



# Payment Application Data Security Standard (PA-DSS)

## *Steps for Successful Validation*

igxglobal White Paper  
March 2010  
Version 1.3

## OVERVIEW OF THE PA-DSS

### What is the PA-DSS?

Achieving PA-DSS validation impacts both the sales of your payment application and the reputation of your company. The window of opportunity for selling un-validated payment applications is closing quickly, as specified in the mandates below. If your payment application is on the “known vulnerable payment applications” list published by Visa, many potential customers are already prohibited from purchasing your payment application and may be required to de-certify it. Further, beginning July 1, 2010, acquirers must ensure their merchants, VNP’s and agents use only PA-DSS or PABP compliant applications.


Numerous applications that collect, process and transmit credit cardholder data, called “payment applications”, have played a role in data compromises. Criminals target payment applications because many of them retain certain authentication information (e.g., full track data, card validation code, or PIN bock data) or their implementation inadvertently provides access to customers’ credit cardholder data (e.g., default accounts, incompatibility with antivirus or encryption, insecure remote access).

The Payment Application Data Security Standard (PA-DSS) is a standard designed to help software vendors develop secure payment applications. For purposes of PA-DSS, a “payment application” is defined as an application that stores, processes, or transmits cardholder data as part of authorization or settlement, where the payment applications is sold, distributed, or licensed to third parties.

The goal of PA-DSS is to help software vendors and others develop secure payment applications that do not store prohibited data (e.g., full magnetic stripe, CVV2 or PIN data) and to ensure the payment applications support compliance with the PCI DSS. Formerly known as the Payment Application Best Practices (PABP) under the supervision of the Visa payment card brand, the PA-DSS is now centrally managed by the Payment Card Industry Security Standards Council (PCI SSC).

### What are the Mandates and their Deadlines?

Below are the five mandates impacting payment applications until 2010. They have been driven primarily by Visa and the PCI SCC now supports these requirements.

<b>PA-DSS Mandates</b>	
<p>★ <b>July 1, 2010</b></p> <ul style="list-style-type: none"> <li>Acquirers must ensure that their Merchants, VNP’s, and Agents use <u>only</u> PA-DSS or PABP-compliant applications</li> </ul>	<p><b>January 1, 2008</b></p> <ul style="list-style-type: none"> <li>Newly boarded Merchants must not use known vulnerable payment applications</li> <li>VNP’s and Agents must not certify new payment apps to their platforms that are known vulnerable payment applications</li> </ul>
<p><b>October 1, 2009</b></p> <ul style="list-style-type: none"> <li>VNP’s and Agents must <u>decertify</u> all vulnerable Payment Applications</li> </ul>	<p><b>July 1, 2008</b></p> <ul style="list-style-type: none"> <li>New payment applications that VNP’s and Agents certify to their platforms must be PABP-compliant</li> </ul>
	
<p><b>October 1, 2008</b></p> <ul style="list-style-type: none"> <li>Newly boarded Level 3 and 4 Merchants must use PA-DSS or PABP-compliant applications or be PCI DSS compliant</li> </ul>	
<p>★ Denotes milestone for 2010.</p>	

## VALIDATING YOUR PAYMENT APPLICATION

Success in validating your payment application with the PA-DSS involves understanding the requirements and the validation process. Following is a brief description of the PA-DSS requirements, basic steps for validating your payment application with the PA-DSS, and tips for ensuring success when validating your payment application. Vendors with payment applications that are already PABP-compliant will be grandfathered into the PA-DSS program for a specified time period, based upon the version of the PABP the application was validated against, and should become familiar with this information. Vendors who are starting the process should carefully review this information.

