Life flows better with Visa

VISA

Visa Europe Security Best Practices

Mobile Payment Acceptance Solutions

Version 2.0
September 2012

Contents

About this guide

Last year, Visa released the first version of this document. It provided guidance around technical and procedural controls to help limit a fraudster's ability to steal sensitive cardholder and account data from Mobile Payment Acceptance Solutions. Over the past year, mobile acceptance has seen tremendous growth globally. Vendors throughout the world are developing new and innovative solutions to help grow acceptance for merchants and provide alternatives to consumers. Visa has remained vigilant in identifying additional controls that can help further protect cardholder and account data when using Mobile Payment Acceptance Solutions.

In our continued commitment to help promote the security and integrity of the payment system, Visa is enhancing its current best practices to provide additional guidance to solution vendors, merchants and acquirers using Mobile Payment Acceptance Solutions.

Scope

The previous version of the best practices was intended for two distinct audiences: vendors that develop Mobile Payment Acceptance Solutions and merchants that use these solutions. For purposes of this document, a vendor is any entity that develops Mobile Payment Acceptance Solutions, either in-house or on behalf of another organization. In this newer version, there is a third audience: Acquirers and Payment Service Providers (PSP). In the context of mobile acceptance, a Payment Service Provider (PSP), commonly called a "Master Merchant," is an entity that contracts with an acquirer to provide payment-related services to sponsored merchants. PSPs and solution vendors should review the new PSP section for applicable best practices.

Beyond these best practices, vendors, 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) and Payment Application Data Security Standard (PA-DSS). As the industry is moving towards chip globally, Visa also encourages solution providers to establish and implement an EMV roadmap in the near future.

Acquirers and PSPs should contact Visa Europe directly for further guidance around Visa's policies on mobile acceptance. In addition, acquirers and PSPs should adhere to due diligence requirements when boarding 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 (AML) due diligence requirements.

Definitions

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

Mobile Payment Acceptance Solution: Consists of mobile payment application, a Consumer Mobile Device and, where account data is electronically read from a payment card, a hardware accessory capable of reading account data. Solutions that do not electronically read account data may not be acceptable in all territories or may be subject to restrictions. Solution providers **must** review local Visa Operating Regulations prior to 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 in a secure manner 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. Develop mobile payment acceptance applications based on secure coding guidelines.** Poor software security coding practices can introduce vulnerabilities and expose customers to the risk of account data compromise. A vendor should be able to demonstrate the following: • The vendor should put in place and conduct security development/ maintenance measures. i. iThese security measures should be documented. The vendor's developers should be trained in these measures and their output monitored to ensure it conforms to these measures. ii. These security measures should ensure timely detection of vulnerabilities that apply to the device by periodic execution of a vulnerability assessment that includes activities such as: analysis, code review, survey of vulnerability information available in the public domain, and testing. At an absolute minimum, the vendor must take steps to mitigate the vulnerabilities found in the CWE/SANS top 25 Most Dangerous Software Errors. iii. These security measures should ensure timely assessment and classification of newly found vulnerabilities. iv. These security measures should ensure timely creation of mitigation measures for newly found vulnerabilities that may impact platform security. • Where deployed platforms can be updated, the vendor should maintain security guidance describing how the update mechanism has to be used. i. The update mechanism should ensure confidentiality, integrity, server authentication and protection against replay by using an appropriate security protocol. If the device allows software and/or configuration

Goal	Best Practices
	updates, the device authenticates the update and if the authenticity is not confirmed, the update is rejected and deleted. ii. The platform vendor should put the security guidance for updating deployed applications at the disposal of application builders, system integrators and end-users of the solution. iii. The security guidance should cover at a minimum the process for updating applications, certificates and keys. iv. The security guidance should describe the responsibilities of application developers, system integrators and end-users of the platform. v. The security guidance should ensure that deployed updates are timely. • Where possible, the application should perform tests to check for signs of privilege escalation by the end user or malware such as jail-breaking or rooting the mobile device. The solution vendor/operator of the solution in turn should establish a risk policy for dealing with these types of devices. • The vendor must assume that shared storage on the Consumer Mobile Device is untrusted and take steps to ensure that information does not leak between applications. **3. Protect encryption keys that secure account data against disclosure and misuse in accordance with industry-accepted standards.** To keep cryptographic keys secure, robust key management standards should be followed. Symmetric and private keys should be protected against physical and logical compromise. Public keys should be protected from substitution, and their integrity and authenticity should be ensured. Any cryptographic implementation must make use of industry-accepted algorithms and appropriate key sizes, and, at a minimum, must be consistent with the key management principles described in the following: • PCI PIN and PCI PIN Transaction Security (PTS) • PCI Point-to-Point Encryption (P2PE) • Payment Application Data Security Standards (PA-DSS) key management procedures **4. Permitted solutions: The following Mobile Payment Acceptance Solutions are permitted within the Visa Europe territory:** 1. Mobile POS solutions consisting of a Consumer Mobile Device used together with a separate hardware accessory to accept a payment transaction, which is securely transmitted to an acquirer or service provider using a payment gateway. The permitted solutions must use a hardware accessory to capture cardholder data electronically and must support EMV chip, magnetic stripe and PIN. Support of proximity payment is optional but recommended. The hardware accessory must be PCI PTS certified including the additional

