Payment Card Industry (PCI)
Data Security Standard

Payment Application Data Security

Template for Report on Validation
for use with PA-DSS v3.0

Version 1.1

July 2014

Document Changes

Date	Version	Description
July 2014	1.1	Errata – Minor edits made to address typos and general errors, slight addition of content
January 2014	1.0	To introduce the template for submitting Reports on Validation. *This document is intended for use with version 3.0 of the PCI Payment Application Data Security Standard.*

Table of Contents

Introduction to the ROV Template

This document, the *PCI PA-DSS Template for Report on Validation for use with PA-DSS v3.0* ("ROV Reporting Template"), is the mandatory template for completing a Report on Validation (ROV) for assessments against the *PA-DSS Requirements and Security Assessment Procedures v3.0.* This Reporting Template provides reporting instructions and the template form for PA-QSAs to provide a more consistent level of reporting among assessors.

Use of this Reporting Template is mandatory for all v3.0 submissions; however, it may NOT be used for 2.0 submissions. Refer to the *ROV Reporting Instructions for PA-DSS v2.0* for guidance on completing 2.0 submissions.

Tables have been included in this template to facilitate the reporting process for certain lists and other information as appropriate. The tables in this template may be modified to increase/decrease the number of rows, or to change column width. Additional appendices may be added if the assessor feels there is relevant information to be included that is not addressed in the current format. However, the assessor must not remove any details from the tables provided in this document. Personalization, such as the addition of company logos, is acceptable.

Do not delete any content from any place in this document, including this section and the versioning above. These instructions are important for the assessor as the report is written and for the recipient in understanding the context the responses and conclusions are made. Addition of text or sections is applicable within reason, as noted above. Refer to the "ROV Reporting Template for PA-DSS v3.0: Frequently Asked Questions (FAQs)" document on the PCI SSC website for further guidance.

A PA-DSS compliance assessment involves thorough testing and assessment activities, from which the assessor will generate detailed work papers. These work papers contain comprehensive records of the assessment activities, including observations, results of system testing, configuration data, file lists, interview notes, documentation excerpts, references, screenshots, and other evidence collected during the course of the assessment. The ROV is effectively a ***summary of evidence*** derived from the assessor's work papers to describe how the assessor performed the validation activities and how the resultant findings were reached. At a high level, the ROV provides a comprehensive ***summary of testing activities performed and information collected*** during the assessment against the *PA-DSS Requirements and Security Assessment Procedures v3.0*. The information contained in a ROV must provide enough detail and coverage to verify that the payment application is compliant with all PA-DSS requirements.

ROV Sections

As defined in the *PA-DSS Requirements and Security Assessment Procedures*, the ROV includes the following sections and appendices:

- Section 1: Contact Information and Report Date
- Section 2: Description of Scope of Review
- Section 3: Summary Overview
- Section 4: Findings and Observations
- Appendix A: Summary of Contents for the *PA-DSS Implementation Guide*
- Appendix B: Testing Laboratory Configuration for PA-DSS Assessments

If the first three sections are not thoroughly and accurately completed, the assessment findings in Section 4 (Findings and Observations) will not have proper context. This Reporting Template includes tables with Reporting Instructions built-in so that there is increased likelihood of providing all required information throughout the document. Responses should be specific, but efficient. Details provided should focus on concise quality of detail, rather than lengthy, repeated verbiage.

ROV Summary of Findings

With the Reporting Template, an effort was made to efficiently use space, and as such, there is one response column for results/evidence ("ROV Reporting Details: Assessor's Response") instead of three.

To designate whether the finding was In Place, Not Applicable, or Not in Place, at each sub-requirement there is a place to designate the result ("Summary of Findings"), which can be checked as appropriate. See the example format below.

The following table is a helpful representation when considering which selection to make. Remember, only one response should be selected at the sub-requirement level, and reporting of that should be consistent with other required documents, such as the Attestation of Validation (AOV).

Refer to the "ROV Reporting Template for PCI DSS v3.0: Frequently Asked Questions (FAQs)" document on the PCI SSC website for further guidance.