### *What are the PA-DSS Requirements?*

The Payment Application Data Security Standard (PA-DSS) defines fourteen (14) requirements addressing the development of secure payment applications to support PCI DSS compliance. Payment application vendors must address and document compliance with each of the following requirements:

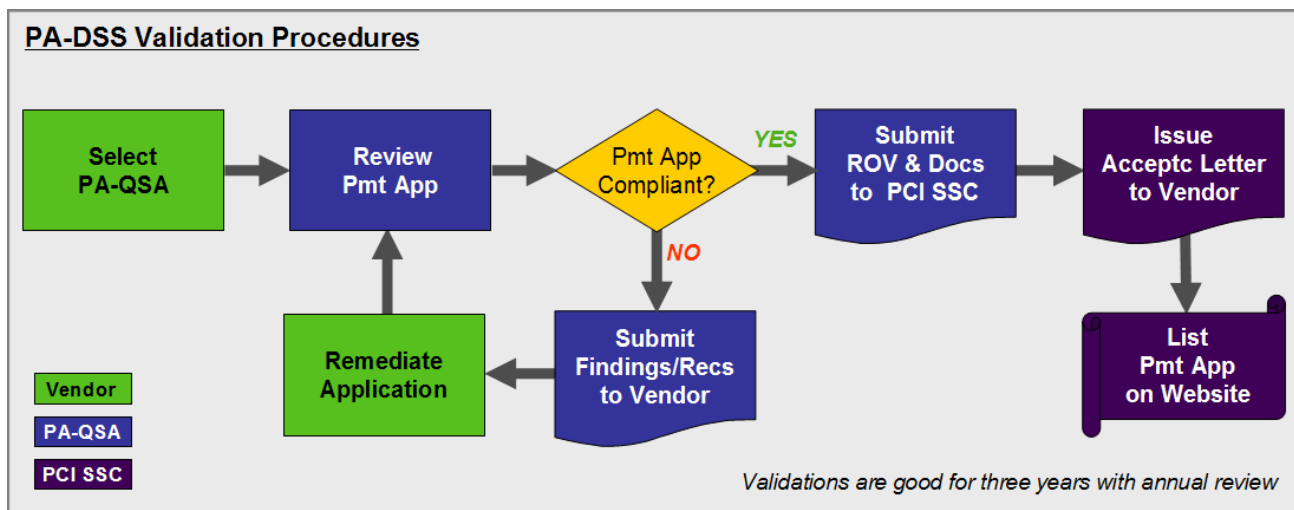
#### **PA-DSS Requirements for Payment Applications**

1. Do not retain full magnetic strip, 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 payment 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 Payment Applications
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

### *What are the Procedures for Validating my Payment Application?*

Five basic steps are involved in validating a payment application to the PA-DSS requirements, as illustrated on the following page. Key players in these steps are the vendor, the Payment Application Qualified Security Assessor (PA-QSA), and the PCI Security Standards Council (PCI DSS).

1. **Vendor Selects a PA-QSA**
2. **PA-QSA reviews the payment application according to the PA-DSS requirements**
  - If the application is non-compliant, the PA-QSA provides the vendor with findings and recommended remediation steps. The application is re-assessed upon completion of remediation.
  - If the application is compliant, the PA-QSA generates the Report on Validation (ROV)
3. **PA-QSA submits the Report on Validation (ROV) and Attestation of Validation to the PCI SSC**
4. **PCI SSC issues an acceptance letter to the vendor**
5. **PCI SSC lists the validated payment application on the PCI SSC website**



### What are My Responsibilities?

Achieving PA-DSS validation of your payment application involves several responsibilities:

- ▶ **Create a PA-DSS compliant application.** The compliance of your application will be assessed and validated by your PA-QSA through both documentation review and laboratory testing;
- ▶ **Create a PA-DSS Implementation Guide.** This requirement, designed to ensure the payment application is implemented in a PCI DSS-compliant manner, is often overlooked. The Implementation Guide is a significant undertaking during the first PA-DSS validation effort, but is straightforward in subsequent validations;
- ▶ **Education.** Customers, resellers and integrators must be educated on how to install and configure the payment application;
- ▶ **Account for Storing Cardholder Data.** Follow PCI DSS requirements if your organization stores, processes or transmits cardholder data; and
- ▶ **Successful Review.** Ensure your application meets PA-DSS requirements by successfully undergoing a PA-DSS review.

