



PA-DSS MANDATE UPDATE

As of July 1, 2010, Visa® requires you to use a payment application that adheres to the Payment Card Industry Security Standards Council's (PCI SSC's) Payment Application Data Security Standard (PA-DSS), formerly known as Visa's Payment Application Best Practices (PABP).

This is the fifth and final phase of a three-year-long endeavor that began on January 1, 2008, when Visa implemented compliance mandates. These

mandates are designed to eliminate the use of non-secure payment applications that store prohibited data elements from Visa's payment system.

According to the PCI SSC, "The goal of PA-DSS is to help software vendors and others develop secure payment applications that do not store prohibited data, such as full magnetic stripe, CVV2 or PIN data, and ensure payment applications support compliance with the [...] PCI DSS."

The fifth phase of the Visa mandates requires your payment application to comply with the PA-DSS requirements, derived from PCI PA-DSS Requirements and Security Assessment Procedures. An application that is PA-DSS compliant meets the following requirements:

1. Does not retain full magnetic stripe, card verification code or value (CAV2, CID, CVC2, CVV2) or PIN block data.
2. Protects stored cardholder data.
3. Provides secure authentication features.
4. Logs payment application activity.
5. Develops secure payment applications.
6. Protects wireless transmissions.
7. Tests payment applications to address vulnerabilities.
8. Facilitates secure network implementation.
9. Never stores cardholder data on a server connected to the Internet.
10. Facilitates secure remote software updates.
11. Facilitates secure remote access to payment application.
12. Encrypts sensitive traffic over public networks.
13. Encrypts all non-console administrative access.
14. Maintains instructional documentation and training programs for customers, resellers and integrators.

FOLLOW THESE BEST PRACTICE TIPS

To ensure your business, including your software or payment application, is compliant:

- **Discuss compliance with your software or payment application vendor**, and let the vendor know that compliance is important to you.
- **Determine the full name and version number of your software/application**, then review the approved List of Validated Payment Applications at pcisecuritystandards.org/security_standards/vpa/vpa_approval_list.html to verify compliance of your software/application and version.
- **Meet all PCI DSS requirements, and validate your compliance** by completing the Self-Assessment Questionnaire (SAQ) and passing network vulnerability scans.
- **Complete the PCI DSS SAQ to identify any vulnerability** using a Qualified Security Assessor (QSA)* to help with your PCI SAQ.
- **Complete a network vulnerability scan if you have an external-facing IP address** by working with an Approved Scanning Vendor (ASV)* listed on the PCI Security Standards Council's website, PCISecurityStandards.org, under "QSA/ASV."
- **Complete additional system reviews** as needed.
- **Consult your payments processor** for help in ensuring your business is PCI compliant.

RESOURCES

For more information about PCI compliance, visit HeartlandPaymentSystems.com/PCICompliance.

Full information about PCI and the necessary forms are available on the PCI Security Standards Council website, PCISecurityStandards.org.

**403 Labs, an industry-approved QSA and ASV, is Heartland's recommended provider for merchant SAQ and network vulnerability scanning services. Visit 403labs.com for more information on how to get started on PCI DSS validation.*



The Highest Standards | The Most Trusted Transactions

HeartlandPaymentSystems.com

866.941.1HPS (1477)