Payment Application Security

As Assessment

Rov Report on Validation

Trustwave's unmatched experience and expertise make it the leading provider of payment application validation services.

For payment application vendors that want to validate their application's compliance with the Payment Application Data Security Standard (PA-DSS)

About Trustwave®

Trustwave is a leading provider of information security and compliance management solutions to large and small businesses throughout the world. Trustwave analyzes, protects and validates an organization's data management infrastructure - from the network to the application layer – to ensure the protection of information and compliance with industry standards and regulations such as the PCI DSS and ISO 27002, among others. Financial institutions, large and small retailers, global electronic exchanges, educational institutions, business service firms and government agencies rely on Trustwave. The company's solutions include on-demand compliance management, managed security services, digital certificates and 24x7 multi-lingual support. Trustwave is headquartered in Chicago with offices throughout North America, South America, Europe, the Middle East, Africa, Asia and Australia.

A Analyze P Protect V Validate

The Name to Trust

In an increasingly cashless world, payment applications play a critical role in the transaction process. Payment applications can also expose their host environment to significant risk because confidential consumer information passes through them. A majority of cases of cardholder data theft result from payment applications that are not secure.

To prevent such theft, Visa, with significant input from Trustwave, developed the Payment Application Best Practices (PABP) in 2004 to aid payment application vendors in the secure development of applications that process, store or transmit cardholder data. In 2008, authority over the standard passed to the PCI Security Standards Council (PCI SSC), and it was renamed the Payment Application Data Security Standard (PA-DSS).

Trustwave has validated the compliance of more payment applications than any other Payment Application Qualified Security Assessor (PA-QSA), companies certified by the PCI SSC to perform such audits. As a result, Trustwave's expertise is unmatched. We have the most experienced team of payment application security specialists in the industry. Trustwave performed the very first PABP assessment in 2004 and has validated hundreds of applications since.

Complete Validation Services

Trustwave's Payment Application Validation services ensure that the payment applications you develop meet or exceed the requirements of the PA-DSS.

Our services for payment applications include the following:

- Interviews with application developers, application support staff and product managers
- Thorough documentation review
- Functional and security testing of the application
- Technical and forensic review of application components, payment transaction logs and cardholder data storage to ensure prohibited data (e.g., full track and card security codes) is not stored
- Follow-up communications with the PCI SSC
- Remediation recommendations and application re-validation
- Final review of the application and submission of Report on Validation to the PCI SSC

Optional services include:

- Application penetration testing
- Minor and major release follow-up reviews and attestation filing with the PCI SSC
- Application code signing using Extended Validation (EV) SSL certificates from Trustwave

70 W. Madison Street, Suite 1050, Chicago, IL 60602
www.trustwave.com
1.888.878.7817

Trustwave® Information Security & Compliance

PA-DSS in Brief

The high-level PA-DSS guidelines for payment applications include:

1. Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2), or PIN block data.
2. Protect stored cardholder data.
3. Provide secure authentication features.
4. Log payment application activity.
5. Develop secure payment applications.
6. Protect wireless transmissions.
7. Test applications to address vulnerabilities.
8. Facilitate secure network implementation.
9. Cardholder data must never be stored on a server connected to the Internet.
10. Facilitate secure remote software updates.
11. Facilitate secure remote access to application.
12. Encrypt sensitive traffic over public networks.
13. Encrypt all non-console administrative access.
14. Maintain instructional documentation and training programs for customers, resellers and integrators.

The Risks Are Clear

Credit card data typically enters a merchant's environment through some form of payment application. Unauthorized parties seeking access to card data often target payment applications because of the lack of proper security controls, improper configuration or insecure implemention securely.

Point-of-Sale (POS) systems and other payment applications contribute to the majority of cardholder data compromises investigated by Trustwave. Payment applications that retain full track data present significant risks to cardholders, merchants and ultimately to the payment application developers themselves.

Frequently Asked Questions

Who oversees the PA-DSS requirements?

The PA-DSS requirements are managed by the PCI SSC, a joint effort founded by the five major card brands (American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa Inc.). The PCI SSC also administers the Payment Card Industry Data Security Standard (PCI DSS). Trustwave communicates regularly with the card brands and the PCI SSC to discuss information security trends and to provide suggestions for program improvement.

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

Any application that processes, stores or transmits cardholder data for the purpose of authorization and/or settlement and is sold to third parties is subject to PA-DSS requirements. If an application performs the same functions but is not sold to third parties (such as payment applications built in-house), it is subject to only the PCI DSS.

Who can perform PA-DSS assessments?

Only vendors recognized by the PCI SSC as PA-QSAs can perform PA-DSS assessments. Trustwave has been certified since 2004 to perform payment application assessments and has performed hundreds of assessments in that time.

How burdensome is the validation process?

Trustwave has developed an efficient PA-DSS validation process to ensure that payment applications are evaluated in a timely and cost-effective manner. This provides a straightforward mechanism for achieving PA-DSS compliance and reduces the burdens of validation on your organization.

What can happen if I don't validate my payment application as PA-DSS compliant?

Developers who do not validate their payment applications as PA-DSS compliant cannot appear on the PCI SSC's list of validated applications. Organizations working toward compliance with the PCI DSS must choose applications from the approved list in order to become compliant.

Visa Payment Application Deadlines

Visa Deadline	Visa Requirement
January 1, 2008	**New merchants, or merchants changing acquiring banks, must not use applications that Visa considers vulnerable.**
July 1, 2008	**Processors cannot allow new applications to connect to their network that are not compliant with PABP or the PA-DSS.**
October 1, 2008	**Level 3 or Level 4 merchants* that are new or changing acquiring banks must validate their PCI DSS compliance or use PABP or PA-DSS-compliant payment applications.**
October 1, 2009	**Processors must block all payment applications that Visa considers vulnerable.**
July 1, 2010	**All merchants must use PABP or PA-DSS-compliant applications. All other applications will no longer be compatible with the Visa payment network.**

**As defined by Visa, Level 3 merchants are any merchant that processes between 20,000 and 1,000,000 Visa e-commerce transactions per year. Visa defines Level 4 merchants as any merchant that processes fewer than 20,000 Visa e-commerce and all other merchants that process fewer than 1,000,000 transactions per year regardless of acceptance channel.*

70 W. Madison Street, Suite 1050, Chicago, IL 60602
www.trustwave.com
1.888.878.7817