



## CISP BULLETIN

# Visa's Payment Application Best Practices adopted as Security Standard

April 15, 2008

---

On November 7, 2007, the Payment Card Industry (PCI) Security Standards Council (SSC) adopted Visa's Payment Application Best Practices (PABP), and in April 2008 it released it as the Payment Application Data Security Standard (PA-DSS). The PA-DSS supports the PCI Data Security Standard (DSS) and reinforces that payment applications must not store sensitive cardholder data. The PCI SSC is an open standards body that similarly manages the PCI DSS and PCI PIN Entry Device (PED) Security Requirements. With the release of the PA-DSS, the PCI SSC now provides a global set of security requirements for payment applications supported by all five global payment card brands.

## Visa's PABP Overview

In 2004, Visa launched PABP to assist vendors in creating secure payment applications that help merchants and agents mitigate compromises, prevent storage of sensitive cardholder data (i.e., full magnetic stripe data, CVV, CVV2 or PIN data) and support overall compliance with the PCI DSS. To promote industry adoption of PABP, Visa contacted over 1000 payment application vendors through letters, webinars and held vendor conferences to build awareness of the need for payment applications that support PCI DSS compliance. Since the launch of PABP, nearly 300 payment applications across more than 120 payment application vendors have been independently validated by a Qualified Security Assessor (QSA). Many acquirers and processors now require their merchants and agents use only PABP validated payment applications. Visa continues to communicate with acquirers, processors, merchants, agents, payment application vendors and other key stakeholders to raise security awareness and encourage the use of payment applications validated against PABP. To promote the use of secure payment applications, Visa provides a list of PABP validated payment applications, publicly available at [www.visa.com/cisp](http://www.visa.com/cisp). Additionally, a list of vulnerable payment applications known to store sensitive cardholder data is distributed to acquirers, processors and other key stakeholders and can be found at Visa Online.

Using PABP validated payment applications does not alone guarantee or ensure compliance with the PCI DSS. Acquirers have an obligation to perform their own evaluation and due diligence to ensure the overall PCI DSS compliance of their merchants and agents. Merchants and agents must implement payment applications in a manner that will meet their requirements for performance and functionality, free from errors or malicious code, and will be compatible with any other systems or applications. It is critical that merchants and agents work with their payment application vendors to ensure secure deployment, implementation, configuration, troubleshooting and maintenance in compliance with the PCI DSS.



## Transitioning from PABP to the PA-DSS

The PCI SSC has now released the PA-DSS as the global set of security requirements for payment applications. In the coming months, the PCI SSC will begin training and qualifying assessors to validate payment applications against the PA-DSS. In late 2008, the PCI SSC will also assume management of the list of validated payment applications.

As part of the transition from PABP to PA-DSS, the PCI SSC has established a transition process to “grandfather” payment applications that have been validated or are currently being validated against PABP. These payment applications will be listed at the PCI SSC’s Web site and will include an expiration date by which the application must be revalidated under PA-DSS. Entities are encouraged to utilize the PA-DSS when initiating a new payment application review. Payment applications that are currently undergoing a review under PABP must submit validation to Visa by September 30, 2008 to be transitioned to the PCI SSC list. If PABP validation is not complete by September 30, 2008, the application will also need to undergo the PCI SSC’s PABP to PA-DSS Transition Procedures in order to be listed. Visa is committed to working with the PCI SSC to ensure a successful transition of PABP to PA-DSS. For more information on the PA-DSS requirements or the transition process, please refer to the Frequently Asked Questions section of the PCI SSC’s Web site at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

Please join Visa during a webinar on April 30, 2008 at 10:00 am PDT (GMT -07:00) to discuss the transition of PABP to PA-DSS. To register for the webinar please visit: <https://visa.webex.com/ec06001/eventcenter/enroll/join.do?siteurl=visa&confId=277926735>

Questions about this bulletin, webinar, or for dates and information on Visa’s data security training seminars may be directed to [CISP@visa.com](mailto:CISP@visa.com).