



NEWS RELEASE

Visa Europe Releases Mobile Acceptance Security Best Practices

Establishes security guidelines necessary for ensuring stakeholder trust in mobile acceptance solutions

Visa Europe in cooperation with Visa Inc. today issued a set of mobile acceptance security best practices for software and hardware providers, retailers and their acquirers. These best practices form part of Visa Europe's ongoing strategy to advance security measures to help protect cardholder and account data when using consumer mobile devices such as smart phones to facilitate the acceptance of card payments.

These best practices build upon Visa Europe's leadership in the areas of encryption and tokenisation technologies which can be used to both simplify and reduce the costs of implementing and maintaining a secure acceptance solution. Encryption and tokenisation technologies are designed to work hand-in-hand with EMV chip acceptance and have already proven to be suitable to different retail and payment processing environments.

Mobile technology is enabling a growing number of small and medium-sized retailers to accept payments using mobile devices. As retailers harness the power of mobile technology to accept payments and grow their businesses, the industry must also build in adequate controls and security measures to maintain stakeholder trust in electronic payments.

As mobile devices and acceptance attachments are not designed to the same security requirements as traditional payment terminals, and retailers do not currently control the security of the network environments to which their acceptance devices connect wirelessly, there are important security considerations above and beyond those for traditional payment acceptance solutions. These best practices are intended for two distinct audiences – mobile payment acceptance application and software/hardware solution providers as well as acquirers and retailers who use these solutions.

"By engaging with industry in issuance of these best practices, and leveraging existing Visa guidance, we can ensure that any mobile acceptance solution deployed is both secure and suitable from the outset," said Stanley Skoglund, Head of Payment Systems and Enterprise Risk, Visa Europe.

"EMV chip, widely adopted across Europe, has proven itself as a powerful technology that underpins Visa Europe's vision for securing all face-to-face transactions, and has directly contributed to our success in tackling fraud.

“Visa Europe will continue to deliver value to its more than 4,000 European member banks by moving to practical and cost-effective solutions that offer maximum protection both to retailers and cardholders.”

To promote the security and integrity of the payment system, Visa is committed to helping mobile payment acceptance providers, vendors, retailers and acquirers better understand their responsibility to keep account data secure when using mobile payment acceptance solutions with consumer devices such as smart phones.

For mobile payments to reach a critical mass, they must work everywhere, every time, with the same reliability of Visa payments today. For more than 50 years, Visa has set a high bar for robust security, privacy protections, and guaranteed payment to retailers and global acceptance ubiquity. Retailers, consumers and financial institutions should expect the same standards for mobile acceptance solutions.

A complete version of Visa’s Best Practices for Mobile Payment Acceptance Practices may be found online at www.visaeurope.com/ais. An abbreviated version is provided below.

Best Practices for Vendors:

Goal	Best Practice
Design and implement secure mobile payment acceptance solutions.	<ol style="list-style-type: none"> 1. Provide payment acceptance applications and any associated updates in a secure manner with a known chain of trust. 2. Develop mobile payment acceptance applications based on secure coding guidelines. 3. Protect encryption keys that secure account data against disclosure and misuse in accordance with industry-accepted standards.
Ensure the secure use of mobile payment acceptance solutions.	<ol style="list-style-type: none"> 4. Provide the ability to disable the mobile payment acceptance solution. 5. Provide functionality to track use and key activities within the mobile payment acceptance solution.
Limit exposure of account data that could be used to commit fraud.	<ol style="list-style-type: none"> 6. Provide the ability to encrypt all public transmission of account data. 7. Ensure that account data electronically read from a payment card is protected against fraudulent use by unauthorized applications in a consumer mobile device. 8. Provide the ability to truncate or tokenize the Primary Account Number (PAN) after authorization to facilitate cardholder identification by the merchant. 9. Protect stored PAN data and/or sensitive authentication data.

Best Practices for Merchants:

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.
Limit the exposure of account data that may be used to commit fraud.	2. Limit access to the mobile payment acceptance solution. 3. Immediately report the loss or theft of a consumer mobile device and/or hardware accessory.
Prevent software attacks on consumer mobile devices.	4. Install software only from trusted sources. 5. Protect the consumer mobile device from malware.

This is the first version of these best practices to support the growth of the emerging mobile acceptance channel. Visa Europe will continue to refine and update the best practices based on industry feedback.

Beyond the best practices, vendors, merchants and acquirers are expected to follow all Visa requirements for magnetic stripe, chip and contactless acceptance. They should also adhere to the principles set forth in the Payment Card Industry Data Security Standard (PCI DSS) and Payment Application Data Security Standards (PA-DSS). Additionally, on top of following Visa Europe Operating Regulations, acquirers must also be in compliance with all local laws and regulations regarding sponsored merchants, including adequate Know Your Customer (KYC) and Anti-Money Laundering (AML) due diligence.

###