



CISP BULLETIN

U.S. Payment Application Security Mandates Frequently Asked Questions

November 6, 2009

On January 1, 2008, Visa implemented a series of mandates to eliminate the use of vulnerable payment applications from the Visa payment system. These mandates require acquirers to ensure that their merchants and agents do not use payment applications known to retain sensitive cardholder data (i.e. full magnetic stripe data, CVV2 or PIN data) and require the use of payment applications that are compliant to the PA-DSS.

Phase	Compliance Mandate	Effective Date
1	Newly boarded merchants must not use known vulnerable payment applications; VisaNet Processors (VNPs) and agents must not certify new payment applications to their platforms that are known vulnerable payment applications	1/1/08
2	VNPs and agents must only certify new payment applications to their platforms that are PA-DSS compliant	7/1/08
3	Newly boarded Level 3 and Level 4 merchants must be PCI DSS compliant or must use PA-DSS compliant applications ¹	10/1/08
4	VNPs and agents must decertify all vulnerable payment applications ²	10/1/09
5	Acquirers must ensure that their merchants, VNPs and agents use only PA-DSS compliant applications	7/1/10

1. In-house use only developed applications and stand-alone hardware terminals are not applicable.

2. VNPs and agents must decertify vulnerable payment applications within 12 months of identification.

In an effort to provide further clarity for the mandates, Visa has provided the following frequently asked questions and answers.

Q1. What are payment applications?

A1. For the purposes of Visa mandates, payment applications are third party applications that store, process or transmit cardholder data as part of the authorization or settlement of a payment card transaction. These applications, traditionally used in point-of-sale (POS) systems, are typically designed for use on a PC-based architecture (e.g., desktops and servers running on a Windows, Unix, or Linux operating system). **Note:** In card data compromise cases, these integrated POS systems are the most prevalent targets under attack by criminals.

Q2. If a merchant uses a front-end integrated POS application, a middleware component and back-end software, are these applications within the scope of the mandates?

A2. Acquirers must ensure that merchants use only Payment Application Data Security Standard (PA-DSS) compliant payment applications anywhere that payment applications are being used in the cardholder data environment as part of authorization or settlement.



Q3. If a merchant or agent is not using a payment application, are they within the scope of the mandates?

A3. Merchants and agents only using in-house developed payment applications, stand-alone hardware terminals or PIN entry devices (PEDs) are not within the scope of the Visa payment application security mandates. While these systems are within the scope of the PCI DSS, merchants and agents using such systems have traditionally had less reliance on third party vendors to facilitate their overall PCI DSS compliance.

In addition, merchants using software-as-a-service (SaaS) solutions or virtual POS terminals hosted completely at a third party are not within the scope of the mandates, provided these solutions are hosted by a third party and no such configurations, controls or systems reside on the merchant's or the agent's systems. Instead, merchants must use PCI DSS compliant service providers to provide SaaS solutions or virtual POS terminals.

Merchants are within the scope of the mandates and must use PA-DSS compliant payment applications if any such configurations, controls or systems do reside at the merchant or the agent location.

Q4. Will PABP compliant payment applications be accepted for the mandates or must applications now be PA-DSS compliant?

A4. Both PABP and PA-DSS compliant applications will satisfy the Visa payment application security mandates.

Q5. Does a PABP or PA-DSS compliant payment application also need to be validated by a Payment Application Qualified Security Assessor (PA-QSA) and listed?

A5. While Visa encourages acquirers to require that merchants and agents use payment applications that have been validated against the PABP or PA-DSS, a payment application is not required to be included on the [Visa List of PABP Validated Payment Applications](#) or the [PCI SSC List of PA-DSS Validated Payment Applications](#).

Acquirers may determine the compliancy of a payment application through alternate validation processes, confirming that the application meets all of the PA-DSS requirements and facilitates compliance with the PCI DSS. However, the vast majority of acquirers have required their merchants to use validated and listed payment applications. Visa reserves the right to review acquirers' and their agents' validation processes.

Q6. What are vulnerable payment applications?

A6. For the purposes of the Visa payment application security mandates, vulnerable payment applications are identified as those payment applications that store sensitive authentication data (e.g., full magnetic-stripe data, CVV2, PIN data) subsequent to authorization. Vulnerable payment applications, confirmed by their vendors, can be found on *Visa's list of vulnerable payment applications*. This list is updated on a quarterly basis and is available to clients and processors in the "Risk Management" section at [Visa Online](#).



Q7. If a vulnerable payment application is recently identified, will an acquirer be in violation of Phase 4 of the mandates if the application is still certified to the processing platform?