### How Can I Increase the Odds of Successfully Validating my Payment Application?

#### 1. Prepare for the Review

Prior to the PA-DSS review, you should become familiar with both PCI DSS and PA-DSS requirements, as the two standards are closely intertwined (visit the PCI SSC's website <https://www.pcisecuritystandards.org> and refer to the end of this whitepaper for free resources). Determine the payment application's readiness for review by performing a "gap" analysis that compares the payment application's functioning and documentation with respect to the PA-DSS requirements. This can be accomplished using in-house resources or by hiring a PA-QSA to complete a preliminary assessment and gap analysis. You should also ensure all appropriate documentation, training materials, and the application's software development life cycle is reviewed. At this point, you can identify issues and remediate them prior to the official validation effort. Remember, if utilizing in-house resources, they should have a solid understanding of both PCI-DSS and PA-DSS requirements.

## 2. Rigorously Vet Potential PA-QSA Vendors

You should interview several potential PA-QSA vendors. Note that your PA-DSS validation must be completed by a company certified by the PCI Security Standards Council and an individual within that company who has successfully completed both the PCI-DSS and PCI-DSS training programs (refer to [https://www.pcisecuritystandards.org/qa\\_asv/find\\_one.shtml](https://www.pcisecuritystandards.org/qa_asv/find_one.shtml) for a list of vendors). Ask potential vendors about the qualifications of the individual PA-QSAs who will be delivering services to you. Request samples of their deliverables and references from other clients. Also assess the compatibility of their styles with your organization; while the PA-DSS requirements are standardized, assessors' styles and temperaments vary surprisingly widely.

## 3. Organize Required Documentation for Your PA-QSA

During the validation process, you must provide the PA-QSA with appropriate documentation and the software, per the PA-DSS requirements. Note that if you do not have this documentation, you may choose to create it yourself or engage a PA-QSA to complete it with you.

Examples of documentation you need to provide include:

- ▶ Documentation that would be provided to customers, reseller, or integrators such as:
  - PA-DSS implementation Guide (refer to the previous page)
  - Software Installation Guide or Instructions
  - Training Materials
  - Payment application operator's manual or instructions
- ▶ Internal documentation that describes the payment application's features and functions
- ▶ The application's version numbering scheme
- ▶ Change control documentation
- ▶ Additional documentation such as data flow diagrams and flowcharts
- ▶ Necessary hardware and software to perform simulated payment transactions

### *What are the Fees for Validating my Payment Application?*

You are responsible for paying for your payment application's PA-DSS validation. All fees and dates related to the PA-QSA's PA-DSS assessment are negotiated between yourself and the PA-QSA, and you pay assessment fees directly to the PA-QSA. Cost factors include the number of software versions to be reviewed, number of supported operating system types (Windows, Unix, MacOS) and your preparedness. The cost of any remediation services is dependent on a pre-compliance review and, therefore, will be specific to individual organizations.

Once your application has been validated as compliant and the PCI SSC has approved your completed Report on Validation (ROV), the PCI SSC requires a fee of \$1,250 for each payment application to be included on the PCI SSC payment application list.

This will also be an annually required fee for including the payment application on the PCI SSC list in subsequent years (please refer to the next page).

## MAINTAINING YOUR PAYMENT APPLICATION'S VALIDATION

### *The Importance of Monitoring*

Compliance validation requirements and enforcement measures are subject to change, so you should closely monitor the requirements of all payment card providers and standards in which you are involved.

### *PA-DSS Revalidation Requirements*

PA-DSS validation is only valid for a three (3) year period, at which point your payment application must undergo a new validation effort by a PA-QSA. Within this three-year period, validation is required by the PCI SSC on an annual basis, which varies according to whether and how your payment application has been updated in the previous year. Specifically there are three scenarios for revalidation:

