Payment Card Industry (PCI)

Payment Application Data Security Standard

Requirements and Security Assessment Procedures

Version 1.2.1
July 2009

Document Changes

Date	Version	Description	Pages
October 1, 2008	*1.2*	*To align content with new PCI DSS v1.2 and to implement minor changes noted since original v1.1.*	
July 2009	*1.2.1*	*Under "Scope of PA-DSS," align content with the* PA-DSS Program Guide, v1.2.1, *to clarify applications to which PA-DSS applies.*	*v, vi*
		Under Laboratory Requirement 6, corrected spelling of "OWASP."	*30*
		In the Attestation of Validation, Part 2a, update Payment Application Functionality to be consistent with the application types listed in the PA-DSS Program Guide, *and clarify annual re-validation procedures in Part 3b.*	*32, 33*

Table of Contents

Introduction

Purpose of This Document

This document is to be used by Payment Application-Qualified Security Assessors (PA-QSAs) conducting payment application reviews, so that software vendors can validate that a payment application complies with the PCI Payment Application Data Security Standard (PA-DSS). This document is also to be used by PA-QSAs as a template to create the Report on Validation.

Relationship between PCI DSS and PA-DSS

The requirements for the Payment Application Data Security Standard (PA-DSS) are derived from the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Security Assessment Procedures*. This document, which can be found at www.pcisecuritystandards.org, details what is required to be PCI DSS compliant (and therefore what a payment application must support to facilitate a customer's PCI DSS compliance).

Traditional PCI Data Security Standard compliance may not apply directly to payment application vendors since most vendors do not store, process, or transmit cardholder data. However, since these payment applications are used by customers to store, process, and transmit cardholder data, and customers are required to be PCI Data Security Standard compliant, payment applications should facilitate, and not prevent, the customers' PCI Data Security Standard compliance. Just a few of the ways payment applications can prevent compliance follow.

1. Storage of magnetic stripe data in the customer's network after authorization;
2. Applications that require customers to disable other features required by the PCI Data Security Standard, like anti-virus software or firewalls, in order to get the payment application to work properly; and
3. Vendor's use of unsecured methods to connect to the application to provide support to the customer.

Secure payment applications, 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, CVV2), PINs and PIN blocks, and the damaging fraud resulting from these breaches.

Scope of PA-DSS

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.

The following guide can be used to determine whether PA-DSS applies to a given payment application:

Note:

All validated payment application products must not be beta versions.

- PA-DSS does apply to payment applications that are typically sold and installed "off the shelf" without much customization by software vendors.
- PA-DSS does apply to payment applications provided in modules, which typically includes a "baseline" module and other modules specific to customer types or functions, or customized per customer request. 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 also 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 payment applications offered by application or service providers only as a service (unless such applications are also sold, licensed, or distributed to third parties) because:

  1) The application is a service offered to customers (typically merchants) and the customers do not have the ability to manage, install, or control the application or its environment;
  2) The application is covered by the application or service provider's own PCI DSS review (this coverage should be confirmed by the customer); and/or
  3) The application is not sold, distributed, or licensed to third parties.

  Examples of these "software as a service" payment applications include:

  1) Those offered by Application Service Providers (ASP) who host a payment application on their site for their customers' use. Note that PA-DSS would apply, however, if the ASP's payment application is also sold to, and implemented on, a third-party site, and the application was not covered by the ASP's PCI DSS review.
  2) Virtual terminal applications that reside on a service providers' site and are used by merchants to enter their payment transactions. Note that PA-DSS would apply if the virtual terminal application has a portion that is distributed to, and implemented on, the merchant's site, and was not covered by the virtual terminal provider's PCI DSS review.
- PA-DSS does NOT apply to non-payment applications that are part of a payment application suite. Such applications (e.g., a fraud-monitoring, scoring or detection application included in a suite) can be, but are not required to be, covered by PA-DSS if the whole suite is assessed together. However, if a payment application is part of a suite that relies on PA-DSS requirements being met by controls in other applications in the suite, a single PA-DSS assessment should be performed for the payment application and all other applications in the

suite upon which it relies. These applications should not be assessed separately from other applications they rely upon since all PA-DSS requirements are not met within a single application.

- PA-DSS does NOT apply to a payment application developed for and sold to only one customer since this application will be covered as part of the customer's normal PCI DSS compliance review. Note that such an application (which may be referred to as a "bespoke" application) is sold to only one customer (usually a large merchant or service provider), and it is designed and developed according to customer-provided specifications.
- PA-DSS does NOT apply to payment applications developed by merchants and service providers if used only in-house (not sold, distributed, or licensed to a third party), since this in-house developed payment application would be covered as part of the merchant's or service provider's normal PCI DSS compliance.

For example, for the last two bullets above, whether the in-house developed or "bespoke" payment application stores prohibited sensitive authentication data or allows complex passwords would be covered as part of the merchant's or service provider's normal PCI DSS compliance efforts and would not require a separate PA-DSS assessment.

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)
- Back-office systems that store cardholder data (for example, for reporting or customer service purposes)

Note:

PCI SSC will ONLY list applications that are payment applications.

The scope of the PA-DSS review should include the following:

- Coverage of all payment application functionality, including but not limited to 1) end-to-end payment functions (authorization and settlement), 2) input and output, 3) error conditions, 4) interfaces and connections to other files, systems, and/or payment applications or application components, 5) all cardholder data flows, 6) encryption mechanisms, and 7) authentication mechanisms.
- Coverage of guidance the payment application vendor is expected to provide to customers and resellers/integrators (see *PA-DSS Implementation Guide* later in this document) to ensure 1) customer knows how to implement the payment application in a PCI DSS-compliant manner and 2) customer is clearly told that certain payment application and environment settings may prohibit their PCI DSS compliance. Note that the payment application vendor may be expected to provide such guidance even when the specific setting 1) cannot be controlled by the payment application vendor once the application is installed by the customer or 2) is the responsibility of the customer, not the payment application vendor.
- Coverage of all selected platforms for the reviewed payment application version (included platforms should be specified)
- Coverage of tools used by or within the payment application to access and/or view cardholder data (reporting tools, logging tools, etc.)

PA-DSS Applicability to Hardware Terminals

Hardware terminals with resident payment applications (also called dumb POS terminals or standalone POS terminals) do not need to undergo a PA-DSS review *if **all** of the following are true*:

- The terminal has no connections to any of the merchant's systems or networks;
- The terminal connects only to the acquirer or processor;
- The payment application vendor provides secure remote 1) updates, 2) troubleshooting, 3) access and 4) maintenance; and
- The following are never stored after authorization: the full contents of any track from the magnetic stripe (that is on the back of a card, in a chip, or elsewhere), card-validation code or value (three- or four-digit number printed on front or back of payment card), PIN or encrypted PIN block**.**

Roles and Responsibilities

There are several stakeholders in the payment application community. Some of these stakeholders have a more direct participation in the PA-DSS assessment process—vendors, PA-QSAs and PCI SSC. Other stakeholders that are not directly involved with the assessment process should be aware of the overall process to facilitate their associated business decisions.

The following defines the roles and responsibilities of the stakeholders in the payment application community. Those stakeholders that are involved in the assessment process have those related responsibilities listed.

Payment Brands

American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. are the payment brands that founded the PCI SSC. These payment brands are responsible for developing and enforcing any programs related to PA-DSS compliance, including, but not limited to, the following:

- Any requirements, mandates, or dates for use of PA-DSS compliant payment applications;
- Any fines or penalties related to use of non-compliant payment applications.

The payment brands may define compliance programs, mandates, dates, etc. using PA-DSS and the validated payment applications listed by PCI SSC. Through these compliance programs, the payment brands promote use of the listed validated payment applications.

Payment Card Industry Security Standards Council (PCI SSC)

PCI SSC is the standards body that maintains the payment card industry standards, including the PCI DSS and PA-DSS. In relation to PA-DSS, PCI SSC:

- Is a centralized repository for PA-DSS Reports of Validation (ROVs)
- Performs Quality Assurance (QA) reviews of PA-DSS ROVs to confirm report consistency and quality
- Lists PA-DSS validated payment applications on the Website.

- Qualifies and trains PA-QSAs to perform PA-DSS reviews
- Maintains and updates the PA-DSS standard and related documentation according to a standards lifecycle management process.

Note that PCI SSC does not approve reports from a validation perspective. The role of the PA-QSA is to document the payment application's compliance to the PA-DSS as of the date of the assessment. Additionally, PCI SSC performs QA to assure that the PA-QSAs accurately and thoroughly document PA-DSS assessments.

