

Payment Application Data Security Standard: Frequently Asked Questions

Q. Why did the PCI Security Standards Council (PCI SSC) assume responsibility for the Payment Application Best Practices (PABP), now called the Payment Application Data Security Standard (PA-DSS)?

- A. *The PABP program was created and overseen by Visa. Now, through PCI SSC, the five major global payment brands (American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.) will support the PA-DSS, allowing even greater opportunity to standardize security requirements, Qualified Security Assessor testing and lab methodologies, and approval processes for payment applications.*

It is a strategic priority for PCI SSC to continue streamlining security standards and the validation of secure payment applications. Common requirements mean more consistent security measures and cost effective market deployment. Common requirements benefit all stakeholders in the payments value chain and are intended to improve the overall security for customer-entered data.

Q. What's involved in the transition from PABP to PCI PA-DSS?

- A. *In the next few months, PCI SSC will be qualifying companies to become Payment Application Qualified Security Assessors (PA-QSAs) Companies approved to become PA-QSAs will be recognized in a PCI SSC list and can begin conducting PA-DSS assessments in accordance with the PA-DSS Security Audit Procedures. In addition, PCI SSC will begin listing payment applications that have been validated in accordance with PA-DSS. The list, to be published towards the latter part of this year, will include both new payment applications that have been successfully validated against the PA-DSS, as well as PABP-validated payment applications that will be transitioned to the PCI SSC list,*

Q. Is the PA-DSS mandatory for all payment application providers?

- A. *Whether PA-DSS is mandatory or not will be determined by the payment brands.*

Q. What types of payment applications are subject to the PA-DSS requirements?

- A. *Payment applications that are sold, distributed or licensed to third parties and are installed "off the shelf" without much customization by software vendors are subject to the PA-DSS requirements.*

Q. What types of payment applications are NOT subject to the PA-DSS requirements?

- A. *Payment applications that are developed for and sold to only one customer are NOT subject to the PA-DSS requirements; however, they must be covered by the customer's PCI DSS assessment. Payment applications that are developed in-house by merchants or service providers and are not sold to a third party are NOT subject to the PA-DSS requirements, however, they must be covered by the merchants' or service providers' PCI DSS assessment. Payment applications that are resident in standalone point-of-sale terminals (also called dumb terminals) are NOT subject to the PA-DSS requirements provided that (1) the terminals have no connection to any of the merchant's systems or networks, (2) the terminals connect only to the merchant's acquirer or processor via a private line, (3) the payment application vendor provides secure remote updates, troubleshooting, access and maintenance, and (4) sensitive authentication data is never stored after authorization.*

Q. What types of payment applications are NOT subject to the PA-DSS requirements?

- A. The following list, while not all inclusive, illustrates applications that are NOT payment applications for purposes of PA-DSS (and therefore do not need to undergo PA-DSS reviews): operating systems onto which a payment application is installed (for example, Windows, Unix), database systems that store cardholder data (for example, Oracle), and back-office systems that store cardholder data (for example, for reporting or customer service purposes).*

Q. What part of the payment transaction process is addressed by the PA-DSS?

- A. The PA-DSS applies to software vendors and others who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement, where these payment applications are sold, distributed, or licensed to third-parties.*

Payment applications validated per PA-DSS, when implemented in a PCI DSS-compliant environment, will minimize the potential for security breaches leading to compromises of full magnetic stripe data, card validation codes and values (CAV2, CID, CVC2, and CVV2), PINs and PIN blocks, and the damaging fraud resulting from these breaches. Internally developed applications that are not sold or distributed to third-parties are not subject to PCI PA-DSS but are subject to PCI DSS.

Q. Will the PCI SSC accept applications that have been previously validated under the existing Visa PABP program?

- A. PCI SSC will recognize PABP validated payment applications and list them with the appropriate PABP version that they were validated against. For payment applications validated against pre-PABP version 1.3, they must undergo a PA-DSS assessment within twelve (12) months after the initial publication of the PCI SSC list otherwise they will expire and will no longer be accepted for new deployments. For payment applications validated against PABP version 1.3, they must undergo a PA-DSS assessment within eighteen (18) months after the initial publication of the PCI SSC list. For payment applications validated against PABP version 1.4, they must undergo a PA-DSS assessment within twenty-four (24) months after the initial publication of the PCI SSC list. Please refer to the table in the Grandfathering PABP Applications section of the PA-DSS Program Guide for more details.*

