

Visa Announces New Payment Application Security Mandates

January 1, 2008

Visa implemented a series of mandates to eliminate the use of non-secure payment applications from the Visa payment system. These mandates require that merchants and agents do not use payment applications known to retain consumer personal information. Merchants are required to use 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
- support overall compliance with the Payment Card Industry Data Security Standard (PCI DSS)

At some point most merchants will be touching credit cards and have access to cardholder data. **The PCI compliancy requirement is for anyone who "stores, transmits, or processes" cardholder data.** Merchants are subject to fines if a credit card company performs an audit and they are found not to be compliant. Credit card companies have put the burden on acquirers, like RBS WordPay to monitor merchants for compliancy and are **required** to report any non-compliant merchants.

A minimum \$5,000 fine will be issued to any merchant who experiences a security breach. In addition to the fine, most breaches require a third party audit. A single merchant should expect to pay \$20,000 to \$30,000 at a minimum between the fine and audit.

Vulnerable payment applications are the leading cause of compromise incidents, particularly among small merchants, and are at high risk of being compromised. **Merchants are prohibited from storing the content of any magnetic-stripe, CVV2 or PIN data.** Merchants that use payment applications that store prohibited data or have inherent security weaknesses will not be compliant with the PCI DSS. It is now CRITICAL to promote customer security through merchant dependence on secure payment applications.

The mandates listed below are intended to prevent cardholder data compromises and thereby help mitigate the risk of associated financial losses. Additionally, they reinforce acquirer compliance efforts and create a level playing field by preventing merchants from migrating from one acquirer to another in attempt to avoid security requirements. © 2007 Visa Inc., all rights reserved. CISP BULLETIN – 102307

Five Phase Compliance Mandates

1. Effective Date: January 1, 2008

Newly boarded merchants must not use known vulnerable payment applications, and VisaNet Processors (VNPs). Agents must not certify new payment applications to their platforms that are known vulnerable payment applications.

2. Effective Date: July 1, 2008

VNPs and agents must only certify new payment applications to their platforms that are PABP-compliant.

3. Effective Date: October 1, 2008

Newly boarded Level 3 and Level 4 merchants must be PCI DSS compliant or use PABP-compliant applications.

4. Effective Date: October 1, 2009

VNPs and agents must decertify all vulnerable payment applications, and all known vulnerable payment applications must be removed from your system.

5. Effective Date: July 1, 2010

Acquirers must ensure their merchants, VNPs and agents use only PABP-compliant applications. This includes Point of Sale Systems, even if the POS is not being used to process credit cards.

Phase I – January 1, 2008

Acquirers 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 acquirer 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

Acquirers 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 acquirer 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 acquirer compliance efforts by preventing merchants from migrating from one acquirer to another in an attempt to avoid compliance requirements.

© 2007 Visa Inc., all rights reserved, CISP BULLETIN – 102307

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 acquirers, merchants and agents within the payment system.

Phase V – July 1, 2010

EVEN IF A MERCHANT DOES NOT PROCESS CREDIT CARDS THROUGH THEIR POINT OF SALE SYSTEM, THEY MUST USE A POINT OF SALE SYSTEM WHICH IS CERTIFIED PABP-COMPLIANT.

Acquirers 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. PCI DSS compliance is required of all entities that store, process, or transmit Visa cardholder data, including merchants. The PCI DSS applies to all payment channels, including retail (brick-and-mortar), mail or telephone order, and e-commerce.

Vulnerable Payment Applications

As a result of an increasing number of merchant compromises, Visa has identified that certain payment applications are designed to store prohibited data, including full magnetic-stripe, CVV2 or PIN data, subsequent to transaction authorization. Storage of these data elements is in violation of the PCI DSS and *Visa U.S.A. Inc. Operating Regulations*. Hackers are targeting merchants and agents using vulnerable payment applications and exploiting vulnerabilities to find this data. It is critical for acquirers to ensure that their merchants and agents do not use payment applications known to retain prohibited data elements and to take corrective actions to address any identified deficiencies. Acquirers, merchants and agents should ask all of their payment application vendors, resellers or system integrators to confirm that software versions used do not store magnetic-stripe, CVV2 or PIN data.

Recently, Visa alerted acquirers of an updated list of vulnerable payment applications that retain prohibited data. Visa will continue to proactively alert acquirers as vulnerable payment applications are identified. The vulnerable payment application list is available on Visa Online at www.us.visaonline.com/us_riskmgmt/cisp. © 2007 Visa Inc., all rights reserved, CISP BULLETIN – 102307

Payment Application Best Practices

Visa developed the PABP to help payment application vendors develop secure applications that do not store prohibited data and that support compliance with the PCI DSS. PABP applies only to third-party payment software that stores, processes or transmits cardholder data. PABP does not apply to hardware terminals or software developed by merchants and agents for in-house use only. A list of payment applications that have been validated against Visa's PABP is available at www.visa.com/pabp. Acquirers should insist that their merchants and agents use PABP-validated applications and upgrade or patch applications that cause the storage of prohibited data.

Summary

To enforce the payment application security mandates, Visa will continue to identify payment applications used by Level 1 and 2 merchants through the PCI Compliance Acceleration Program, monitor acquirers' Level 4 merchant compliance plans and determine payment applications certified by VNPs. Visa may also consider a compromised entity's use of vulnerable payment applications or PABP-validated applications in fine and ADCR determinations. Visa will continue to work with all key stakeholders — acquirers, processors, merchants, agents and payment application vendors — to raise security awareness and promote the use of payment applications validated against the PABP. **In many cases, acquirers, processors and agents have indicated that they already have more aggressive plans in place to support these mandates.**

A list of PABP-validated applications is available at: www.visa.com/pabp.