RESPONSE	WHEN TO USE THIS RESPONSE:	USING THE SAMPLE BELOW:
In Place	The expected testing has been performed, and all elements of the requirement have been met as stated.	*In the sample, the Summary of Assessment Findings at 1.1 is "in place" if all report findings are in place for 1.1.a and 1.1.b or a combination of in place and not applicable.*
Not in Place	Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before it will be known if they are in place.	*In the sample, the Summary of Assessment Findings at 1.1 is "not in place" if either 1.1.a or 1.1.b are concluded to be "not in place."*
N/A (Not Applicable)	The requirement does not apply to the payment application. All "not applicable" responses require reporting on testing performed to confirm the "not applicable" status. Note that a "Not Applicable" response still requires a detailed description explaining how it was determined that the requirement does not apply. Certain requirements are always applicable and that will be designated by a grey box under "Not Applicable."	*In the sample, the Summary of Assessment Findings at 1.1 is "not applicable" if both 1.1.a and 1.1.b are concluded to be "not applicable." A requirement is applicable if any aspects of the requirement apply to the environment being assessed, and a "Not Applicable" designation in the Summary of Assessment Findings should not be used in this scenario.*

Requirement X: Sample

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
1.1 Sample sub-requirement					
1.1.a Sample testing procedure	▪ Reporting Instruction	*<Report Findings Here>*			
1.1.b Sample testing procedure	▪ Reporting Instruction	*<Report Findings Here>*			

ROV Reporting Details

The reporting instructions in the Reporting Template are clear as to the intention of the response required. There is no need to repeat the testing procedure, the reporting instruction, or such within each assessor response. As noted earlier, responses should be specific, but simple. Details provided should focus on concise quality of detail, rather than lengthy, repeated verbiage.

Assessor responses will generally fall into categories such as the following:

- **One word (yes/no)**

  *Example Reporting Instruction: **Identify** whether the payment application stores sensitive data after authorization. **(yes/no)***

- Document name or interviewee reference (at 2.7 Documentation Reviewed and 2.8 Individuals Interviewed, there is a space for a reference number and it is the PA-QSA's choice to use the document name/interviewee job title or the reference number in responses)

  *Example Reporting Instruction: **Identify** the document that defines vendor software development processes.*

- **Short listing**

  *Example Reporting Instruction: **Identify the sampled tables or files from data repositories** created or generated by the application observed to verify the PAN is rendered unreadable.*

- **Brief description/short answer**

  *Example Reporting Instruction: **Describe how** the processes were observed to verify that patches and updates are delivered to customers in a secure manner with a known chain-of-trust.*

PA-DSS Implementation Guide

As defined in the *PA-DSS Requirements and Security Assessment Procedures*, payment application vendors are required to provide a *PA-DSS Implementation Guide* to:

- Instruct their customers and resellers/integrators on secure product implementation,
- Document the secure configuration specifics required throughout the PA-DSS, and
- Clearly delineate vendor, reseller/integrator, and customer responsibilities for meeting PCI DSS requirements.

The Implementation Guide must be specific to each application and provide instructions on how to implement the application in a PCI DSS compliant manner. It is not sufficient for the Implementation Guide to simply reiterate requirements from the PA-DSS and PCI DSS, and the testing procedures have been made stronger in 3.0 to give greater assurance that the guidance is accurate and effective.

As part of the assessment, the PA-QSA verifies that the Implementation Guide contains proper instructions and guidance for customers and resellers/integrators to install, configure, and maintain the payment application in a PCI DSS compliant manner.

For reporting on the PA-DSS Implementation Guide content, the assessor response will need to be the Section and/or page number(s) of the Implementation Guide where the guidance was found. There is no need to describe the content in this instruction.

