

Visa Announces New Payment Application Security Mandates

In Brief

Beginning January 1, 2008, Visa will implement a series of mandates to eliminate the use of non-secure payment applications from the Visa payment system. These mandates require members to ensure that their merchants and agents do not use payment applications known to retain prohibited data elements and require the use of payment applications that adhere to Visa's Payment Application Best Practices (PABP). PABP-compliant applications help merchants and agents mitigate compromises, prevent storage of prohibited data and support overall compliance with the Payment Card Industry Data Security Standard (PCI DSS) and the *Visa U.S.A. Inc. Operating Regulations*. A list of PABP-validated applications is available at www.visa.com/pabp.

Audience:

- Acquirers
- Issuers
- Processors

Suggested Audience

- Technical Staff
- Business Staff
- Back Office Staff
- Regulatory Compliance
- Risk Control

Vulnerable payment applications have proved to be the leading cause of compromise incidents, particularly among small merchants. *Visa U.S.A. Inc. Operating Regulations* prohibit the storage of the full content of any magnetic-stripe, CVV2 or PIN data and require compliance with the Payment Card Industry Data Security Standard (PCI DSS). Merchants and agents that use payment applications that store prohibited data or have inherent security weaknesses will not be compliant with the PCI DSS and are at high risk of being compromised.

In light of the criticality of promoting payment application security and merchant dependence on secure payment applications to achieve compliance, Visa will implement a series of mandates, beginning January 1, 2008, to eliminate the use of vulnerable payment applications from the Visa payment system. These mandates support compliance with the *Visa U.S.A. Inc. Operating Regulations*, Section 5.2.1.3 and Section 1.16.B.43, which prohibit the storage of magnetic-stripe, CVV2 and PIN data. Further, Section 2.2.Q requires that members comply — and ensure that their merchants and agents comply — with the requirements of the Cardholder Information Security Program. These mandates are intended to prevent cardholder data compromises and thereby help mitigate the risk of associated financial losses such as liability from the Account Data Compromise Recovery (ADCR) program. Additionally, Visa's payment application security mandates reinforce member compliance efforts and create a level playing field by preventing merchants from migrating from one acquirer to another in attempt to avoid security requirements.

Outlined below are each of the five mandates, which will take effect over the next three years.

Phase	Compliance Mandates	Effective Date
I.	Newly boarded merchants must not use known vulnerable payment applications, and VisaNet Processors (VNPs) and agents must not certify new payment applications to their platforms that are known vulnerable payment applications	1/1/08
II.	VNPs and agents must only certify new payment applications to their platforms that are PABP-compliant	7/1/08
III.	Newly boarded Level 3 and 4 merchants must be PCI DSS compliant or use PABP-compliant applications	10/1/08
IV.	VNPs and agents must decertify all vulnerable payment applications	10/1/09
V.	Members must ensure their merchants, VNPs and agents use only PABP-compliant applications	7/1/10

Phase I – January 1, 2008

Members must not board new merchants that use known vulnerable payment applications. Furthermore, VNPs and agents must not certify new applications to their platforms that are known vulnerable payment applications. A list of vulnerable payment applications is updated quarterly and is available on Visa Online at www.us.visaonline.com/us_riskmgmt/cisp.

Phase I will deter vendors from introducing new vulnerable payment applications into the payment system and will reinforce member compliance efforts by preventing merchants from migrating from one acquirer to another in an attempt to avoid upgrading a vulnerable payment application.

Phase II – July 1, 2008

VNPs and agents must only certify new payment applications to their platforms that are PABP-compliant. A list of payment applications that have been validated against Visa's PABP is available at www.visa.com/pabp.

Phase II promotes the use of payment applications that adhere to PABP and support merchant PCI DSS compliance. This phase will also further prevent vendors from introducing new vulnerable payment applications into the payment system.

Phase III – October 1, 2008

Members must only board new Level 3 and Level 4 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 hardware terminals.

Phase III mitigates member risk associated with boarding new merchants that are not PCI DSS compliant or that rely on payment applications that are not PABP-compliant. Further, Phase III reinforces member compliance efforts by preventing merchants from migrating from one acquirer to another in an attempt to avoid compliance requirements.

Phase IV – October 1, 2009

VNPs and agents must decertify all known vulnerable payment applications, including those published on Visa's quarterly list of vulnerable payment applications. As future vulnerable payment applications are identified, VNPs and agents must decertify these applications within 12 months.

Phase IV is intended to eliminate the continued use of vulnerable payment applications by members, merchants and agents within the payment system.

Phase V – July 1, 2010

Members must ensure their merchants and agents use only PABP-compliant applications. A list of payment applications that have been validated against Visa's PABP is available at www.visa.com/pabp.

Phase V mandates the use of payment applications that support PCI DSS compliance, requiring acquirers, merchants and agents to use only those payment applications that can be validated as PABP-compliant. It is important to note that the deadline for Phase V is aligned with the Triple Data Encryption Standard (TDES) usage mandate for all Point-of-Sale (POS) PIN-entry devices (PEDs) to be using TDES to protect PINs. Additionally, all attended POS PEDs must be evaluated by a Visa-recognized laboratory and approved by Visa prior to this same date.