No Changes are made to the listed application	Minor Changes are made that do not impact PA-DSS Requirements	Major Changes are made that impact PA-DSS requirements
<p>The vendor must prepare an annual Attestation Letter and submit the letter to the PCI SSC. The renewal date of the application will be updated upon receipt of the letter.</p>	<p>The vendor must prepare a "Change Analysis Document" and submit this document to a PA-QSA for review. Once the PSA-QSA is satisfied with the information documented within the "Change Analysis" document and verifies that there is no impact to PA-DSS requirements, the PA-QSA will submit a properly endorsed annual attestation letter along with the Change Analysis document to the PCI SSC. The renewal date of the application will be updated upon receipt of the letter and Change Analysis document and acceptance by the PCI SSC.</p>	<p>The application must undergo a new validation effort by a vendor selected PA-QSA. Once the validation effort has been completed and all required documents submitted to the PCI SSC, the new application will be listed.</p>
<p><b>Note:</b> All PA-DSS validated applications will have an expiration date of <b>three (3) years</b> after a change to the standard. Upon expiration, the application must be validated against the updated standard in order to be considered acceptable for merchants or service providers to use for new deployments.</p>		

As part of the Annual Revalidation process, you will be billed annually by the PCI SSC for each application you wish to have listed as a PA-DSS compliant payment application on their PCI SSC List of Validated Payment Applications. The initial fee required by the PCI SSC for each application to be validated and posted on the List of Validated Payment Applications is \$1,250, with an additional \$500 fee per annum to keep the application posted on the List of Validated Payment Applications. If changes are made to your payment application, associated fees will also be charged by the PCI SSC.

### *Grandfathering and Transitioning of PABP Certified Applications to PA-DSS*

The PCI SSC in coordination with Visa USA has developed a grandfathering and transitioning process for PABP certified applications to PA-DSS. If your Payment Application is currently validated to PABP version 1.3 or 1.4, you can have it listed by the PCI SSC as "Validated according to PA-DSS" for a period of 18 or 24 months, respectively, from its original validation date upon completion of the mandated Transition Procedures. If the application was validated to a pre-PABP 1.3 standard, you can obtain a 12 month extension but your application will not be recommended for new deployments. Note that you should an approved PA-QSA validate your application to PA-DSS before the end of the grandfathered extension period, so your payment application can remain on the approved application list posted by the PCI SSC. If an application is not validated against the PA-DSS standard prior to its expiration date, it will be removed from the list, and merchants or service providers utilizing the application risk their PCI DSS compliance status.

## SOURCES OF INFORMATION ABOUT PA-DSS

A range of free information about PA-DSS compliance is available, including:

- ▶ PCI Standards Council homepage  
(<https://www.pcisecuritystandards.org>)
- ▶ PA-DSS Security Audit Procedures  
([https://www.pcisecuritystandards.org/pdfs/pci\\_pa-dss\\_security\\_audit\\_procedures\\_v1-1.pdf](https://www.pcisecuritystandards.org/pdfs/pci_pa-dss_security_audit_procedures_v1-1.pdf))
- ▶ PA-DSS Frequently Asked Questions  
([https://www.pcisecuritystandards.org/pdfs/pci\\_pa-dss\\_faqs.pdf](https://www.pcisecuritystandards.org/pdfs/pci_pa-dss_faqs.pdf))
- ▶ PCI DSS General Information  
([https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml))
- ▶ List of PCI SSC Certified QSAs  
([https://www.pcisecuritystandards.org/qa\\_asv/find\\_one.shtml](https://www.pcisecuritystandards.org/qa_asv/find_one.shtml))
- ▶ Visa Cardholder Information Security Program – Payment Applications - United States  
([http://usa.visa.com/merchants/risk\\_management/cisp\\_payment\\_applications.html?it=l2/merchants/risk\\_management/cisp\\_service\\_providers.html|Payment%20Applications](http://usa.visa.com/merchants/risk_management/cisp_payment_applications.html?it=l2/merchants/risk_management/cisp_service_providers.html|Payment%20Applications))
- ▶ Visa List of PABP-Validated Payment Applications  
([http://usa.visa.com/download/merchants/validated\\_payment\\_applications.pdf](http://usa.visa.com/download/merchants/validated_payment_applications.pdf))
- ▶ Payment Application Security Mandates Bulletin  
([usa.visa.com/download/merchants/payment\\_application\\_security\\_mandates.pdf](http://usa.visa.com/download/merchants/payment_application_security_mandates.pdf))
- ▶ Visa Account Information Security Program – Europe  
(<http://www.visaeurope.com/aboutvisa/security/ais/resourcesanddownloads.jsp>)
- ▶ Identity Theft Information and Rates – United States  
(<http://www.ustreas.gov>)
- ▶ Fraud Prevention – United Kingdom  
(<http://www.cifas.org.uk>)
- ▶ Fraud Prevention – South Africa  
(<http://www.safps.org.za>)
- ▶ A Chronology of Data Breaches  
(<http://www.privacyrights.org/ar/ChronDataBreaches.htm>)