Goal	Best Practices
	SRED module. The acquirer's or service provider's gateway must be PCI DSS certified and support point-to-point encryption. 2. Mobile Commerce solutions where the cardholder enters payment details on his/her own mobile device, or they are on file and never seen by the mobile device owned/operated by the merchant. Any merchant m-commerce site or account-on-file solution must be compliant with PCI DSS.
Ensure the secure use of Mobile Payment Acceptance Solutions	**5. 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. **6. Provide functionality 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 integrity, account data must be encrypted during transmission over wireless and/or public networks. All account data originating from a Mobile Payment Acceptance Solution sent to any other termination point must be encrypted in accordance with industry-accepted encryption standards using industry-accepted algorithms and appropriate key sizes. Hardware accessories must be PCI PTS-SRED certified (PCI PTS is not sufficient). The overall solution, in addition to be compliant with PCI DSS, must also be maintained in a manner consistent with PCI SSC's point-to-point encryption requirements. **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 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.

Goal	Best Practices
	9. Ensure chip acceptance devices are implemented correctly When accepting EMV chip transactions, the device must (1) have a valid and current EMV type approval, (2) have passed the Visa Acquirer Device Validation Toolkit (ADVT) for EMV contact, and (3) for certain regions, where contactless technology is used, have passed the Visa payWave Test Tool (VpTT) or Contactless Device Evaluation Toolkit (CDET). **10. Provide the ability to truncate or tokenize the Primary Account Number (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. **11. Protect stored PAN data and/or sensitive authentication data.** If a Consumer Mobile Device is temporarily unable to transmit account data to the acquirer or PSP (for example, due to a poor network connection), 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 number 9, above). 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. Any other personal information and/or personally identifiable information captured either as part of, or as a consequence of, the payment process must be protected in accordance with any applicable local/regional laws, government regulations, or other legal requirements. **12. 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. With some services, 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. In registering new card details, the solution should take steps to establish the legitimacy of the enrolling card/cardholder. If available, Verified by Visa and address verification checks should be performed as part of the registration process. The registration process should not occur 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.

Goal	Best Practices
	Where tokens are used, tokens should be time-bounded and be revocable. Where possible, the solution vendor should take steps to limit the value of the stolen tokens to fraudulent users. For example, in a parking garage the token could be bound to the cardholder's registered vehicle license plate. The registration of additional benefactors should follow a similar process to that of registering new card details with the solution. For account on file solutions, CVV2 must never be retained after initial authorization. To avoid disruption in customer relationships due to Visa account information changes, when making account on file based payments, solutions vendors should consider subscribing to Visa Account Updater (VAU) if the vendor's operating market supports the solution.

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 and solution provider. This includes ensuring 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. **3. Immediately report the loss or theft of a Consumer Mobile Device and/or hardware accessory.** Contact the acquiring bank 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. Please consult Visa's guide on What To Do If Compromised for further instruction. This guide is intended for Visa clients (i.e., acquirers and issuers), merchants, agents, and third-party service providers. It contains step-by-step instructions on how to respond to a security incident and provides specific time frames for the delivery of information or reports outlining actions taken by Visa, its clients, and its agents.
Prevent software attacks on Consumer Mobile Devices	**4. 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.

Goal	Best Practices
	5. 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 regularly update the firmware of their device and install any application updates whenever a new update becomes available. Merchants who choose to deliberately 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 on-boarding 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. Treatment of Cardholder Data** The following solutions are not permitted: solutions where cardholder data is entered onto an application residing on a mobile device owned and/or operated by the merchant (either key entered or electronically captured) to then be processed either as a face to face transaction with key entry, e-commerce transaction or mail order/telephone order transaction.
Design and Implement appropriate controls when on-boarding merchants	**3. Ensure appropriate due-diligence when on-boarding and monitoring merchants including adequate Know Your Customer (KYC) and Anti-Money Laundering (AML) procedures** Acquirer and Payment Service Providers must be in compliance with all local laws and regulations regarding merchants, including adequate Know Your Customer (KYC) and Anti-Money Laundering (AML) 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 Visa Europe's Operating Regulations. Acquirers are responsible for the actions of their PSPs and the PSPs' sponsored merchants.

Goal	Best Practices
	• 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
Ensure proper monitoring of Mobile Payment Acceptance Solutions	**4. 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 reducing the possibility of fraudulent transactions. Also, online processing easily allows for other value add services such as couponing. **5. Develop fraud monitoring capability specifically for mobile payment acceptance** An acquirer or payment service provider should 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. 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

As a leader in the payments industry, Visa has developed this version of these best practices to support the growth of the emerging mobile acceptance channel. As such, Visa welcomes any feedback on these best practices. To provide feedback or comments on these best practices, send an e-mail to datasecuritystandards@visa.com with "Mobile Payment Acceptance Best Practices" in the subject line.