A7. For newly identified vulnerable payment applications, acquirers must ensure that processors and agents take immediate action and fully remove vulnerable payment applications from their processing platform within 12 months from the time of identification. Acquirers remain liable for any compromises resulting from the use of a vulnerable payment application by its merchants or agents.

Q8. Will a merchant's, processor's or agent's use of an automated process or solution to scan for vulnerable payment applications suffice as an alternate validation process?

A8. Acquirers must ensure that payment applications used by merchants, processors, and agents are compliant with all of the PA-DSS requirements and not to just a subset of the requirements.

Q9. When using a payment application that is not listed as PA-DSS or PABP validated, is a merchant in compliance with the Visa payment application security mandates?

A9. For the purposes of these mandates, payment applications that are not identified on the *Visa List of PABP Validated Payment Applications* or the *PCI SSC List of PA-DSS Validated Payment Applications*, or are not on the *Visa List of Vulnerable Payment Applications that Store Sensitive Authentication Data* (located at www.visaonline.com), are considered to be unconfirmed payment applications. While these payment applications may be PA-DSS compliant, acquirers must ensure that only applications that meet all of the PA-DSS requirements are being used by their merchants, processors and agents.

It is critical that acquirers using alternate validation processes verify that these unconfirmed payment applications are PA-DSS compliant and continue to be supported by the software vendor. Under these circumstances, acquirers may require their merchants to validate full PCI DSS compliance as an alternate validation process.

Q10. The PCI SSC List of PA-DSS Validated Payment Applications includes an expiration date for each payment application. When should a payment application with expired validation be retired by a merchant or agent?

A10. Expiration dates provided on the *PCI SSC List of PA-DSS Validated Payment Applications* are for listing purposes only and are intended to alert vendors to any products that will soon be listed as expired. Applications that are not revalidated against the PA-DSS through a Payment Application Qualified Security Assessor (PA-QSA) by the posted expiration date are noted as expired on the *PCI SSC List of PA-DSS Validated Payment Applications*. This does not mean that the payment application is no longer compliant; it simply means that the vendor did not re-validate the payment application. Merchants and agents should contact the vendor to determine the application's continued compliance.

The PA-DSS is revised every two years to respond to compromise trends. Payment applications continue to be the target of criminals exploiting vulnerabilities and weaknesses in the cardholder data environment. Acquirers should urge their merchants and agents to use payment applications validated against the latest PA-DSS requirements to ensure higher levels of protection.



In addition, to be in compliance with the PCI DSS, merchants and agents are already required to maintain software patches for all systems. Merchants and agents are advised to carefully consider the risks of remaining on older payment applications when deciding whether to deploy more recent versions.

Q11. What is a newly boarded merchant?

A11. For the purposes of these mandates, a newly boarded merchant is defined as a newly executed merchant account with an acquirer. Acquirers may have chosen to apply Phases 1 and 3 to their merchant portfolios more broadly to facilitate compliance with future mandates and better manage their overall risks. Although additional locations of existing merchants are not considered to be newly executed merchant accounts, acquirers are encouraged to ensure that these locations also use PA-DSS compliant payment applications.

Q12. If a merchant or agent is using a PA-DSS compliant payment application, is the entity PCI DSS compliant?

A12. Merchants and agents should understand that solely using a PA-DSS compliant payment application does not in and of itself cause them to be PCI DSS compliant. Merchants must additionally ensure that the application is implemented properly and must protect cardholder data anywhere it is being stored, processed or transmitted in accordance with PCI DSS requirements.

Q13. For Phase 3 of these mandates, Visa allows acquirers to board new merchants if they are using a PA-DSS compliant payment application or if they are PCI DSS compliant at the time of boarding. Is this permitted for Phase 5?

A13. Yes, acquirers must ensure that all of their Level 3 and 4 merchants, processors and agents either use only PA-DSS compliant payment applications or validate their PCI DSS compliance by July 1, 2010, to adhere to Phase 5. Acquirers may also request validation of full PCI DSS compliance for Level 3 and 4 merchants that have implemented adequate compensating controls to remediate any non-compliant payment applications.

Q14. Visa recently announced payment application security mandates for Visa regions outside of the U.S. Is the enforcement deadline for U.S. acquirers also being extended?

A14. In June 2009, Visa announced payment application security mandates for Visa regions including Latin America and Caribbean (LAC), Central and Eastern Europe, Middle East and Africa (CEMEA), and Asia Pacific (AP). These mandates do not supersede earlier deadlines and related enforcement programs already in place for the U.S. and Canada.

Questions about this bulletin may be directed to CISP@visa.com.