Visa Best Practices for Mobile Payment Acceptance Solutions Version 1.0

The payment and mobile worlds are rapidly converging as merchants begin to use consumer mobile devices (such as smart phones and tablet computing platforms) to facilitate card payments both within and, increasingly, outside of the traditional retail environment.

As with any new acceptance mechanism, there are security considerations that need to be addressed prior to use. For example, as part of a mobile acceptance solution a consumer mobile device may be used to facilitate face-to-face customer payments; however, these mobile devices have limited native security controls. Additionally, merchants that use a consumer mobile device (or a similar device) as part of an acceptance solution may not have direct control of the security of the environment in which the device is used. Therefore, a mobile acceptance solution must include adequate supplementary technical and procedural controls to limit a fraudster's ability to steal sensitive account information.

To promote the security and integrity of the payment system, Visa is committed to helping mobile payment acceptance solution vendors, merchants and acquirers better understand their responsibility to keep account data secure when using mobile payment acceptance solutions.

Scope

These best practices are intended for two distinct audiences: vendors that develop mobile payment acceptance solutions and merchants that use these solutions. For the purposes of this document, a vendor is any entity that develops mobile payment acceptance solutions, either in-house or on behalf of another organization.

Beyond these best practices, vendors, merchants and acquirers must follow all Visa requirements for magnetic stripe, chip and contactless acceptance (where supported)[1]. 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).

Although not in the scope of this document, acquirers must follow the practices outlined in Visa Operating Regulations and adopt the guidelines established in other related ancillary documents. In particular, acquirers must adhere to Visa Operating Regulations due diligence requirements when on-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 face some restrictions. Clients must review local Visa Operating Regulations prior to providing mobile payment acceptance solutions to merchants.

---

[1] For EMV acceptance, the device must (1) have a valid and current type approval, (2) have passed the Visa Acquirer Device Validation Toolkit (ADVT) for EMV contact, and (3) where contactless technology is used, have passed the Visa payWave Test Tool (VpTT). For PIN-based transactions, a consumer mobile device is not acceptable for PIN entry. Instead, an additional hardware accessory that is PCI PTS approved and that functionally supports the Secure Reading and Exchange of Data (SRED) module must be used.

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 into the consumer mobile device and expose customers to the risk of data compromise. 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 included in the following: • PCI PIN and PCI PIN Transaction Security (PTS) • Payment Application Data Security Standards (PA-DSS) key management procedures
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 merchant mobile payment acceptance solution should be disabled. 5. **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.	6. **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 known algorithms and appropriate key sizes.

Goal	Best Practices
	7. Ensure that account data electronically read from a payment card is protected against fraudulent use by unauthorized applications in a consumer mobile device. Visa recommends encryption at the electronic reader (e.g., magnetic stripe 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. **8. 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*. **9. Protect stored PAN data and/or sensitive authentication data.** If a consumer mobile device is temporarily unable to transmit account data to the acquirer (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. Any PANs that are retained after authorization (e.g., in logs), must be truncated or tokenized (refer to best practice number 8, 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.

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 Practice
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. PANs required after authorization must be truncated or tokenized.
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 must have a valid agreement with the acquirer. Merchants may not process Visa transactions on behalf of other merchants. **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.
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. **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).

Best Practices Feedback

As a leader in the payments industry, Visa has developed the first 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 inforisk@visa.com with "Mobile Payment Acceptance Best Practices" in the subject line.