CISP BULLETIN

Visa Announces New Payment Application Security Mandates

October 23, 2007

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 acquirers to ensure 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.

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 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*, which prohibit the storage of magnetic-stripe, CVV2 and PIN data. Further, the Operating Regulations require that acquirers comply — and ensure that their merchants and agents comply — with the requirements of the Cardholder Information Security Program (CISP). 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 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.

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.	Acquirers must ensure their merchants, VNPs and agents use only PABP-compliant applications	7/1/10

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.

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

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.

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.

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.

The PCI Security Standards Council (PCI SSC) will be adopting Visa's PABP and plans to release the standard as the Payment Application Data Security Standard (PA-DSS) in the next year. References to PABP will be modified to reflect PA-DSS upon release.

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. It is critical for acquirers and processors to begin integrating these mandates into their processes. Acquirers should also revisit their Level 4 merchant compliance plans and adjust accordingly to support these mandates. In an effort to mitigate the risk of compromise, acquirers must take prompt action to ensure that merchants and agents discontinue use of vulnerable payment applications and begin moving merchants and agents toward using only PABP-compliant applications.

For more information on Visa's PABP, please visit http://www.visa.com/pabp. Questions about this bulletin may be directed to CISP@visa.com. For the complete VBR, Visa acquirers may refer to the *Visa Business Review* article, "Visa Announces New Payment Application Security Mandates," October 2007; Issue 07100902.