Software Vendors

Software vendors ("vendors") develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement, and then sell, distribute, or license these payment applications to third parties (customers or resellers/integrators). Vendors are responsible for:

- Creating PA-DSS compliant payment applications that facilitate and do not prevent their customers' PCI DSS compliance. (The application cannot require an implementation or configuration setting that violates a PCI DSS requirement.);
- Following PCI DSS requirements whenever the vendor stores, processes or transmits cardholder data (for example, during customer troubleshooting);
- Creating a *PA-DSS Implementation Guide*, specific to each payment application, according to the requirements in this document;
- Educating customers, resellers, and integrators on how to install and configure the payment applications in a PCI DSS-compliant manner;
- Ensuring payment applications meet PA-DSS by successfully passing a PA-DSS review as specified in this document.

PA-QSAs

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.*

PA-QSAs are responsible for:

- Performing assessments on payment applications in accordance with the Security Assessment Procedures and the PA-QSA Validation Requirements
- Providing an opinion regarding whether the payment application meets PA-DSS requirements
- Providing adequate documentation within the ROV to demonstrate the payment application's compliance to the PA-DSS
- Submitting the ROV to PCI SSC, along with the Attestation of Validation (signed by both PA-QSA and vendor)
- Maintaining an internal quality assurance process for their PA-QSA efforts

It is the PA-QSA's responsibility to state whether the payment application has achieved compliance. PCI SSC does not approve ROVs from a technical compliance perspective, but performs QA reviews on the ROVs to assure that the reports adequately document the demonstration of compliance.

Resellers and Integrators

Resellers and integrators are those entities that sell, install, and/or service payment applications on behalf of software vendors or others. Resellers and integrators are responsible for:

- Implementing a PA-DSS-compliant payment application into a PCI DSS-compliant environment (or instructing the merchant to do so);
- Configuring the payment application (where configuration options are provided) according to the *PA-DSS Implementation Guide* provided by the vendor;
- Configuring the payment application (or instructing the merchant to do so) in a PCI DSS-compliant manner;
- Servicing the payment applications (for example, troubleshooting, delivering remote updates, and providing remote support) according to the *PA-DSS Implementation Guide* and PCI DSS.

Resellers and integrators do not submit payment applications for assessment. Products can only be submitted by the vendor.

Customers

Customers are merchants, service providers, or others who buy or receive a third-party payment application to store, process, or transmit cardholder data as part of authorizing or settling of payment transactions. Customers who want to use applications that are compliant with PA-DSS are responsible for:

- Implementing a PA-DSS-compliant payment application into a PCI DSS-compliant environment;
- Configuring the payment application (where configuration options are provided) according to the *PA-DSS Implementation Guide* provided by the vendor;
- Configuring the payment application in a PCI DSS-compliant manner;
- Maintaining the PCI DSS-compliant status for both the environment and the payment application configuration.

Note:

A PA-DSS compliant payment application alone is no guarantee of PCI DSS compliance.

PA-DSS Implementation Guide

Validated payment applications must be capable of being implemented in a PCI DSS-compliant manner. Software vendors are required to provide a *PA-DSS Implementation Guide* to instruct their customers and resellers/integrators on secure product implementation, to document the secure configuration specifics mentioned throughout this document, and to clearly delineate vendor, reseller/integrator, and customer responsibilities for meeting PCI DSS requirements. It should detail how the customer and/or reseller/integrator should enable security settings within the customer's network. For example, the *PA-DSS Implementation Guide* should cover responsibilities and basic features of PCI DSS password security even if this is not controlled by the payment application, so that the customer or reseller/integrator understands how to implement secure passwords for PCI DSS compliance.

Payment applications, when implemented according to the *PA-DSS Implementation Guide*, and when implemented into a PCI DSS-compliant environment, should facilitate and support customers' PCI DSS compliance.

Refer to "Appendix A: Summary of Contents for the *PA-DSS Implementation Guide*" for a comparison of responsibilities for implementing the controls specified in the *PA-DSS Implementation Guide*.

Payment Application Qualified Security Assessor (PA-QSA) Requirements

- Only Payment Application Qualified Security Assessors (PA-QSAs) employed by Qualified Security Assessor (QSA) companies are allowed to perform PA-DSS assessments. Please see the Qualified Security Assessor list at www.pcisecuritystandards.org for a list of companies qualified to perform PA-DSS assessments.
- The PA-QSA must utilize the testing procedures documented in this Payment Application Data Security Standard document.

Testing Laboratory

- The PA-QSA must have access to a laboratory where the validation process is to occur. This laboratory should be able to simulate real-world use of the payment application.
- Please refer to *Appendix B: Confirmation of Testing Laboratory Configuration Specific to PA-DSS Assessment* in this document for detailed requirements for the laboratory and related laboratory processes.
- PA-QSA must complete and submit Appendix B, completed for the specific laboratory used for the payment application under review, as part of the completed PA-DSS report.

PCI DSS Applicability Information

(Excerpted from PCI DSS v1.2)

The following table from the *Payment Card Industry Data Security Standard* (PCI DSS) illustrates commonly used elements of cardholder data and sensitive authentication data, whether **storage** of that data is permitted or prohibited, and whether this data needs to be **protected**. This table is not meant to be exhaustive; its sole purpose is to illustrate the different type of requirements that apply to each data element.

The Primary Account Number (PAN) is the defining factor in the applicability of PCI DSS requirements and PA-DSS. If PAN is not stored, processed, or transmitted, PCI DSS and PA-DSS do not apply.

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3, 4
Cardholder Data	Primary Account Number	Yes	Yes	Yes
	Cardholder Name [1]	Yes	Yes [1]	No
	Service Code [1]	Yes	Yes [1]	No
	Expiration Date [1]	Yes	Yes [1]	No
Sensitive Authentication Data [2]	Full Magnetic Stripe Data[3]	No	N/A	N/A
	CAV2/CID/CVC2/CVV2	No	N/A	N/A
	PIN/PIN Block	No	N/A	N/A

[1] *These data elements must be protected if stored in conjunction with the PAN. This protection should be per PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS; however, does not apply if PANs are not stored, processed, or transmitted.*

[2] *Do not store sensitive authentication data after authorization (even if encrypted).*

[3] *Full track data from the magnetic stripe, magnetic-stripe image on the chip, or elsewhere.*

Instructions and Content for Report on Validation

This document is to be used by PA-QSAs as the template for creating the Report on Validation. All PA-QSAs must follow instructions in this document for report content and format when completing a Report on Validation.

The Report on Validation should contain the following information as a preface to the detailed Requirements and Security Assessment Procedures:

1. **Description of Scope of Review**
   - Describe scope of review coverage, per the Scope of PA-DSS section above
   - Timeframe of validation
   - PA-DSS version used for the assessment
   - List of documentation reviewed
2. **Executive Summary**

   Include the following:
   - Product Name
   - Product Version and related platforms covered
   - List of resellers and/or integrators for this product
   - Operating system(s) with which the payment application was tested
   - Database software used or supported by the payment application
   - Brief description of the payment application/family of products (2-3 sentences)
   - Network diagram of a typical implementation of the payment application (not necessarily a specific implementation at a customer's site) that includes, at high level:
     - Connections into and out of a customer's network
     - Components within the customer's network, including POS devices, systems, databases, and web servers as applicable
     - Other necessary payment application/components, as applicable
   - Description or diagram of each piece of the communication link, including (1) LAN, WAN or Internet, (2) host to host software communication, and (3) within host where software is deployed (for example, how two different processes communicate with each other on the same host)
   - A dataflow diagram that shows all flows of cardholder data, including authorization, capture, settlement, and chargeback flows as applicable

- Brief description of files and tables that store cardholder data, supported by an inventory created (or obtained from the software vendor) and retained by the PA-QSA in the work papers—this inventory should include, for each cardholder data store (file, table, etc.):
  - List of all elements of stored cardholder data
  - How data store is secured
  - How access to data store is logged
- List all payment application related software components, including third-party software requirements and dependencies
- Description of payment application's end to end authentication methods, including application authentication mechanism, authentication database, and security of data storage
- Description of role of payment application in a typical implementation and what other types of payment applications are necessary for a full payment implementation
- Description of the typical customer that this product is sold to (for example, large, small, whether industry-specific, Internet, brick-and-mortar) and vendor's customer's base (for example, market segment, big customer names).
- Definition of vendor's versioning methodology, to describe/illustrate how vendor indicates major and minor version changes via their version numbers, and to define what types of changes the vendor includes in major and minor version changes.

Note that *Appendix B: Confirmation of Testing Laboratory Configuration Specific to PA-DSS Assessment* must also be completed and submitted with the completed PA-DSS report.

3. Findings and Observations

- All PA-QSAs must use the following template to provide detailed report descriptions and findings
- Describe tests performed other than those included in the testing procedures column.