## APPENDIX: ADDITIONAL PA-DSS INFORMATION

### *To Which Applications does PA-DSS Apply?*

For purposes of PA-DSS, a “payment application” is defined as an application that stores, processes, or transmits cardholder data as part of authorization or settlement, where the payment applications is sold, distributed, or licensed to third parties. This definition applies to hardware terminals as well. The following guide can be used to determine whether PA-DSS applies to a given payment application:

- ▶ PA-DSS applies to payment applications that are typically sold and installed “off the shelf” without much customization by software vendors.
- ▶ PA-DSS applies to payment applications provided in modules, which typically include a “baseline” module and other modules specific to customer types, functions, or customized requests. PA-DSS may only apply to the baseline module if that module is the only one performing payment functions (once confirmed by a PA-QSA). If other modules perform payment functions, PA-DSS applies to those modules as well. Note that it is considered a “best practice” for software vendors to isolate payment functions into a single or small number of baseline modules, reserving other modules for non-payment functions. This best practice (though not a requirement) can limit the number of modules subject to PA-DSS.
- ▶ PA-DSS does NOT apply to a payment application developed for and sold to only one customer (usually a large merchant or service provider) and designed and developed according to customer-provided specifications. This application (which may be referred to as a “bespoke” application) is not considered a PA-DSS application and its compliance will be covered as part of the customer’s normal PCI DSS compliance review.
- ▶ PA-DSS does NOT apply to payment applications developed by merchants and service providers if used only in-house (i.e., not sold, distributed, or licensed to a third party). This in-house developed payment application would be covered as part of the merchant’s or service provider’s PCI DSS compliance.
- ▶ PA- DSS does NOT apply to a hardware terminal only if all of these items are true:
  - The terminal has no connection to any of the merchant’s systems or networks;
  - The terminal only connects to the acquirer or processor;
  - The vendor provides secure remote updates, troubleshooting, access and maintenance; and
  - Sensitive authentication data is never stored post authorization.

Following are examples of applications that are NOT payment applications for purposes of PA-DSS:

- ▶ 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).

### *What is the Relationship Between PABP and PA-DSS?*

Visa developed the Payment Application Best Practices (PABP) program in 2005 to eliminate the storage of prohibited data and to facilitate PCI DSS compliance for merchants and agents. Visa has listed validated payment applications monthly since January 2006 and published a list of vulnerable applications quarterly since April 2007. In 2008, Visa announced that it would transition PABP oversight to the PCI Security Standard Council (PCI SSC). The PCI SSC reviewed the existing PABP standard and has issued a revision to the standard and renamed it to the Payment Application Data Security Standard (PA-DSS).

### *PA-DSS Roles and Responsibilities*

Cardholder data security is a shared responsibility and all participants must do their part to prevent fraud. As such, the PA-DSS has a set of defined roles and responsibilities as shown below:

Payment Brands: The payment brands include American Express, Discover, JCB, MasterCard, and Visa. They are responsible for:

- ▶ Developing compliance programs;
- ▶ Enforcing compliance programs;
- ▶ Defining compliance programs using PA-DSS and listed validated payment applications; and
- ▶ Promoting the use of validated payment applications.

PCI Security Standards Council (PCI SSC): The PCI SSC maintains the PA-DSS and related PCI standards, including PCI-DSS. It is responsible for:

- ▶ Maintaining a centralized repository for PA-DSS Reports of Validation (ROV);
- ▶ Performing QA reviews of PA-DSS ROVs;
- ▶ Listing PA-DSS validated payment applications; and
- ▶ Qualifying and training PA-QSAs.

