Visa Business News

Risk Management | Data Security

June 24, 2009

Payment Application Security Mandates Set Across Regions

New payment application security mandates require Visa clients to use, and ensure that their merchants and agents use, payment applications that adhere to the Payment Card Industry Payment Application Data Security Standard (PA-DSS). These security mandates require **full compliance by July 1, 2012**, and will not supersede any applicable, earlier regional deadlines and related enforcement programs already in place. For a list of products that have been independently validated against Visa's Payment Application Best Practices (PABP) or the PA-DSS, please visit www.visa.com and www.pcisecuritystandards.org/security_standards/vpa.

These mandates apply to all Visa regions. **Note:** Visa Europe operates as an independent company and licensee of Visa Inc. for business operations in Visa Europe markets. Visa Europe is aligned with the Visa payment application security framework, but has implemented its own set of mandates to drive compliance validation with the security initiatives detailed in this article. For information on the Visa Europe framework, please contact datasecuritystandards@visa.com.

About Payment Application Security Mandates

Vulnerable payment applications that store sensitive authentication data post authorization have proven to be the leading cause of compromise incidents, particularly among small merchants.

Merchants must not use known vulnerable payment applications that store sensitive authentication data post authorization. Storage of sensitive authentication data post authorization is strictly prohibited per the PCI DSS and *Visa International Operating Regulations*. For a list of vulnerable payment applications, Visa clients can refer to the *Visa List of Payment Applications that Store Sensitive Cardholder Data*, available at Visa Online or by request from your regional Account Information Security (AIS) or Cardholder Information Security Program (CISP) contact.

Accordingly, Visa will implement a series of mandates to eliminate the use of non-secure payment applications from the Visa payment system. These mandates, which will become effective over the next few years, require Visa clients to ensure that their merchants and agents use payment applications that are compliant with the PA-DSS. Compliance will be mandated in two phases:

Phase	Compliance Mandate	Effective Date
1	Newly boarded merchants that use payment application software must use PA-DSS compliant applications or be PCI	7/1/2010

Related Information

Visa Business News Archive

Key Dates

Visa Online

	DSS compliant	
2	Acquirers must ensure that merchants and agents use PA-DSS compliant payment applications	7/1/2012

Note: These mandates will not supersede any applicable earlier deadlines and related enforcement programs already in place for the U.S. and Canada, which require acquirers to ensure that their merchants and agents use PA-DSS compliant payment applications **by 1 July 2010**. For details on the U.S. and Canada payment application mandates, please visit www.visa.com/cisp and www.visa.ca/en/merchant/fraud-prevention/account-information-security/.

- **Phase 1 – July 1, 2010**

  Visa acquirers must only board new merchants that are PCI DSS compliant or that utilize PA-DSS compliant applications. For the purposes of this mandate, a new merchant is defined as a newly executed merchant account with an acquirer.

  Phase 1 reinforces acquiring member compliance efforts by preventing merchants from migrating from one acquirer to another in an attempt to avoid compliance requirements.

  Acquirers may choose to apply Phase 1 to their merchant portfolios more broadly to facilitate compliance with Phase 2 and better manage overall risk. 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.

- **Phase 2 – July 1, 2012**

  Visa acquirers must ensure that all merchants and agents use PA-DSS compliant applications.

  Phase 2 mandates the use of payment applications that support PCI DSS compliance, requiring acquirers to ensure that their merchants and agents (new and existing) use payment applications that are PA-DSS compliant and eliminate the use of known vulnerable payment applications.

  While use of PA-DSS validated payment applications is recommended, a payment application does not need to be included on the *List of Validated Payment Applications* in order to comply with these mandates for use of PA-DSS compliant applications. Acquirers may determine the PA-DSS compliance of a payment application through their own alternate validation processes, which confirm that applications meet the PA-DSS requirements and facilitate compliance with the PCI DSS.

For the purposes of these mandates, payment applications apply only to third-party payment application software that stores, processes or transmits cardholder data as part of the authorization or settlement of a payment card transaction. Traditionally used in point-of-sale systems, payment applications are typically designed for use on a PC-based architecture (e.g., desktops and servers running on a Windows, Unix or Linux operating system).

PA-DSS does not apply to merchant or agent in-house developed applications, stand-alone hardware terminals or PIN Entry Devices (PEDs). 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, software-as-a-service (SaaS) solutions hosted completely at a third party are not within the scope of these mandates, provided that 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. PA-DSS compliant payment applications must be used if any such configurations, controls or systems do reside at the merchant or agent location.

About the PA-DSS

The Payment Card Industry PA-DSS is a comprehensive set of international security requirements for software vendors and others that develop secure payment applications that do not store prohibited data, such as full magnetic-stripe, other sensitive authentication data or PIN data, as part of the authorization or settlement of a payment card transaction.

PA-DSS compliant applications help merchants and agents mitigate compromises, prevent storage of sensitive cardholder data, and support overall compliance with the PCI DSS.

In the past, merchants expressed difficulty in meeting compliance with the PCI DSS due to reliance on third-party payment application software designed with settings or features that hindered the merchants from meeting critical compliance requirements. The PA-DSS was developed by Visa, along with the four other founding payment brands of the PCI Security Standards Council, to help facilitate the broad adoption of consistent data security measures on a global basis.

Merchants and agents should understand that the use of a PA-DSS compliant payment application does not provide full PCI DSS compliance. They must additionally ensure that the application is implemented properly and must protect cardholder data anywhere it is stored, processed or transmitted in the payment environment, in accordance with PCI DSS requirements.

For More Information

Contact your Visa Account Manager, e-mail esupport@visa.com or call (888) 847-2488 to speak with a Visa subject matter expert.

Notice: This Visa communication is furnished to you solely in your capacity as a customer of Visa Inc. and member of the Visa payments system. By accepting this Visa communication, you acknowledge that the information contained herein (the "Information") is confidential and subject to the confidentiality restrictions contained in Visa's operating regulations, which limit your use of the Information. You agree to keep the Information confidential and not to use the Information for any purpose other than in your capacity as a customer of Visa Inc. or as a member of the Visa payments system. The Information may only be disseminated within your organization on a need-to-know basis to enable your participation in the Visa payments system.

Please be advised that the Information may constitute material nonpublic information under U.S. federal securities laws and that purchasing or selling securities of Visa Inc. while being aware of material nonpublic information would constitute a violation of applicable U.S. federal securities laws. This information may change from time to time. Please contact your Visa representative to verify current information. Visa is not responsible for errors in this publication. The Visa Non-Disclosure Agreement can be obtained from your VisaNet Account Manager or the nearest Visa Office.