



Visa Inc.

[About Visa Inc.](#)

[Products](#)

[Security](#)

[Careers](#)

[Media Center](#)

[Investor Relations](#)



Press Releases

[Printable Format](#)

[Press Releases](#)

[Media Contacts](#)

[Statistics](#)

[Fact Sheets](#)

[Downloadable Assets](#)

[Press Kit](#)

[Speeches & Presentations](#)

[Interchange](#)

[Understanding Visa Transactions](#)

[Economics of the Visa System](#)

[Facts About Interchange](#)

[Interchange FAQ](#)

Visa Mandates Use of Secure Payment Software in the United States

Payment Systems Storing Prohibited Card Data Put Merchants at Risk for Breaches

SAN FRANCISCO, 8 November 2007

Visa Inc. today announced a series of requirements for U.S. merchants and their agents to use payment system software that does not store sensitive card information. The requirements are designed to protect cardholder information and complement other security efforts including compliance with the Payment Card Industry Data Security Standard (PCI DSS).

The phased-in mandates, which begin January 1, 2008, require U.S. banks that service merchants (acquirers) to ensure that their merchant customers and agents only use versions of payment applications that do not store prohibited data elements such as full magnetic stripe (track), CVV2 and PIN data and that adhere to Visa's Payment Application Best Practices (PABP). In most cases, data storage can be eliminated by using an updated version of a business' existing payment software.

Visa research confirms that vulnerable payment applications are the leading cause of compromise incidents, particularly among small merchants. "Criminals are targeting certain versions of software because of their known security gaps," said Michael E. Smith, senior vice president, payment system risk, Visa Inc. "Some versions of software in use today are known to store the full content of the magnetic stripe, PIN data or security codes contrary to Visa rules and the PCI Data Security Standard," he said. According to Smith, criminals are seeking card data because of the information's potential use in creating counterfeit cards.

Visa introduced PABP in 2005 to assist software vendors in creating secure payment applications. The PCI Security Standards Council (PCI SSC) recently announced that it has adopted Visa's PABP and plans to release the latest industry standard as the Payment Application Data Security Standard (PA-DSS) in early 2008. Visa mandates pertaining to PABP will be modified to reflect the PA-DSS upon its final release.

The series of Visa requirements will take effect over the next three years to allow for an effective transition. Beginning January 1, 2008, U.S. acquirers are no longer allowed to sign new merchants that use known vulnerable payment applications. Furthermore, processors on the Visa network (VisaNet) and their agents must not certify new payment applications to their platforms that have been identified as vulnerable. A list of vulnerable payment applications is updated quarterly and made available to merchants and agents through their respective acquirers.

Effective July 1, 2008, VisaNet processors and agents can only certify new payment applications to their platforms that are PABP-compliant. Starting October 1, 2008 acquirers can only board new Level 3¹ and Level 4² merchants that are PCI DSS compliant or utilize PABP-compliant applications. PABP does not apply to applications developed for in-house use only or to stand-alone terminals.

VisaNet processors and agents are required to decertify all known vulnerable payment applications by October 1, 2009, including those published on Visa's list of vulnerable payment applications. As future vulnerable payment applications are identified, VisaNet processors and agents must decertify these applications within 12 months of identification. Finally, by July 1, 2010, acquirers must ensure their merchants and agents only use PABP-compliant applications.

Under the Visa PABP program, vendors submit specific versions of payment applications for assessment by a qualified payment application security assessor approved by Visa. In addition to

preventing the retention of prohibited data, the PABP requires payment applications to include security controls in support of a merchant or service provider's ability to comply with the PCI DSS. The PABP validation process also verifies that payment applications are developed using secure coding procedures to guard against common attack methods. A list of PABP-validated applications is available at www.visa.com/pabp. Visa makes no endorsement of applications or products and disclaims all warranties.

Smith calls on merchants and agents to ask their payment application vendors, resellers or system integrators to confirm that software versions used do not store magnetic-stripe, PIN data or security codes. "Merchants with vulnerable payment applications should move quickly to either patch or upgrade their systems," said Smith.

###

Note to editors:

About Visa: Visa connects cardholders, merchants and financial institutions through the world's largest electronic payments network. Visa products allow buyers and sellers to conduct commerce with ease and confidence in both the physical and virtual worlds. As an association owned by 21,000 member financial institutions, Visa is committed to the sustained growth of electronic payment systems to support the needs of all stakeholders and to drive economic growth. For more information, visit www.corporate.visa.com.

[1] Level 3 includes any merchant processing 20,000 to 1 million Visa e-commerce transactions per year.

[2] Level 4 includes any merchant processing less than 20,000 Visa e-commerce transactions per year, and all other merchants processing up to 1 million Visa transactions per year.

Contact: Jay Hopkins, CRC Public Relations for Visa Inc., Tel: +1 703-683-5004 ext 107 at jhopkins@crccpublicrelations.com

[Go back to Press Releases](#)

[Privacy Policy](#) | [Terms of Use](#) | [Contact Us](#) | [Site Map](#) | [Global Visa Sites](#)

© Copyright 2008, Visa Inc. All Rights Reserved