Do's and Don'ts: Reporting Expectations

DO:	*DON'T:*
▪ Use this Reporting Template, if assessing against v3.0 of the PA-DSS. ▪ Complete all sections in the order specified, with concise detail. ▪ Read and understand the intent of each Requirement and Testing Procedure. ▪ Provide a response for every Testing Procedure. ▪ Provide sufficient detail and information to demonstrate a finding of "in place" or "not applicable." ▪ Describe how a Requirement was verified as the Reporting Instruction directs, not just that it was verified. ▪ Ensure the parts of the Testing Procedure are addressed. ▪ Ensure the response covers all applicable application and/or system components. ▪ Perform an internal quality assurance review of the ROV for clarity, accuracy, and quality. ▪ Provide useful, meaningful diagrams, as directed.	▪ Don't report items in the "In Place" column unless they have been verified as being "in place." ▪ Don't include forward-looking statements or project plans in the "In Place" column. ▪ Don't simply repeat or echo the Testing Procedure in the response. ▪ Don't copy responses from one Testing Procedure to another. ▪ Don't copy responses from previous assessments. ▪ Don't include information irrelevant to the assessment.

ROV Template for PCI Payment Application Data Security Standard v3.0

This template is to be used for creating a Report on Validation. Content and format for a ROV is defined as follows:

1. Contact Information and Report Date

1.1 Contact Information

Payment Application Vendor	
Company name:	
Company address:	
Company URL:	
Company contact name:	
Contact phone number:	
Contact e-mail address:	
PA-QSA Company	
Company name:	
Company address:	
Company website:	
PA-QSA Assessor	
Assessor name:	
Assessor phone number:	
Assessor e-mail address:	
Assessor Quality Assurance (QA) Primary Reviewer for this specific report (not the general QA contact for the PA-QSA)	
Reviewer name:	
Reviewer phone number:	
Reviewer e-mail address:	

1.2 Date and Timeframe of Assessment

Date of Report:	
Timeframe of assessment (start date to completion date):	
Dates spent onsite:	
Description of how the actual time during the timeframe was used for actively working on the assessment. Include description of actual time the assessor spent performing assessment activities (including lab time).	

1.3 PA-DSS Version

Version of the *PA-DSS Requirements and Security Assessment Procedures* used for the assessment (should be 3.0):	

1.4 Additional Services Provided by PA-QSA/QSA Company

The PCI DSS Validation Requirements for QSAs v1.2, Section 2.2 "Independence" specifies requirements for QSAs around disclosure of such services and/or offerings that could reasonably be viewed to affect independence of assessment. Complete the below after review of this portion of the Validation Requirements, to ensure responses are consistent with documented obligations.

▪ Disclose all services offered to the assessed entity by the PA-QSA/QSAC, including but not limited to whether the assessed entity uses any security-relates devices or security-related applications that have been developed or manufactured by the QSA, or to which the QSA owns the rights or that the QSA has configured or manages:	
▪ Describe efforts made to ensure no conflict of interest resulted above mentioned services provided by the PA-QSA/QSAC:	

2. Description of Scope of Work

2.1 Scope Overview

Identify the application and all application components included in this review

Application included in this review	
All application components included in this review	

2.2 Scope Description

Provide a full description of the application, including:

▪ The type of application (for example, POS terminal, payment switch, shopping cart, kiosk, etc.)	
▪ Application Use and Purpose general description	
• Identify the types of transactions	
• List any specific payment acceptance channels (for example, card present and card not present) the application is designed for	
• Describe how the application stores, processes, or transmits cardholder data as part of authorization or settlement	
• Describe how the payment application is sold, distributed, or licensed to third parties	

2.3 PA-DSS Eligibility

▪ Describe how the PA-QSA evaluated PA-DSS eligibility for the tested payment application, per the *PA-DSS Program Guide, v3.0*	
▪ If PA-DSS validation is being sought for resident payment applications on hardware terminals, identify which of the following has been met for PA-DSS validation. *At least one of the two below must be "Yes" to be eligible for PA-DSS validation.*	
▪ The resident payment application directly meets all PA-DSS requirements and is validated according to standard PA-DSS procedures **(yes/no)**	
▪ The resident payment application does not meet all PA-DSS requirements, but the hardware on which the application resides is listed on the PCI SSC's list of Approved PIN Transaction Security Devices as a current PCI PTS approved Point of Interaction (POI) device. In this scenario, it may be possible for the application to satisfy PA-DSS requirements through a combination of the PA-DSS and PTS validated controls. **(yes/no)** ***Note**: This dependency must be documented at 3.7 of the Summary Overview.*	

2.4 Payment Application Functionality Assessed

Briefly describe the payment application functionality that was assessed, specifically the following:

▪ End-to-end payment functions (authorization and settlement)	
▪ Input and output	
▪ Error conditions	
▪ Interfaces and connections to other files, systems, and/or payment applications or application components	
▪ All cardholder data flows	
▪ Encryption mechanisms	
▪ Authentication mechanisms	
▪ Other functions of the application relevant to the protection of cardholder data	

2.5 Payment Application Functionality Excluded from Assessment

Identify whether any functionality of the payment application was excluded in the assessment. (yes/no) *If "yes," complete the following:*	
▪ Identify and describe excluded functionalities.	
▪ For each excluded functionality, describe why it was excluded.	

2.6 Tools Used by or Within the Payment Application to Access and/or View Cardholder Data

Identify all tools used by or within the payment application to access and/or view cardholder data, including:

▪ Reporting tools	
▪ Logging tools	
▪ Other tools	

2.7 Documentation Reviewed

Provide details for the *PA-DSS Implementation Guide* (or "IG") prepared by the vendor for customers and integrators/resellers (as applicable):

Note: *Add additional rows as needed. If the IG consists of more than one document, the brief description below should explain the purpose of each document it includes, such as if it is for a different OS, for different functions, etc.*

Reference Number	**Document Name (including version, if applicable)**	**Brief description of document purpose** (if the IG consists of more than one document)	**Document date** (latest version date)
Doc-1			
Doc-2			
Doc-3			
Doc-4			
▪ Confirm that all references to the *PA-DSS Implementation Guide* or IG in the responses in the body of this report refer to the above. (yes/no)			
If "no," please explain here.			
▪ Provide the name of the PA-QSA who attests that the *PA-DSS* Implementation *Guide* was reviewed and tested by the PA-QSA to verify the guidance for customers and integrators/resellers is both accurate and appropriate as follows: • The customer is clearly instructed how to implement the payment application in a PCI DSS compliant manner. • The customer is clearly instructed that certain payment application and environment settings may prohibit their PCI DSS compliance. • Appropriate and accurate guidance is provided even when a specific setting cannot be controlled by the payment application vendor once the application is installed by the customer. • Appropriate and accurate guidance is provided even when a specific setting is the responsibility of the customer, not the payment application vendor.		

Identify and list all other reviewed documents. Include the following:

Reference Number	Document Name (including version, if applicable)	Brief description of document purpose	Document date (latest version date)
Doc-3			
Doc-4			

2.8 Individuals Interviewed

Identify and list the individuals interviewed. Include the following:

Reference Number	Individual's Name	Role/Job Title	Organization	Summary of Topics Covered (high-level summary only)
Int-1				
Int-2				
Int-3				
Int-4				

3. Summary Overview

3.1 Assessment Overview

▪ Identify the application included in this review:	
• Software vendor name:	
• Full product name:	
• Product version: (Only one version can be included per submission)	
▪ Provide a description of the payment application, including a description of the family of products.	

If the payment application is part of a larger suite of applications, identify any other modules or products in the application suite which were tested with the payment application:

Modules or products tested with the payment application:	**Does the module or product perform payment functions?** (yes/no)

3.2 Testing Overview

Identify all platforms with which the payment application was tested during this assessment:

Platform:	**Details of the underlying hardware architectures** *(For example, mainframe, client-server, clusters, virtualized environments, hardware terminals, etc.),* **as well as user interfaces, programming languages, application frameworks, etc.:**

Identify all operating system(s) with which the payment application was tested during this assessment:

Operating system:	Identify specific versions or service pack level, as applicable:

Identify all operating system(s) with which the payment application was NOT tested during this assessment, but which are supported:

Note: *Only tested operating systems are considered part of a validated solution. Untested supported operating systems will not be listed on the PCI SSC website.*

Operating system:	Identify specific versions or service pack level, as applicable:

Identify all database software with which the payment application was tested in this assessment:

Database software:	Identify specific versions, as applicable:

3.3 Network diagram(s) of a typical implementation of the payment application

Provide one or more simple, high level diagrams(s) showing the overall architecture of the environment for a typical implementation (not necessarily a specific implementation at a customer's site). The diagrams should identify all relevant systems and the relationship between them.