Q. How does the PA-DSS impact customers?

- A. Secure payment applications help to facilitate a customer's PCI DSS compliance. When implemented in a DSS-compliant environment, PA-DSS validated payment applications will minimize the potential for security breaches leading to compromises of full magnetic stripe data, card validation codes and values (CAV2, CID, CVC2, and CVV2), PINs and PIN blocks.*

Q. How will the migration to PA-DSS impact vendors previously validated under PABP?

- A. Vendors with applications validated under PABP will have three options as follows:*
- 1. PCI SSC will recognize applications validated under PABP and included on Visa's list as answered above, depending on whether the application was reviewed per PABP version 1.3 or 1.4, or per a PABP version prior to 1.3. Please refer to answer above as well as the table in the Grandfathering PABP Applications section of the PA-DSS Program Guide for more details.*
 - 2. For applications that are under PABP review at the time of the transition, if the review is completed and accepted by Visa prior to October 15, 2008, the application will be "grandfathered" in accordance with Step 1 above. For reviews that are not completed*

and accepted by Visa prior to October 15, 2008, PA-QSAs must additionally complete the PA-DSS Transition Procedures to have their application recognized per PA-DSS.

3. For an application previously recognized under PABP, but for which a vendor wants to be recognized per PA-DSS, a PA-QSA must additionally complete the PA-DSS Transition Procedures.

Q. Who will perform PA-DSS assessments?

- A. Only PA-QSAs will be recognized by PCI SSC to validate payment applications. PA-QSAs are QSAs that have been qualified and trained by PCI SSC to perform PA-DSS reviews. Note that all QSAs are not PA-QSAs – there are additional qualification requirements that must be met for a QSA to become a PA-QSA, and PA-QSAs will need to apply and be qualified by PCI SSC. The list of PA-QSAs will be published by PCI SSC towards the latter part of this year.

Q. Where can I find the list of PA-DSS applications?

- A. The list of those validated applications is targeted to be published by PCI SSC toward the end of September. Grandfathered PABP applications, PABP applications that go through the PA-DSS Transition Procedures, and newly validated PA-DSS applications will be on this list. Visa will continue to publish their list of PABP applications until publication of PCI SSC's list.

Q. How much will it cost for a vendor to have their products validated to PA-DSS by a PA-QSA?

- A. The prices and fees charged by PA-QSAs are not set by PCI SSC; these fees are negotiated between the PA-QSA and their customer, and paid directly to the PA-QSA. Before deciding on a PA-QSA, it is recommended that entities talk to several PA-QSA firms.

Q. How can I be assured that PA-QSAs operate on an even playing field? What assurances can the Council give me regarding the quality of organizations assessing and remediating my systems for PA-DSS compliance?

- A. The Council will maintain the list of approved PA-QSAs and has incorporated a PA-DSS quality assurance program to ensure that services provided are of an appropriate level. PA-QSAs that do not meet the quality criteria set forth by the Council will be subject to adverse action including, but not limited to, probation, penalty fees and/or revocation.

Q. Will there be any program fees?

- A. The PA-DSS program will impose annual fees for PA-QSAs to be recognized by PCI SSC and permitted to conduct PA-DSS assessments. Please refer to the PA-QSA Validation Requirements for additional information regarding PA-QSA annual fees including region-specific fees. The PA-DSS program will also impose an annual fee to recognize a PA-DSS validated application on the PCI SSC list. Please refer to the PA-DSS Program Guide for more details.

Q. Will PCI SSC continue to recognize PA-QSAs previously recognized by Visa for PABP assessments?

- A. If a company that was previously recognized by Visa for PABP assessments is interested in performing PA-DSS assessments, PCI SSC requires those companies to enroll and qualify as a new PA-QSA. In accordance with the PA-QSA Validation Requirements, PA-QSAs must submit the appropriate documentation and their employees must undergo training.

Q. How does the PCI PA-DSS integrate with the PCI Data Security Standard (DSS)?

- A. *The requirements for Payment Application Data Security Standard (PA-DSS) are derived from the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS details what is required for a customer to be PCI DSS compliant (and therefore what a payment application must support to facilitate a customer's PCI DSS compliance).*

Traditional PCI DSS compliance may not apply to payment application vendors since most vendors do not store, process, or transmit cardholder data. However, because these payment applications are used by customers to store, process, and transmit cardholder data, and customers are required to be PCI DSS compliant, payment applications should facilitate, and not prevent, customers' PCI DSS compliance. A few of the ways payment applications can prevent a customer's compliance are: 1) storage of magnetic stripe data in the customer's network after authorization; 2) applications that require customers to disable other features required by PCI DSS, such as anti-virus software or firewalls, and; 3) vendors that use unsecured methods to connect to the application to provide support to the customer.