4. Contact Information and Report Date

- Software vendor contact information (include URL, phone number, and e-mail address)
- PA-QSA contact information (include name, phone number and e-mail address)
- PA-QSA Quality Assurance (QA) primary contact information (include primary QA contact's name, phone number and e-mail address)
- Date of report

PA-DSS Completion Steps

This document contains the Requirements and Security Assessment Procedures table, as well as *Appendix B: Confirmation of Testing Laboratory Configuration Specific to PA-DSS Assessment* and *Appendix C: Attestation of Validation*. The Requirements and Security Assessment Procedures detail the procedures that must be performed by the PA-QSA. The *Appendix B: Confirmation of Testing Laboratory Configuration Specific to PA-DSS Assessment* must be completed by the PA-QSA to confirm the status and capabilities of the testing laboratory used to conduct this PA-DSS assessment. The *Appendix C: Attestation of Validation* is for the PA-QSA and software vendor to complete and sign after completion of the Report on Validation.

The PA-QSA must perform the following steps:

1. Complete the Report on Validation using this document as a template:
    a. Complete the preface for the Report on Validation, in accordance with the section entitled "Instructions and Content for Report on Validation"
    b. Complete and document all steps detailed in the Requirements and Security Assessment Procedures, including brief descriptions of controls observed in the "In Place" column, and noting any comments. *Please note that a report with any "Not in Place" opinions should not be submitted to PCI SSC until all items are noted as "In Place."*
2. Complete *Appendix B: Confirmation of Testing Laboratory Configuration Specific to PA-DSS Assessment.*
3. Complete and sign *Appendix C: Attestation of Validation* (both PA-QSA and software vendor).
4. After completion, submit all of the above documents to PCI SSC according to the *PA-DSS Program Guide.*

PA-DSS Program Guide

Please refer to the *PA-DSS Program Guide* for information about PA-DSS program management, including the following topics:

- PA-DSS report submission and acceptance processes
- Annual renewal process for payment applications included on the List of PA-DSS Validated Applications
- Transition of PABP-validated applications to the List of PA-DSS Validated Payment Applications
- Notification responsibilities in the event a listed payment application is determined to be at fault in a compromise.

PCI SSC reserves the right to require revalidation due to significant changes to the Payment Application Data Security Standard and/or due to specifically identified vulnerabilities in a listed payment application.

PA-DSS Requirements and Security Assessment Procedures

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
1. Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2), or PIN block data				
1.1 Do not store sensitive authentication data after authorization (even if encrypted): Sensitive authentication data includes the data as cited in the following Requirements 1.1.1 through 1.1.3. ***PCI Data Security Standard Requirement 3.2*** *Note: By prohibiting storage of sensitive authentication data after authorization, the assumption is that the transaction has completed the authorization process and the customer has received the final transaction approval. After authorization has completed, this sensitive authentication data cannot be stored.*	**1.1** If sensitive authentication data (see 1.1.1–1.1.3 below) is stored prior to authorization and then deleted, obtain and review methodology for deleting the data to determine that the data is unrecoverable. For each item of sensitive authentication data below, perform the following steps after completing numerous test transactions that simulate all functions of the payment application, to include generation of error conditions and log entries.			

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
1.1.1 After authorization, do not store the full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. *In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* ▪ *The accountholder's name,* ▪ *Primary account number (PAN),* ▪ *Expiration date, and* ▪ *Service code* *To minimize risk, store only those data elements needed for business.* *Note: See* PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms *for additional information.* ***PCI Data Security Standard Requirement 3.2.1***	**1.1.1** Use forensic tools and/or methods (commercial tools, scripts, etc.)[4] to examine all output created by the payment application and verify that the full contents of any track from the magnetic stripe on the back of the card are not stored after authorization. Include the following types of files (as well as any other output generated by the payment application): ▪ Incoming transaction data ▪ All logs (for example, transaction, history, debugging, error) ▪ History files ▪ Trace files ▪ Non-volatile memory, including non-volatile cache ▪ Database schemas ▪ Database contents			

[4] Forensic tool or method: A tool or method for uncovering, analyzing and presenting forensic data, which provides a robust way to authenticate, search, and recover computer evidence rapidly and thoroughly. In the case of forensic tools or methods used by PA-QSAs, these tools or methods should accurately locate any sensitive authentication data written by the payment application. These tools may be commercial, open-source, or developed in-house by the PA-QSA.

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
1.1.2 After authorization, do not store the card-validation value or code (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions. *Note: See* PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms *for additional information.* ***PCI Data Security Standard Requirement 3.2.2***	**1.1.2** Use forensic tools and/or methods (commercial tools, scripts, etc.)[5] to examine all output created by the payment application and verify that the three-digit or four-digit card-validation code printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored after authorization. Include the following types of files (as well as any other output generated by the payment application): ▪ Incoming transaction data ▪ All logs (for example, transaction, history, debugging, error) ▪ History files ▪ Trace files ▪ Non-volatile memory, including non-volatile cache ▪ Database schemas ▪ Database contents			
1.1.3 After authorization, do not store the personal identification number (PIN) or the encrypted PIN block. *Note: See* PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms *for additional information.* ***PCI Data Security Standard Requirement 3.2.3***	**1.1.3** Use forensic tools and/or methods (commercial tools, scripts, etc.)[5] to examine all output created by the payment application, and verify that PINs and encrypted PIN blocks are not stored after authorization. Include the following types of files (as well as any other output generated by the payment application). ▪ Incoming transaction data ▪ All logs (for example, transaction, history, debugging, error) ▪ History files ▪ Trace files ▪ Non-volatile memory, including non-volatile cache ▪ Database schemas ▪ Database contents			

[5] Forensic tool or method: A tool or method for uncovering, analyzing and presenting forensic data, which provides a robust way to authenticate, search, and recover computer evidence rapidly and thoroughly. In the case of forensic tools or methods used by PA-QSAs, these tools or methods should accurately locate any sensitive authentication data written by the payment application. These tools may be commercial, open-source, or developed in-house by the PA-QSA.

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
1.1.4 Securely delete any magnetic stripe data, card validation values or codes, and PINs or PIN block data stored by previous versions of the payment application, in accordance with industry-accepted standards for secure deletion, as defined, for example by the list of approved products maintained by the National Security Agency, or by other State or National standards or regulations. ***PCI Data Security Standard Requirement 3.2*** *Note: This requirement only applies if previous versions of the payment application stored sensitive authentication data.*	**1.1.4.a** Review the *PA-DSS Implementation Guide* prepared by the vendor and verify the documentation includes the following instructions for customers and resellers/integrators: ▪ That historical data must be removed (magnetic stripe data, card validation codes, PINs, or PIN blocks stored by previous versions of the payment application) ▪ How to remove historical data ▪ That such removal is absolutely necessary for PCI DSS compliance			
	1.1.4.b Verify the vendor provides a secure wipe tool or procedure to remove the data.			
	1.1.4.c Verify, through the use of forensic tools and/or methods, that the secure wipe tool or procedure provided by vendor securely removes the data, in accordance with industry-accepted standards for secure deletion of data.			
1.1.5 Securely delete any sensitive authentication data (pre-authorization data) used for debugging or troubleshooting purposes from log files, debugging files, and other data sources received from customers, to ensure that magnetic stripe data, card validation codes or values, and PINs or PIN block data are not stored on software vendor systems. These data sources must be collected in limited amounts and only when necessary to resolve a problem, encrypted while stored, and deleted immediately after use. ***PCI Data Security Standard Requirement 3.2***	**1.1.5.a** Examine the software vendor's procedures for troubleshooting customers' problems and verify the procedures include: ▪ Collection of sensitive authentication data only when needed to solve a specific problem ▪ Storage of such data in a specific, known location with limited access ▪ Collection of only a limited amount of data needed to solve a specific problem ▪ Encryption of sensitive authentication data while stored ▪ Secure deletion of such data immediately after use			
	1.1.5.b Select a sample of recent troubleshooting requests from customers, and verify each event followed the procedure examined at 1.1.5.a.			

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
	1.1.5.c Review the *PA-DSS Implementation Guide* prepared by the vendor and verify the documentation includes the following instructions for customers and resellers/integrators: ▪ Collect sensitive authentication only when needed to solve a specific problem. ▪ Store such data only in specific, known locations with limited access. ▪ Collect only the limited amount of data needed to solve a specific problem. ▪ Encrypt sensitive authentication data while stored. ▪ Securely delete such data immediately after use.			
2. Protect stored cardholder data				
2.1 Software vendor must provide guidance to customers regarding purging of cardholder data after expiration of customer-defined retention period. ***PCI Data Security Standard Requirement 3.1***	**2.1.a** Review the *PA-DSS Implementation Guide* prepared by the vendor and verify the documentation includes the following guidance for customers and resellers/integrators: ▪ That cardholder data exceeding the customer-defined retention period must be purged ▪ A list of all locations where the payment application stores cardholder data (so that customer knows the locations of data that needs to be deleted)			
2.2 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). *Notes:* ▪ *This requirement does not apply to those employees and other parties with a legitimate business need to see full PAN;* ▪ *This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts.* ***PCI Data Security Standard Requirement 3.3***	**2.2** Review displays of credit card data, including but not limited to POS devices, screens, logs, and receipts, to determine that credit card numbers are masked when displaying cardholder data, except for those with a legitimate business need to see full credit card numbers.			