Ensure the diagram(s) are clearly labeled and include the following:

- Connections into and out of a customer's network
  - All connections into and out of the network
  - All connections between the payment application and other applications, systems, networks or zones
- Components within the customer's network, including POS devices, systems, databases, and web servers as applicable
  - All critical components and systems, as well as their locations and the boundaries between them, including POS devices, systems, databases, web servers, and other components as applicable
- Other necessary payment application/components, as applicable
  - All other necessary payment components or systems, as applicable
  - Any components external to the customer's network—for example, payment processor channels, etc.

<Insert network diagram(s) of a typical implementation of the payment application>

3.4 Communication points description

- In the first column below, identify all communication points inbound, outbound and between application components, including:
  - LAN, WAN or Internet connections
  - Host to host software communications
  - Communications internal to the host
  - All other connection points applicable to the assessment
- Next, provide brief descriptions to illustrate each communication point:
  - Identification of the communication endpoints (for example, POS terminal, database server, same-host reporting application, etc.)
  - Boundaries between trusted and untrusted components
  - Connection methods and communication protocol

Note: *These detailed descriptions are additional to the high-level network diagram required above, and should provide a more detailed view of the communication points.*

List of all identified communication points:	**Identification of the communication endpoints:** *(for example, POS terminal, database server, same-host reporting application, etc.)*	**Boundaries between trusted and untrusted components:**	**Connection methods and communication protocol:**

3.5 Dataflow diagram

Note: *Include all types of data flows, including any involving hard copy / paper media.*

▪ Indicate the existence of all flows of cardholder data present:	
• Authorization (yes/no)	
• Capture (yes/no)	
• Settlement (yes/no)	
• Chargeback (yes/no)	
▪ List any other data flows present, as applicable:	

- Provide a data-flow diagram that shows all identified flows of cardholder data. Ensure the diagram includes all of the following for each data flow present:
  - Describe how cardholder data is transmitted, processed and/or stored.
  - Identify the types of cardholder data involved (for example, full track, PAN, expiry date, etc.).
  - Describe any protection mechanisms (for example, encryption, truncation, masking, etc.) applied to the cardholder data.
  - Identify the components involved in the transmission, processing or storage of cardholder data.
  - Include all types of data flows, including any involving hard copy / paper media.

<Insert data-flow diagram here>

3.6 Cardholder Data Storage

Identify and list all databases, tables, and files storing cardholder data (including electronic and hard copy) and provide the following details:

Data Store (file, table, etc.)	**Cardholder Data Elements stored** (PAN, expiry, any elements of SAD)	**How data store is secured** (for example, encryption, access controls, truncation, etc.)	**How is access to data store is logged** (logging mechanism)

3.7 Third-Party Software Dependencies and Requirements

Identify and list all *payment application dependencies*, including software and hardware components, as applicable:

Note: *Refer to the* PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms *for guidance on a dependency versus a payment application-related software component.*

Vendor	Name of Product	Version of Product	Function of Product

Identify and list all *payment application-related software and/or hardware components*, including third-party software and/or hardware requirements, as applicable:

Vendor	Name of Product	Version of Product	Function of Product

3.8 Payment Application End-to-End Authentication Methods

Describe the payment application's end-to-end authentication methods, including details of:

▪ The application's authentication mechanism(s)	
▪ The application's authentication database	
▪ How authentication data (for example, passwords, pins, tokens, etc.) is secured in storage (for example, encryption mechanisms, etc.)	

3.9 The Role of the Payment Application in a Typical Implementation

▪ Describe how the payment application functions in a typical implementation.	
▪ Identify whether any other types of payment applications are necessary for a full payment implementation. (yes/no) *If yes, complete the following:*	

List of Necessary Payment Applications:	Describe the role of each necessary payment application:

3.10 Description of the Typical Customer

Identify the vendor's customer's base, including a description of the typical customer this product is sold to, including:

▪ Type of customer (for example, merchant, service provider, issuer, etc.)	
▪ Size of customer (for example, global, national, regional, local, etc.) including country/regions, where appropriate	
▪ Whether the application is designed for industry-specific customers (for example, healthcare, travel, etc.)	
▪ Customer channel that product is designed for (for example, e-commerce, brick-and-mortar (card present), Mail Order / Telephone Order (MOTO), mixed use, etc.)	

