proper monitoring of Mobile Payment Acceptance Solutions

GOAL	BEST PRACTICES
Design and deploy robust Mobile Payment Acceptance Solutions	1. **Provide the ability to uniquely identify a transaction coming from a merchant.** The acquirer or payment service provider should be able to uniquely identify the Consumer Mobile Device, mobile terminal and/or mobile acceptance application. Among other benefits, this will allow recognition of unique fraud patterns emerging from Mobile Payment Acceptance Solutions used to accept payments. 2. **Restrict manual PAN Key Entered transactions on a Consumer Mobile Device to a minimum.** Key-entered transactions should never be used as a primary means of capturing account data. In the event of chargebacks or refunds, the acquirer or PSP should provide a means that allows for the chargeback or refund to be processed without requiring the input/display of a full PAN. 3. **Deploy Visa Ready certified solutions.** Participating labs will validate mPOS solutions for compliance with the Visa Ready Program requirements. After successful lab testing of the solution and execution of the Visa Ready Program for mPOS agreement, Visa will add details of the approved offering to its directory of Visa Ready Program mPOS solutions. In addition, Visa will provide access to the Visa Ready Program symbol and other associated program collateral.
Design and implement appropriate controls when onboarding merchants	4. **Ensure appropriate due diligence when onboarding and monitoring merchants including adequate KYC and anti-money laundering procedures.** Acquirers and PSPs must be in compliance with all local laws and regulations regarding merchants, including adequate Know Your Customer and anti-money laundering due diligence requirements. The PSP interfaces with the acquirer on behalf of its sponsored merchants, and must ensure that its sponsored merchants are contractually obligated to operate according to Visa requirements. These obligations include, but are not limited to: • A sponsored merchant (seller) contracts with a PSP to obtain payment services. PSPs are responsible for their sponsored merchants, bear financial liability for their actions and must ensure that the sponsored merchants operate according to Visa rules and requirements. • Acquirers must thoroughly vet and monitor the actions of each PSP and their sponsored merchants. In addition, acquirers are responsible for all merchant agreement requirements as specified in the *Visa International Operating Regulations*. Acquirers are responsible for the actions of their PSPs and the PSP-sponsored merchants. • PSPs must be registered with Visa. An acquirer must send registration forms and supporting documents as specified by Visa to confirm that it has performed comprehensive due diligence and financial review of the PSP. • PSPs must encode a short code in the merchant descriptor field.

GOAL	BEST PRACTICES
Design and implement appropriate controls when onboarding merchants [continued]	PSPs should also ensure that: • All merchants are reported in the Visa system using a Merchant Category Code (MCC) representing the goods or services they are selling. Only when a merchant is selling different types of goods or services over time (e.g., garage sale, etc.) should the MCC 7299—Miscellaneous Personal Services) be used. 5. **Ensure risks can be easily managed when deploying solutions to merchants.** If an acquirer or PSP is new to mPOS solutions or to a certain market, they should deploy solutions in a manner that will not expose them to excessive risk. For example, consider initially deploying only to established merchants or merchants the PSP or acquirer considers trustworthy.
Ensure proper monitoring of Mobile Payment Acceptance Solutions	6. **Where network connectivity is available, ensure that all authorizations are processed online.** Online processing provides the ability to monitor transactions and detect fraud. It reduces the exposure that a business may have to fraudulent transactions through use of the most up-to-date fraud monitoring system and thereby helps to reduce the possibility of fraudulent transactions. Also, online processing allows for other value-added services such as couponing. 7. **Develop fraud monitoring capability specifically for mobile payment acceptance.** Acquirers currently connected to Visa will be required to submit a new value that identifies transactions originated by a merchant mPOS acceptance device. Acquirers will submit the value "9" in Field 60.1—Terminal Type in BASE I and VisaNet Integrated Payment (V.I.P.) System POS messages. This value can be used to specifically identify mPOS transactions. An acquirer or payment service provider should also have the capability to identify unique fraud patterns for mobile payment acceptance. Examples of patterns unique to mobile payment acceptance include, but are not limited to: • Geo-location can be used to supplement existing fraud detection systems whereby action can be taken if, for example, two transactions come through for authorization from physically disparate locations where it is not physically possible to travel between these locations within the time period in which the authorization requests arrived or where the acceptance device is found to operating outside of an agreed geographic boundary. • Implement velocity tracking capabilities in the terminal management system. This may be defined by individual merchant locations, merchant or merchant category level. • Monitor settlement of funds and hold funds if a merchant's risk profile has not been defined. A quick response to a fraud incident or identified fraud patterns, in the form of application updates or otherwise, is critical to ensuring that the Mobile Payment Acceptance Solution maintains security.

Best Practices Feedback

To provide feedback or comments on these best practices, e-mail InfoRisk@visa.com with "Mobile Payment Acceptance Best Practices" in the subject line.