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
2.3 Render PAN, at a minimum, unreadable anywhere it is stored, (including data on portable digital media, backup media, and in logs) by using any of the following approaches: ▪ One-way hashes based on strong cryptography ▪ Truncation ▪ Index tokens and pads (pads must be securely stored) ▪ Strong cryptography with associated key management processes and procedures. The MINIMUM account information that must be rendered unreadable is the PAN. ***PCI Data Security Standard Requirement 3.4*** *The PAN must be rendered unreadable anywhere it is stored, even outside the payment application.* *Note: "Strong cryptography" is defined in the* PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms.	**2.3.a** Verify that the PAN is rendered unreadable anywhere it is stored, in accordance with PCI DSS Requirement 3.4.			
	2.3.b If the software vendor stores the PAN for any reason (for example, because log files, debugging files, and other data sources are received from customers for debugging or troubleshooting purposes), verify that the PAN is rendered unreadable in accordance with PCI DSS Requirement 3.4.			
2.4 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts. ***PCI Data Security Standard Requirement 3.4.1***	**2.4** If disk encryption is used, verify that it is implemented in accordance with PCI DSS Requirements 3.4.1.a through 3.4.1.c.			
2.5 Payment application must protect cryptographic keys used for encryption of cardholder data against disclosure and misuse. ***PCI Data Security Standard Requirement 3.5***	**2.5** Verify the payment application protects keys against disclosure and misuse, per PCI DSS Requirement 3.5.1 and 3.5.2.			
2.6 Payment application must implement key management processes and procedures for cryptographic keys used for encryption of cardholder data. ***PCI Data Security Standard Requirement 3.6***	**2.6** Verify the payment application implements key-management techniques for keys, per PCI DSS Requirements 3.6.1 through 3.6.8.			

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
2.7 Securely delete any cryptographic key material or cryptogram stored by previous versions of the payment application, in accordance with industry-accepted standards for secure deletion, as defined, for example the list of approved products maintained by the National Security Agency, or by other State or National standards or regulations. These are cryptographic keys used to encrypt or verify cardholder data. ***PCI Data Security Standard Requirement 3.6*** *Note: This requirement only applies if previous versions of the payment application used cryptographic key materials or cryptograms to encrypt cardholder data.*	**2.7.a** Review the *PA-DSS Implementation Guide* prepared by the vendor and verify the documentation includes the following instructions for customers and resellers/integrators: ▪ That cryptographic material must be removed ▪ How to remove cryptographic material ▪ That such removal is absolutely necessary for PCI DSS compliance ▪ How to re-encrypt historic data with new keys			
	2.7.b Verify vendor provides a secure wipe tool or procedure to remove cryptographic material.			
	2.7.c Verify, through use of forensic tools and/or methods, that the secure wipe tool or procedure securely removes the cryptographic material, in accordance with industry-accepted standards for secure deletion of data.			
3. Provide secure authentication features				
3.1 The "out of the box" installation of the payment application in place at the completion of the installation process, must facilitate use of unique user IDs and secure authentication (defined at PCI DSS Requirements 8.1, 8.2, and 8.5.8–8.5.15) for all administrative access and for all access to cardholder data. ***PCI Data Security Standard Requirements 8.1, 8.2, and 8.5.8–8.5.15***	**3.1.a** Test the payment application to verify that unique user IDs and secure authentication are required for all administrative access and for all access to cardholder data, in accordance with PCI DSS Requirements 8.1, 8.2, and 8.5.8–8.5.15.			
	3.1.b Test the payment application to verify the payment application does not use (or require the use of) default administrative accounts for other necessary software (for example, the payment application must not use the administrative account for database software).			

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
Note: These password controls are not intended to apply to employees who only have access to one card number at a time to facilitate a single transaction. These controls are applicable for access by employees with administrative capabilities, for access to servers with cardholder data, and for access controlled by the payment application. *This requirement applies to the payment application and all associated tools used to view or access cardholder data.*	**3.1.c** Examine *PA-DSS Implementation Guide* created by vendor to verify the following: ▪ Customers and resellers/integrators are advised against using default administrative accounts for payment application logins (for example, don't use the "sa" account for payment application access to the database). ▪ Customers and resellers/integrators are advised to assign secure authentication to these default accounts (even if they won't be used), and then disable or do not use the accounts. ▪ Customers and resellers/integrators are advised to assign secure authentication for payment applications and systems whenever possible. ▪ Customers and resellers/integrators are advised how to create PCI DSS-compliant secure authentication to access the payment application, per PCI DSS Requirements 8.5.8 through 8.5.15 ▪ Customers and resellers/integrators are advised that changing "out of the box" installation settings for unique user IDs and secure authentication will result in non-compliance with PCI DSS.			
3.2 Access to PCs, servers, and databases with payment applications must require a unique user ID and secure authentication. ***PCI Data Security Standard Requirements 8.1 and 8.2***	**3.2** Examine *PA-DSS Implementation Guide* created by vendor to verify customers and resellers/integrators are strongly advised to control access, via unique user ID and PCI DSS-compliant secure authentication, to any PCs, servers, and databases with payment applications and cardholder data.			
3.3 Render payment application passwords unreadable during transmission and storage, using strong cryptography based on approved standards *Note: "Strong cryptography" is defined in* PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms. ***PCI Data Security Standard Requirement 8.4***	**3.3** Examine payment application password files during storage and transmission to verify that passwords are unreadable at all times.			

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
4. Log payment application activity				
4.1 At the completion of the installation process, the "out of the box" default installation of the payment application must log all user access (especially users with administrative privileges), and be able to link all activities to individual users. ***PCI Data Security Standard Requirement 10.1***	**4.1** Examine payment application settings to verify that payment application audit trails are automatically enabled or are available to be enabled by customers.			
4.2 Payment application must implement an automated audit trail to track and monitor access. ***PCI Data Security Standard Requirements 10.2 and 10.3***	**4.2.a** Examine payment application log parameters and verify that logs contain the data required in PCI DSS Requirements 10.2.1 through 10.2.7 and 10.3.1 through 10.3.6.			
	4.2.b If payment application log settings are configurable by the customer and resellers/integrators, or customers or resellers/integrators are responsible for implementing logging, examine *PA-DSS Implementation Guide* prepared by the vendor to verify the following information is included: ▪ How to set PCI DSS-compliant log settings, per PCI DSS Requirements 10.2.1 through 10.2.7 and 10.3.1 through 10.3.6 ▪ That disabling of the logs should not be done and will result in non-compliance with PCI DSS			

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
5. Develop secure payment applications				
5.1 Develop all payment applications in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices and incorporate information security throughout the software development life cycle. These processes must include the following: ***PCI Data Security Standard Requirement 6.3***	**5.1** Obtain and examine written software development processes to verify that they are based on industry standards, that security is included throughout the life cycle, and that software applications are developed in accordance with PCI DSS. From an examination of written software development processes, interviews of software developers, and examination of relevant data (network configuration documentation, production and test data, etc.), verify that:			
5.1.1 Testing of all security patches and system and software configuration changes before deployment, including but not limited to testing for the following.	**5.1.1** All security patches and system and software changes are tested before being deployed, including but not limited to testing for the following.			
5.1.1.1 Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)	**5.1.1.1** Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)			
5.1.1.2 Validation of proper error handling	**5.1.1.2** Validation of proper error handling			
5.1.1.3 Validation of secure cryptographic storage	**5.1.1.3** Validation of secure cryptographic storage			
5.1.1.4 Validation of secure communications	**5.1.1.4** Validation of secure communications			
5.1.1.5 Validation of proper role-based access control (RBAC)	**5.1.1.5** Validation of proper role-based access control (RBAC)			
5.1.2 Separate development/test, and production environments	**5.1.2** The test/development environments are separate from the production environment, with access control in place to enforce the separation.			
5.1.3 Separation of duties between development/test, and production environments	**5.1.3** There is a separation of duties between personnel assigned to the development/test environments and those assigned to the production environment.			