3.11 Vendor's Versioning Methodology

▪ Provide the exact version number that this assessment was performed against.	
▪ Describe the vendor's versioning methodology, as reviewed at PA-DSS Requirement 5.4:	
• Describe the format of the version scheme, such as number of elements, number of digits used for each element, format of separators used between elements and character set used for each element (consisting of alphabetic, numeric and/or alphanumeric characters)	
▪ Describe the hierarchy of the elements:	
• Define what each element represents in the version scheme.	
• If wildcards are used in the versioning methodology, describe how wildcards are used. ***Note:*** *All changes impacting security functionality and/or any PA-DSS requirements must result in a change to the version number listed on the PCI SSC website; wildcards are not permitted for changes which impact security functionality and/or any PA-DSS requirements.*	

▪ Provide the name of the PA-QSA who attests that the version methodology was reviewed to verify it to be consistent with the requirements in the *PA-DSS Program Guide v3.0* and PA-DSS Requirement 5.4.	

3.12 List of Resellers and/or Integrators

▪ Identify whether the product has resellers and/or integrators (yes/no) *If there are no resellers and/or integrators, there is no need to state that repeatedly throughout the report where there are references to "integrators and resellers." Disregard those references.* *However, in Requirement 14 where resellers and integrators are referenced specifically, ensure responses there are consistent with the response here.*	
▪ Provide a full list of all resellers and/or integrator for this product, if applicable	

4. Findings and Observations

Requirement 1: Do not retain full track data, card verification code or value (CAV2, CID, CVC2, CVV2), or PIN block data

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not In Place
1.1 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. Sensitive authentication data includes the data as cited in the following Requirements 1.1.1 through 1.1.3. ***Aligns with PCI DSS Requirement 3.2***					
1.1.a If this payment application stores sensitive authentication data, verify that the application is intended only for issuers and/or companies that support issuing services.	▪ **Identify** whether the payment application stores sensitive authentication data (SAD) after authorization **(yes/no)** *If "no," proceed to 1.1.b.*	<Report Findings Here>			
	▪ *If "yes,"* **describe how** it was verified that the application is only intended for use by issuers and/or companies that support issuing services.	*<Report Findings Here>*			
1.1.b For all other payment applications, if sensitive authentication data (see 1.1.1–1.1.3 below) is stored prior to authorization, obtain and review methodology for securely deleting the data to verify that the data is unrecoverable.	▪ *If "no" at 1.1.a,* **identify** whether the payment application stores sensitive authentication data prior to authorization. **(yes/no)**	<Report Findings Here>			
	If "yes":				
	▪ **Identify** the document that defines the methodology for deleting the data such that the data is unrecoverable.	*<Report Findings Here>*			
	▪ **Describe how** the documented methodology was tested to confirm that that the data is unrecoverable.	*<Report Findings Here>*			
	If "no":				
	▪ **Describe the testing performed** to confirm that SAD is not stored by the application.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not In Place
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, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. ***Note:*** *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.* ***Aligns with PCI DSS Requirement 3.2.1***					

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not In Place
1.1.1 Install the payment application and perform numerous test transactions that simulate all functions of the payment application, including generation of error conditions and log entries. Use forensic tools and/or methods (commercial tools, scripts, etc.)[1] 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 or equivalent data on a chip are not stored after authorization. Include at least 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 *(continued on next page)*	▪ **Describe** the test transactions observed for this testing procedure.	*<Report Findings Here>*			
	▪ **Describe how** test transactions observed simulate all functions of the payment application, including generation of error conditions and log entries.	*<Report Findings Here>*			
	▪ **Identify forensic tools and/or methods (commercial tools, scripts, etc.) used** to examine all output created by the payment application to verify that the full contents of any track from the magnetic stripe on the back of the card or equivalent data on a chip are not stored after authorization.	*<Report Findings Here>*			
	For each data source type below, ***summarize the specific examples of each data source type observed*** *to confirm that full track data is never stored after authorization. If that type of data source is not present, indicate that in the space.*				
	▪ Incoming transaction data	*<Report Findings Here>*			
	▪ All logs (for example, transaction, history, debugging error)	*<Report Findings Here>*			
	▪ History files	*<Report Findings Here>*			
	▪ Trace files	*<Report Findings Here>*			
	▪ Non-volatile memory, including non-volatile cache	*<Report Findings Here>*			
	▪ Database schemas	*<Report Findings Here>*			