Software Vendors: Software vendors develop payment applications and sell, distribute, or license these applications to third parties. They are responsible for:

- ▶ Creating PA-DSS compliant applications;
- ▶ Following PCI DSS requirements if the vendor ever stores, processes, or transmits cardholder data; Creating a PA-DSS Implementation Guide;
- ▶ Educating customers, resellers and integrators on how to install and configure the payment application;
- ▶ Ensuring payment applications meet PA-DSS requirements by successfully undergoing a PA-DSS review.

Payment Application-Qualified Security Assessor (PA-QSA): PA-QSAs have been qualified and trained by the PCI SSC to perform PA-DSS reviews. They are responsible for:

- ▶ Performing payment application assessments;
- ▶ Providing opinions regarding payment applications' compliance with PA-DSS requirements;
- ▶ Generating the Report on Validation (ROV), and
- ▶ Submitting the ROV to PCI SSC.

Customers: Customers are the merchants, service providers, or others who buy or receive a third-party payment application. Customers are responsible for:

- ▶ Implementing PA-DSS compliant applications into a PCI DSS compliant environment;
- ▶ Configuring the application according to the PA-DSS Implementation Guide; and
- ▶ Maintaining a PCI compliant status for both the environment and the application.

## ABOUT IGXGLOBAL

### *PA-DSS and PCI DSS Experience*

igxglobal's Threat Mitigation team members have worked with companies having assets ranging from \$250K to over \$7 billion in a wide range of industries ranging from the electronic payment and eCommerce software to the financial, hospitality, retail, medical, and educational fields.

igxglobal, Inc. has been a focused provider of audits and assessments for information security systems since 2000.

- ▶ We are certified world-wide by Visa as a Qualified Payment Application Security Company (PA-QSAC) with staff trained and approved as Qualified Payment Application Security Professionals (PA-QSA's) to complete PA-DSS assessments.
- ▶ We are a certified Payment Card Industry (PCI) Data Security Assessor (approved by Visa USA, Visa International, American Express and the Payment Card Industry) and both a Qualified Security Assessor (QSA) and an Approved Scanning Vendor (ASV) (approved by the PCI Security Standards Council).
- ▶ We are certified in the US, Europe, LAC, and CEMEA regions which allows us to help our clients with their international and US-based locations.

This range of credentials means our staff are trained and certified by leading industry entities to meet our customers' information security assessment and validation needs.

### *Our Mission*

igxglobal provides information technology services and solutions designed to improve the performance, infrastructure and security of our clients' operations.

At igxglobal, we are committed to helping our customers operate their networks with more security, efficiency and reliability. We pledge to understand your business model, your customers, and your expectations in order to provide you with the most viable information technology solution.

With a customer focused approach and a comprehensive life cycle model of solutions, we will be your long term partners in ensuring the performance, infrastructure and security of your information networks.

### *Services and Solutions*

igxglobal's services and solutions provide our clients with: risk analyses to pinpoint and address vulnerabilities and threats; assessments and audits to ensure compliance with regulations; tools to improve performance and strengthen infrastructure; subject matter experts to provide technical expertise and impartial advice; specialists to resource short term services or long term deployments; and information security intelligence to sustain our clients' infrastructure investments. These solutions are systematically delivered in our core practice areas:

- ▶ Threat Mitigation Services
- ▶ Information Technologies
- ▶ Professional Services
- ▶ Security Operations Services

## We Are Here To Help You

**The Threat Mitigation Division of igxglobal, Inc. specializes in bringing you the expertise and knowledge to protect your information assets.**

### **Corporate Headquarters**

50 Inwood Road  
Rocky Hill, CT 06067  
860.513.0112  
888.393.4449  
info@igxglobal.com

### **Threat Mitigation Division**

5710 Ogeechee Road  
Suite 200-304  
Savannah, GA 31405  
912.220-6664  
888.393.4449

### **Metro NJ & NYC Sales and Professional Services**

100 Delawanna Avenue  
Clifton, NJ 07601  
201.498.0555  
888.393.4449

### **UK-EMEA Operations igxglobal Ltd**

33 Throgmorton Street  
Bank, London EC2N 2BR  
United Kingdom  
+44.0.207.156.5065