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
5.1.4 Live PANs are not used for testing or development.	**5.1.4** Live PANs are not used for testing and development, or are sanitized before use.			
5.1.5 Removal of test data and accounts before production systems become active	**5.1.5** Test data and accounts are removed before a production system becomes active.			
5.1.6 Removal of custom payment application accounts, user IDs, and passwords before payment applications are released to customers	**5.1.6** Custom payment application accounts, user IDs, and passwords are removed before payment application is released to customers.			
5.1.7 Review of payment application code prior to release to customers after any significant change, to identify any potential coding vulnerability. *Note: This requirement for code reviews applies to all payment application components (both internal and public-facing web applications), as part of the system development life cycle required by PA-DSS Requirement 5.1 and PCI DSS Requirement 6.3. Code reviews can be conducted by knowledgeable internal personnel or third parties.*	**5.1.7.a** Confirm the vendor performs code reviews for all application code changes for *internal applications* (either using manual or automated processes), as follows: ▪ Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. ▪ Appropriate corrections are implemented prior to release. ▪ Code review results are reviewed and approved by management prior to release.			
	5.1.7.b Confirm the vendor performs code reviews for all application code changes for *web applications* (using either manual or automated processes) as follows: ▪ Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. ▪ Code reviews ensure code is developed according to secure coding guidelines such as the *Open Web Security Project Guide.* (See PA-DSS Requirement 5.2 and PCI DSS Requirement 6.5.) ▪ Appropriate corrections are implemented prior to release. ▪ Code review results are reviewed and approved by management prior to release.			

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
5.2 Develop all web payment applications (internal and external, and including web administrative access to product) based on secure coding guidelines such as the *Open Web Application Security Project Guide*. Cover prevention of common coding vulnerabilities in software development processes, to include: *Note: The vulnerabilities listed in PA-DSS Requirements 5.2.1 through 5.2.10 and in PCI DSS at 6.5.1 through 6.5.10 were current in the OWASP guide when PCI DSS v1.2 was published. However, if and when the OWASP guide is updated, the current version must be used for these requirements.* ***PCI Data Security Standard Requirement 6.5***	**5.2.a** Obtain and review software development processes for any web-based payment applications (internal and external, and including web-administrative access to product). Verify the process includes training in secure coding techniques for developers, and is based on guidance such as the OWASP guide (http://www.owasp.org). Interview a sample of developers and obtain evidence that they are knowledgeable in secure coding techniques.			
	5.2.b For web payment applications included in review, verify that the payment applications are not vulnerable to common coding vulnerabilities by performing manual or automated penetration testing that specifically attempts to exploit each of the following:			
5.2.1 Cross-site scripting (XSS).	**5.2.1** Cross-site scripting (XSS) (Validate all parameters before inclusion.)			
5.2.2 Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws, as well as other injection flaws.	**5.2.2** Injection flaws, particularly SQL injection (Validate input to verify user data cannot modify meaning of commands and queries.)			
5.2.3 Malicious file execution	**5.2.3** Malicious file execution (Validate input to verify application does not accept filenames or files from users.)			
5.2.4 Insecure direct object references.	**5.2.4** Insecure direct object references (Do not expose internal object references to users.)			
5.2.5 Cross-site request forgery (CSRF).	**5.2.5** Cross-site request forgery (CSRF) (Do not rely on authorization credentials and tokens automatically submitted by browsers.)			
5.2.6 Information leakage and improper error handling	**5.2.6** Information leakage and improper error handling (Do not leak information via error messages or other means.)			
5.2.7 Broken authentication and session management	**5.2.7** Broken authentication and session management (Properly authenticate users and protect account credentials and session tokens.)			

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
5.2.8 Insecure cryptographic storage	**5.2.8** Insecure cryptographic storage (Prevent cryptographic flaws.)			
5.2.9 Insecure communications	**5.2.9** Insecure communications (Properly encrypt all authenticated and sensitive communications.)			
5.2.10 Failure to restrict URL access.	**5.2.10** Failure to restrict URL access (Consistently enforce access control in presentation layer and business logic for all URLs.)			
5.3 Software vendor must follow change control procedures for all product software configuration changes. The procedures must include the following: ***PCI Data Security Standard Requirement 6.4***	**5.3.a** Obtain and examine the vendor's change-control procedures for software modifications, and verify that the procedures require items 5.3.1–5.3.4 below.			
	5.3.b Examine recent payment application changes, and trace those changes back to related change control documentation. Verify that, for each change examined, the following was documented according to the change control procedures:			
5.3.1 Documentation of impact	**5.3.1** Verify that documentation of customer impact is included in the change control documentation for each change.			
5.3.2 Management sign-off by appropriate parties	**5.3.2** Verify that management sign-off by appropriate parties is present for each change.			
5.3.3 Testing of operational functionality	**5.3.3** Verify that operational functionality testing was performed for each change.			
5.3.4 Back-out or product de-installation procedures	**5.3.4** Verify that back-out or product de-installation procedures are prepared for each change.			
5.4 The payment application must not use or require use of unnecessary and insecure services and protocols (for example, NetBIOS, file-sharing, Telnet, unencrypted FTP, etc.). ***PCI Data Security Standard Requirement 2.2.2***	**5.4** Examine system services, daemons, and protocols enabled or required by the payment application. Verify that unnecessary and insecure services or protocols are not enabled by default or required by the payment application (for example, FTP is not enabled, or is encrypted via SSH or other technology).			

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
6. Protect wireless transmissions				
6.1 For payment applications using wireless technology, the wireless technology must be implemented securely. ***PCI Data Security Standard Requirements 1.2.3 & 2.1.1***	**6.1.a** For payment applications developed by the vendor using wireless technology, and other wireless applications bundled with the payment application, verify that the wireless applications do not use vendor default settings and are configured in accordance with PCI Data Security Standard Requirement 2.1.1.			
	6.1.b Examine the *PA-DSS Implementation Guide* prepared by the vendor to verify that customers and resellers/integrators are instructed, if wireless is used, to install a firewall per PCI DSS Requirement 1.2.3.			
6.2 For payment applications using wireless technology, payment application must facilitate use of industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. Payment applications using wireless technology must facilitate the following regarding use of WEP: ▪ *For new wireless implementations, it is prohibited to implement WEP after March 31, 2009.* ▪ *For current wireless implementations, it is prohibited to use WEP after June 30, 2010.* ***PCI Data Security Standard Requirement 4.1.1***	**6.2.a** For payment applications developed by the vendor using wireless technology, and other wireless applications bundled with the vendor application, verify that industry best practices (for example, IEEE 802,11.i) were used to include or make available strong encryption for authentication and transmission, in accordance with PCI DSS Requirement 4.1.1.			
	6.2.b If customers could implement the payment application into a wireless environment, examine *PA-DSS Implementation Guide* prepared by vendor to verify customers and resellers/integrators are instructed on PCI DSS-compliant wireless settings, per PCI DSS Requirements 1.2.3, 2.1.1 and 4.1.1.			

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
7. Test payment applications to address vulnerabilities				
7.1 Software vendors must establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet) and to test their payment applications for vulnerabilities. Any underlying software or systems that are provided with or required by the payment application (for example, web servers, 3rd-party libraries and programs) must be included in this process. ***PCI Data Security Standard Requirement 6.2***	**7.1.a** Obtain and examine processes to identify new vulnerabilities and to test payment applications for new vulnerabilities. Verify the processes include: ▪ Using outside sources for security vulnerability information ▪ Testing of payment applications for new vulnerabilities			
	7.1.b Verify that processes to identify new vulnerabilities and implement corrections into payment application apply to all software provided with or required by the payment application (for example, web servers, third-party libraries and programs).			
7.2 Software vendors must establish a process for timely development and deployment of security patches and upgrades, which includes delivery of updates and patches in a secure manner with a known chain-of-trust, and maintenance of the integrity of patch and update code during delivery and deployment.	**7.2.a** Obtain and examine processes to develop and deploy security patches and upgrades for software. Verify the processes include: ▪ Timely development and deployment of patches to customers ▪ Delivery of patches and updates in a secure manner with a known chain-of-trust ▪ Delivery of patches and updates in a manner that maintains the integrity of the deliverable ▪ Integrity testing of the patch or update by the target system prior to installation			
	7.2.b To verify that the integrity of patch and update code is maintained, run the update process with arbitrary code and determine that the system will not allow the update to occur.			

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
8. Facilitate secure network implementation				
8.1 The payment application must be able to be implemented into a secure network environment. Application must not interfere with use of devices, applications, or configurations required for PCI DSS compliance (for example, payment application cannot interfere with anti-virus protection, firewall configurations, or any other device, application, or configuration required for PCI DSS compliance). ***PCI Data Security Standard Requirements 1, 3, 4, 5, and 6.6***	**8.1** Test the payment application in a lab to obtain evidence that it can run in a network that is fully compliant with PCI DSS. Verify that the payment application does not inhibit installation of patches or updates to other components in the environment.			
9. Cardholder data must never be stored on a server connected to the Internet				
9.1 The payment application must be developed such that the database server and web server are not required to be on the same server, nor is the database server required to be in the DMZ with the web server. ***PCI Data Security Standard Requirement 1.3.2***	**9.1.a** To verify that the payment application stores cardholder data in the internal network, and never in the DMZ, obtain evidence that the payment application does not require data storage in the DMZ, and will allow use of a DMZ to separate the Internet from systems storing cardholder data (for example, payment application must not require that the database server and web server be on the same server, or in the DMZ with the web server).			
	9.1.b If customers could store cardholder data on a server connected to the Internet, examine *PA-DSS Implementation Guide* prepared by vendor to verify customers and resellers/integrators are told not to store cardholder data on Internet-accessible systems (for example, web server and database server must not be on same server).			

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
10. Facilitate secure remote software updates				
10.1 If payment application updates are delivered via remote access into customers' systems, software vendors must tell customers to turn on remote-access technologies only when needed for downloads from vendor, and to turn off immediately after download completes. Alternatively, if delivered via VPN or other high-speed connection, software vendors must advise customers to properly configure a firewall or a personal firewall product to secure "always-on" connections. ***PCI Data Security Standard Requirements 1 and 12.3.9***	**10.1** If the vendor delivers payment application and/or updates via remote access to customer networks, examine *PA-DSS Implementation Guide* prepared by vendor, and verify it contains: ▪ Instructions for customers and resellers/integrators regarding secure use of remote-access technologies, per PCI DSS Requirement 12.3.9 ▪ Recommendation for customers and resellers/ integrators to use a firewall or a personal firewall product if computer is connected via VPN or other high-speed connection, to secure these "always-on" connections, per PCI DSS Requirement 1			
11. Facilitate secure remote access to payment application				
11.1 The payment application must not interfere with use of a two-factor authentication mechanism. The payment application must allow for technologies such as RADIUS or TACACS with tokens, or VPN with individual certificates. ***PCI Data Security Standard Requirement 8.3***	**11.1** Test the payment application in a lab to obtain evidence that it can run with a two-factor authentication mechanism (the payment application must not prohibit an organization's ability to implement two-factor authentication).			
11.2 If the payment application may be accessed remotely, remote access to the payment application must be authenticated using a two-factor authentication mechanism. ***PCI Data Security Standard Requirement 8.3***	**11.2** If the payment application may be accessed remotely, examine *PA-DSS Implementation Guide* prepared by the software vendor, and verify it contains instructions for customers and resellers/integrators regarding required use of two-factor authentication (user ID and password and an additional authentication item such as a smart card, token, or PIN).			

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
11.3 If vendors, resellers/integrators, or customers can access customers' payment applications remotely, the remote access must be implemented securely. ***PCI Data Security Standard Requirement 8.3***	**11.3.a** If the software vendor uses remote access products for remote access to the customers' payment application, verify that vendor personnel implement and use remote access security features. *Note: Examples of remote access security features include*: ▪ *Change default settings in the remote access software (for example, change default passwords and use unique passwords for each customer).* ▪ *Allow connections only from specific (known) IP/MAC addresses.* ▪ *Use strong authentication and complex passwords for logins according to PCI DSS Requirements 8.1, 8.3, and 8.5.8–8.5.15* ▪ *Enable encrypted data transmission according to PCI DSS Requirement 4.1* ▪ *Enable account lockout after a certain number of failed login attempts according to PCI DSS Requirement 8.5.13* ▪ *Configure the system so a remote user must establish a Virtual Private Network ("VPN") connection via a firewall before access is allowed.* ▪ *Enable the logging function.* ▪ *Restrict access to customer passwords to authorized reseller/integrator personnel.* ▪ *Establish customer passwords according to PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.*			

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
	11.3.b If resellers/integrators or customers can use remote access software, examine *PA-DSS Implementation Guide* prepared by the software vendor, and verify that customers and resellers/integrators are instructed to use and implement remote access security features. *Note: Examples of remote access security features include*: ▪ *Change default settings in the remote access software (for example, change default passwords and use unique passwords for each customer).* ▪ *Allow connections only from specific (known) IP/MAC addresses.* ▪ *Use strong authentication and complex passwords for logins, according to PCI DSS Requirements 8.1, 8.3, and 8.5.8–8.5.15.* ▪ *Enable encrypted data transmission according to PCI DSS Requirement 4.1.* ▪ *Enable account lockout after a certain number of failed login attempts according to PCI DSS Requirement 8.5.13.* ▪ *Configure the system so a remote user must establish a Virtual Private Network ("VPN") connection via a firewall before access is allowed.* ▪ *Enable the logging function.* ▪ *Restrict access to customer passwords to authorized reseller/integrator personnel.* ▪ *Establish customer passwords according to PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.*			

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
12. Encrypt sensitive traffic over public networks				
12.1 If the payment application sends, or facilitates sending, cardholder data over public networks, the payment application must support use of strong cryptography and security protocols such as SSL/TLS and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks. *Examples of open, public networks that are in scope of the PCI DSS are:* ▪ *The Internet* ▪ *Wireless technologies* ▪ *Global System for Mobile Communications (GSM)* ▪ *General Packet Radio Service (GPRS)* ***PCI Data Security Standard Requirement 4.1***	**12.1.a** If the payment application sends, or facilitates sending, cardholder data over public networks, verify that secure encryption transmission technology (for example, IPSEC, VPN or SSL/TLS) is provided, or that use thereof is specified.			
	12.1.b If the payment application allows data transmission over public networks, examine *PA-DSS Implementation Guide* prepared by the vendor, and verify the vendor includes directions for customers and resellers/integrators to use secure encryption transmission technology (for example, IPSEC, VPN or SSL/TLS).			
12.2 The payment application must never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat). ***PCI Data Security Standard Requirement 4.2***	**12.2.a** If the payment application allows and/or facilitates sending of PANs by end-user messaging technologies, verify that a strong cryptography solution is provided, or that use thereof is specified.			
	12.2.b If the payment application allows and/or facilitates the sending of PANs by end-user messaging technologies, examine *PA-DSS Implementation Guide* prepared by the vendor, and verify the vendor includes directions for customers and resellers/integrators to use a solution that implements strong cryptography.			

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
13. Encrypt all non-console administrative access				
13.1 Instruct customers to encrypt all non-console administrative access using technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access. ***PCI Data Security Standard Requirement 2.3*** *Telnet or rlogin must never be used for administrative access.*	**13.1** If payment application or server allows non-console administration, examine the *PA-DSS Implementation Guide* prepared by vendor, and verify vendor recommends use of SSH, VPN, or SSL/TLS for encryption of non-console administrative access.			
14. Maintain instructional documentation and training programs for customers, resellers, and integrators				
14.1 Develop, maintain, and disseminate a *PA-DSS Implementation Guide(s)* for customers, resellers, and integrators that accomplishes the following:	**14.1** Examine the *PA-DSS Implementation Guide* and related processes, and verify the guide is disseminated to all relevant payment application users (including customers, resellers, and integrators).			
14.1.1 Addresses all requirements in this document wherever the *PA-DSS Implementation Guide* is referenced.	**14.1.1** Verify the *PA-DSS Implementation Guide* covers all related requirements in this document.			
14.1.2 Includes a review at least annually and updates to keep the documentation current with all major and minor software changes as well as with changes to the requirements in this document.	**14.1.2.a** Verify the *PA-DSS Implementation Guide* is reviewed on an annual basis and updated as needed to document all major and minor changes to the payment application.			
	14.1.2.b Verify the *PA-DSS Implementation Guide* is reviewed on an annual basis and updated as needed to document changes to the PA-DSS requirements.			
14.2 Develop and implement training and communication programs to ensure payment application resellers and integrators know how to implement the payment application and related systems and networks according to the *PA-DSS Implementation Guide* and in a PCI DSS-compliant manner.	**14.2** Examine the training materials and communication program for resellers and integrators, and confirm the materials cover all items noted for the *PA-DSS Implementation Guide* throughout this document.			

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
14.2.1 Update the training materials on an annual basis and whenever new payment application versions are released.	**14.2.1.a** Examine the training materials for resellers and integrators and verify the materials are reviewed on an annual basis and when new payment application versions are released, and updated as needed.			
	14.2.1.b Examine the distribution process for new payment application versions and verify that updated documentation is distributed with the updated payment application.			
	14.2.1.c Select a sample of resellers and integrators and interview them to verify they received the training materials.			

Appendix A: Summary of Contents for the *PA-DSS Implementation Guide*

The intent of this Appendix is to summarize those PA-DSS requirements that have related *PA-DSS Implementation Guide* topics, to explain the content for the *PA-DSS Implementation Guide,* and to spell out responsibilities for implementing the related controls.

PA-DSS Requirement	PA-DSS Topic	Implementation Guide Content	Control Implementation Responsibility
1.1.4	Delete sensitive authentication data stored by previous payment application versions.	▪ Historical data must be removed (magnetic stripe data, card validation codes, PINs, or PIN blocks stored by previous versions of the payment application) ▪ How to remove historical data ▪ Such removal is absolutely necessary for PCI DSS compliance	**Software Vendor**: Provide tool or procedure for customers to securely remove data stored by previous versions, per PA-DSS Requirement 1.1.4. **Customers & Resellers/Integrators**: Delete any historical data per the *PA-DSS Implementation Guide* and PA-DSS Requirement 1.1.4.
1.1.5	Delete any sensitive authentication data (pre-authorization) gathered as a result of troubleshooting the payment application.	▪ Sensitive authentication data (pre-authorization) must only be collected when needed to solve a specific problem ▪ Such data must be stored only in specific, known locations with limited access ▪ Only collect a limited amount of such data as needed to solve a specific problem ▪ Sensitive authentication data must be encrypted while stored ▪ Such data must be securely deleted immediately after use	**Software Vendor**: Perform any troubleshooting of customer's problems according to PA-DSS Requirement 1.1.6.a. **Customers & Resellers/Integrators:** Troubleshoot any problems per the *PA-DSS Implementation Guide* and PA-DSS Requirement 1.1.6.a.
2.1	Purge cardholder data after customer-defined retention period.	▪ Cardholder data must be purged after it exceeds the customer-defined retention period ▪ All locations where payment application stores cardholder data	**Software Vendor**: Provide guidance to customers that cardholder data exceeding customer-defined retention periods must be purged and where such data is stored by the payment application. **Customers & Resellers/Integrators**: Purge cardholder data exceeding customer-defined retention period.

PA-DSS Requirement	PA-DSS Topic	Implementation Guide Content	Control Implementation Responsibility
2.7	Delete cryptographic key material or cryptograms stored by previous payment application versions.	▪ Cryptographic material must be removed ▪ How to remove cryptographic material ▪ Such removal is absolutely necessary for PCI compliance ▪ How to re-encrypt historic data with new keys	**Software Vendor**: Provide tool or procedure to securely remove cryptographic key material or cryptograms stored by previous versions, per PA-DSS Requirement 1.1.5, provide tool or procedure to re-encrypt historic data with new keys. **Customers & Resellers/Integrators**: Delete any historical cryptographic material per *PA-DSS Implementation Guide* and PA-DSS Requirement 1.1.5.
3.1	Use unique user IDs and secure authentication for administrative access and access to cardholder data.	▪ Do not use default administrative accounts for payment application logins. ▪ Assign secure authentication to default accounts (even if not used), and disable or do not use the accounts. ▪ Use secure authentication for the payment application and system whenever possible. ▪ How to create secure authentication to access the payment application, per PCI DSS Requirements 8.5.8 through 8.5.15.	**Software Vendor**: Ensure payment application supports customer's use of unique user IDs and secure authentication for payment application accounts/passwords, per PCI DSS Requirements 8.1 and 8.2. **Customers & Resellers/Integrators**: Establish and maintain unique user IDs and secure authentication per the *PA-DSS Implementation Guide* and PCI DSS Requirements 8.1 and 8.2.
3.2	Use unique user IDs and secure authentication for access to PCs, servers, and databases with payment applications.	Use unique user names and secure authentication to access any PCs, servers, and databases with payment applications and/or cardholder data, per PCI DSS Requirements 8.5.8 through 8.5.15.	**Software Vendor**: Ensure payment application supports customer's use of unique user IDs and secure authentication for accounts/passwords if set by vendor to access PCs, servers, and databases, per PCI DSS Requirements 8.1, 8.2, and 8.5.8–8.5.15. **Customers & Resellers/Integrators**: Establish and maintain unique user IDs and secure authentication per the *PA-DSS Implementation Guide* and PCI DSS Requirements 8.1, 8.2, and 8.5.8–8.5.15.
4.2	Implement automated audit trails.	▪ Set PCI DSS-compliant log settings, per PCI DSS Requirement 10. ▪ Logs must be enabled, and disabling the logs will result in non-compliance with PCI DSS.	**Software Vendor**: Ensure payment application supports customer's use of compliant logs per PCI DSS Requirement 10. **Customers & Resellers/Integrators:** Establish and maintain PCI DSS-compliant logs per the *PA-DSS Implementation Guide* and PCI DSS Requirement 10.

PA-DSS Requirement	PA-DSS Topic	Implementation Guide Content	Control Implementation Responsibility
6.1	Securely implement wireless technology.	If wireless is used within payment environment, install a firewall per PCI DSS Requirement 1.3.8.	**Software Vendor**: Instruct customers and resellers/integrators, that if wireless technology is used with the payment application, that wireless vendor default settings must be changed per PCI DSS Requirement 2.1.1. **Customers & Resellers/Integrators**: For wireless implemented into the payment environment by customers or resellers/integrators, install a firewall per the *PA-DSS Implementation Guide* and PCI DSS Requirement 2.1.1.
6.2	Secure transmissions of cardholder data over wireless networks.	If payment application is implemented into a wireless environment, use PCI DSS-compliant wireless settings, per PCI DSS Requirement 4.1.1.	**Software Vendor**: Instruct customers and resellers/integrators, that if wireless technology is used with the payment application, that secure encrypted transmissions must be implemented, per PCI DSS Requirement 4.1.1. **Customers & Resellers/Integrators**: For wireless implemented into the payment environment by customers or resellers/integrators, use secure encrypted transmissions per the *PA-DSS Implementation Guide* and PCI DSS Requirement 4.1.1.
9.1	Store cardholder data only on servers not connected to the Internet.	Do not store cardholder data on Internet-accessible systems (for example, web server and database server must not be on same server).	**Software Vendor**: Ensure payment application does not require data storage in the DMZ or on Internet-accessible systems, and will allow use of a DMZ per PCI DSS Requirement 1.3.4. **Customers & Resellers/Integrators**: Establish and maintain payment applications so that cardholder data is not stored on Internet-accessible systems, per the *PA-DSS Implementation Guide* and PCI DSS Requirement 1.3.4.

PA-DSS Requirement	PA-DSS Topic	Implementation Guide Content	Control Implementation Responsibility
10.1	Securely deliver remote payment application updates.	▪ Receive remote payment application updates via secure modems, per PCI DSS Requirement 12.3. ▪ If computer is connected via VPN or other high-speed connection, receive remote payment application updates via a firewall or a personal firewall per PCI DSS Requirement 1 or 1.3.9.	**Software Vendor**: Deliver remote payment application updates securely per PCI DSS Requirements 1, 1.3.9, and 12.3.9. **Customers & Resellers/Integrators**: Receive remote payment application updates from vendor securely, per the *PA-DSS Implementation Guide* and PCI DSS Requirements 1, 1.3.9, and 12.3.9.
11.2	Implement two-factor authentication for remote access to payment application.	Use two-factor authentication (user ID and password and an additional authentication item such as a token) if the payment application may be accessed remotely.	**Software Vendor**: Ensure payment application supports customers' use of two-factor authentication, per PCI DSS Requirement 8.3. **Customers & Resellers/Integrators**: Establish and maintain two-factor authentication for remote access to payment application, per the *PA-DSS Implementation Guide* and PCI DSS Requirement 8.3.
11.3	Securely implement remote access software.	Implement and use remote access software security features if remote access software is used to remotely access the payment application or payment environment.	**Software Vendor**: (1) If vendor uses remote access products to access customer sites, use remote access security features such as those specified in PA-DSS Requirement 11.3.a. (2) Ensure payment application supports customers' use of remote access security features. **Customers & Resellers/Integrators**: Use remote access security features if you allow remote access to payment applications, per the *PA-DSS Implementation Guide* and PA-DSS Requirement 11.3.b.
12.1	Secure transmissions of cardholder data over public networks.	Implement and use SSL for secure cardholder data transmission over public networks, in accordance with PCI DSS Requirement 4.1	**Software Vendor**: Ensure payment application supports customer's use of secure transmissions of cardholder data over public networks, per PCI DSS Requirement 4. **Customers & Resellers/Integrators**: Establish and maintain secure transmissions of cardholder data, per the *PA-DSS Implementation Guide* and PCI DSS Requirement 4.

PA-DSS Requirement	PA-DSS Topic	Implementation Guide Content	Control Implementation Responsibility
12.2	Encrypt cardholder data sent over end-user messaging technologies.	Implement and use an encryption solution for if PANs can be sent with end-user messaging technologies.	**Software Vendor**: Ensure payment application supports customer's encryption of PANs if sent with end-user messaging technologies, per PCI DSS Requirement 4.2. **Customers & Resellers/Integrators**: Encrypt all PANs sent with end-user messaging technologies, per the *PA-DSS Implementation Guide* and PCI DSS Requirement 4.2.
13.1	Encrypt non-console administrative access.	Implement and use SSH, VPN, or SSL/TLS for encryption of any non-console administrative access to payment application or servers in cardholder data environment.	**Software Vendor**: Ensure payment application supports customer's encryption of any non-console administrative access, per PCI DSS Requirement 2.3. **Customers & Resellers/Integrators**: Encrypt all non-console administrative access, per the *PA-DSS Implementation Guide* and PCI DSS Requirement 2.3.

Appendix B: Confirmation of Testing Laboratory Configuration Specific to PA-DSS Assessment

For: *Software Vendor Application Name Version Number*

For each PA-DSS assessment conducted, the PA-QSA must complete this document to confirm the status and capabilities of the laboratory used to conduct the testing for the PA-DSS assessment. This completed document must be submitted along with the completed PA-DSS Requirements and Security Assessment Procedures document.

For each Laboratory Validation Procedures, indicate (by using columns titled "Completed in PA-QSA's Lab" or "Completed in Vendor's Lab") whether laboratory used for the assessment and the laboratory undergoing these Validation Procedures was the PA-QSA's laboratory or software vendor's laboratory.

Describe laboratory testing architecture and environment in place for this PA-DSS review:

Describe how the real-world use of the payment application was simulated in the laboratory for this PA-DSS review:

Laboratory Requirement	Laboratory Validation Procedure	Completed in PA-QSA's Lab	Completed in Vendor's Lab	Comments
1. Install payment application per vendor's installation instructions or training provided to customer.	**1.** Verify that the vendor's installation manual or training provided to customers was used to perform the default installation for the payment application product on all platforms listed in the PA-DSS report.			
2. Install and test all payment application versions listed in PA-DSS report.	**2.a** Verify that all common implementations (including region/country specific versions) of the payment application to be tested were installed.			
	2.b Verify that all payment application versions and platforms were tested.			
	2.c Verify that all critical payment application functionalities were tested.			

Laboratory Requirement	Laboratory Validation Procedure	Completed in PA-QSA's Lab	Completed in Vendor's Lab	Comments
3. Install and implement all PCI DSS required security devices.	**3.** Verify that all security devices required by PCI DSS (for example, firewalls and anti-virus software) were implemented on test systems.			
4. Install and/or configure all PCI DSS required security settings.	**4.** Verify all PCI DSS-compliant system settings, patches, etc. were implemented on test systems for operating systems, system software, and applications used by the payment application.			
5. Simulate real-world use of the payment application.	**5.a** The laboratory simulates the 'real world' use of the payment application, including all systems and applications where the payment application is implemented. For example, a standard implementation of a payment application might include a client/server environment within a retail storefront with a POS machine, and back office or corporate network. The laboratory simulates the total implementation.			
	5.c The laboratory runs the payment application's authorization and/or settlement functions and all output is examined per item 6 below.			
	5.d The laboratory and/or processes map all output produced by the payment application for every possible scenario, whether temporary, permanent, error processing, debugging mode, log files, etc.			
	5.e The laboratory and/or processes simulate and validate all functions of the payment application, to include generation of all error conditions and log entries using both simulated 'live' data and invalid data.			

Laboratory Requirement	Laboratory Validation Procedure	Completed in PA-QSA's Lab	Completed in Vendor's Lab	Comments
6. Provide capabilities for, and test using, the following penetration testing methodologies:	**6.a Use of forensic tools/methods[6]:** Forensic tools/methods were used to search all identified output for evidence of sensitive authentication data (commercial tools, scripts, etc.), per PA-DSS Requirement 1.1.1–1.1.3.[6]			
	6.b Attempt to exploit OWASP vulnerabilities: OWASP vulnerabilities were used to attempt to exploit the payment application(s), per PA-DSS Requirement 5.1.1–5.1.10.			
	6.c Laboratory and/or processes attempted to execute arbitrary code during the payment application update process: Run the update process with arbitrary code per PA-DSS requirement 7.2.b.			
7. Use vendor's lab ONLY after verifying all requirements are met.	**7.a** If use of the software vendor's lab is necessary (for example, the PA-QSA does not have the mainframe, AS400, or Tandem the payment application runs on), the PA-QSA can either (1) use equipment on loan from the Vendor or (2) use the vendor's lab facilities, provided that this is detailed in the report together with the location of the tests. For either option, the PA-QSA verified that the vendor's equipment and lab meet the following requirements:			
	7.b The PA-QSA verifies that the vendor's lab meets all above requirements specified in this document and documents the details in the report.			
	7.c All testing is executed by the PA-QSA (the vendor cannot run tests against their own application).			

[6] Forensic tool or method: A tool or method for uncovering, analyzing and presenting forensic data, which provides a robust way to authenticate, search, and recover computer evidence rapidly and thoroughly. In the case of forensic tools or methods used by PA-QSAs, these tools or methods should accurately locate any sensitive authentication data written by the payment application. These tools may be commercial, open-source, or developed in-house by the PA-QSA.

Laboratory Requirement	Laboratory Validation Procedure	Completed in PA-QSA's Lab	Completed in Vendor's Lab	Comments
	7.d All testing is either (1) performed while on-site at the vendor's premises, or (2) performed remotely via a network connection using a secure link (for example, VPN).			
	7.e Use only test card numbers for the simulation/testing—do not use live PANs for testing. These test cards can usually be obtained from the vendor or a processor or acquirer.			
8. Maintain an effective quality assurance (QA) process	**8.a** PA-QSA QA personnel verifies that all platforms identified in the PA-DSS report were included in testing.			
	8.b PA-QSA QA personnel verify that all PA-DSS requirements were tested against.			
	8.c The PA-QSA QA personnel verify that PA-QSA laboratory configurations and processes meet requirements and were accurately documented in the report.			
	8.d PA-QSA QA personnel verify that the report accurately presents the results of testing.			

Appendix C: Attestation of Validation

Instructions for Submission

The Payment Application Qualified Security Assessor (PA-QSA) must complete this document as a declaration of the payment application's validation status with the Payment Application Data Security Standard (PA-DSS). Complete all applicable sections of this Attestation of Validation. Submit the PA-DSS Report on Validation (ROV), this attestation, and the completed PA-DSS Appendix B to PCI SSC. Once accepted by PCI SSC, the payment application will be posted on the PCI SSC website as a PA-DSS validated payment application.

The PA-QSA and Payment Application Software Vendor should complete all sections and submit this document along with copies of all required validation documentation to PCI SSC, per PCI SSC's instructions for report encryption and submission.

Part 1. Payment Application Qualified Security Assessor (PA QSA) Company Information					
Company Name:					
Lead PA-QSA Contact Name:		*Title:*			
Telephone:		*E-mail:*			
Business Address:		*City:*			
State/Province:		*Country:*		*ZIP:*	
URL:					

Part 2. Payment Application Vendor Information					
Company Name:					
Contact Name:		*Title:*			
Telephone:		*E-mail:*			
Business Address:		*City:*			
State/Province:		*Country:*		*ZIP:*	
URL:					

Part 2a. Payment Application Information

List Payment Application Name(s) and Version Number(s) included in PA-DSS review:

Payment Application Functionality (check all that apply):		
☐ POS Suite	☐ POS Admin	☐ Shopping Cart & Store Front
☐ POS Face-to-Face	☐ Payment Middleware	☐ Others (please specify):
☐ POS Kiosk	☐ Payment Back Office	
☐ POS Specialized	☐ Payment Gateway/Switch	

Target Market for Application:

Part 3. PCI PA-DSS Validation

Part 3a. Confirmation of Validated Status

Based on the results noted in the PA-DSS ROV dated *(date of ROC)*, *(QSA Name)* asserts the following validation status for the application(s) and version(s) identified in Part 2a of this document as of *(date)* (check one):

☐	**Fully Validated:** All requirements in the ROV are marked "in place," thereby *(Payment Application Name(s) and Version(s))* has achieved full validation with the Payment Application Data Security Standard.
☐	The ROV was completed according to the PA-DSS, version *(insert version number)*, in adherence with the instructions therein.
☐	All information within the above-referenced ROV and in this attestation represents the results of the assessment fairly in all material respects.
☐	No evidence of magnetic stripe (i.e., track) data[7], CAV2, CVC2, CID, or CVV2 data[8], or PIN data[9] storage after transaction authorization on ANY files or functionalities generated by the application during this PA-DSS assessment.

Part 3b. Annual Re-Validation Confirmation:

☐	The contents of the above-referenced ROV continue to be applicable to the following software version: *(Payment Application Name and version)*.

Note: Section 3b is for the required Annual Attestation for listed payment applications, and should ONLY be completed if no modifications have been made to the Payment Application covered by the above-referenced ROV. For the annual re-validation, the software vendor can complete, sign, and submit this form. The PA-QSA is not required to sign the annual re-validation.

Part 3c. PA-QSA and Application Vendor Acknowledgments

Signature of Lead PA-QSA ↑	*Date* ↑
Lead PA-QSA Name ↑	*Title* ↑
Signature of Application Vendor Executive Officer ↑	*Date* ↑
Application Vendor Executive Officer Name ↑	*Title* ↑

Application Vendor Company Represented ↑

[7] Magnetic Stripe Data (Track Data) – Data encoded in the magnetic stripe used for authorization during a card-present transaction. Entities may not retain full magnetic stripe data after authorization. The only elements of track data that may be retained are account number, expiration date, and name.

[8] The three- or four-digit value printed on the signature panel or face of a payment card used to verify card-not-present transactions.

[9] PIN Data – Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.