[1] 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 and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not In Place
	▪ Database contents	*<Report Findings Here>*			
	▪ If applicable, **any other output observed** to be generated by the payment application	*<Report Findings Here>*			
1.1.2 After authorization, do not store the card verification 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. ***Aligns with PCI DSS Requirement 3.2.2***					
1.1.2 Install the payment application and perform numerous test transactions that simulate all functions of the payment application, including generation of error conditions and log entries. Use forensic tools and/or methods (commercial tools, scripts, etc.) to examine all output created by the payment application and verify that the three-digit or four-digit card verification code printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored after authorization. Include at least 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 *(continued on next page)*	▪ **Describe** the test transactions observed for this testing procedure.	*<Report Findings Here>*			
	▪ **Describe how** test transactions observed simulate all functions of the payment application, including generation of error conditions and log entries.	*<Report Findings Here>*			
	▪ **Identify forensic tools and/or methods (commercial tools, scripts, etc.) used** to examine all output created by the payment application to verify that the three-digit or four-digit card-validation code printed on the card (CVV2, CVC2, CID, CAV2 data) is not stored after authorization.	*<Report Findings Here>*			
	For each data source type below, ***summarize the specific examples of each data source type observed*** *to confirm that card verification value or code is never stored after authorization.* *(If that type of data source is not present, indicate that in the space).*				
	▪ Incoming transaction data	*<Report Findings Here>*			
	▪ All logs (for example, transaction, history, debugging error)	*<Report Findings Here>*			
	▪ History files	*<Report Findings Here>*			
	▪ Trace files	*<Report Findings Here>*			
	▪ Non-volatile memory, including non-volatile cache	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not In Place
	▪ Database schemas	<*Report Findings Here*>			
	▪ Database contents	<*Report Findings Here*>			
	▪ If applicable, **any other output observed** to be generated by the payment application	<*Report Findings Here*>			
1.1.3 After authorization, do not store the personal identification number (PIN) or the encrypted PIN block. ***Aligns with PCI DSS Requirement 3.2.3***					
1.1.3 Install the payment application and perform numerous test transactions that simulate all functions of the payment application, including generation of error conditions and log entries. Use forensic tools and/or methods (commercial tools, scripts, etc.) to examine all output created by the payment application, and verify that PINs and encrypted PIN blocks are not stored after authorization. Include at least 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 *(continued on next page)*	▪ **Describe** the test transactions observed for this testing procedure.	<*Report Findings Here*>			
	▪ **Describe how** test transactions observed simulate all functions of the payment application, including generation of error conditions and log entries.	<*Report Findings Here*>			
	▪ **Identify forensic tools and/or methods (commercial tools, scripts, etc.) used** to examine all output created by the payment application to verify that the personal identification number (PIN) or the encrypted PIN block is not stored after authorization.	<*Report Findings Here*>			
	For each data source type below, ***summarize the specific examples of each data source type observed*** *to confirm that PIN or encrypted PIN block is never stored after authorization. If that type of data source is not present, indicate that in the space.*				
	▪ Incoming transaction data	<*Report Findings Here*>			
	▪ All logs (for example, transaction, history, debugging error)	<*Report Findings Here*>			
	▪ History files	<*Report Findings Here*>			
	▪ Trace files	<*Report Findings Here*>			
	▪ Non-volatile memory, including non-volatile cache	<*Report Findings Here*>			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not In Place
	▪ Database schemas	<*Report Findings Here*>			
	▪ Database contents	<*Report Findings Here*>			
	▪ If applicable, **any other output observed** to be generated by the payment application	<*Report Findings Here*>			
1.1.4 Securely delete any track data (from the magnetic stripe or equivalent data contained on a chip), card verification 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. ***Note:*** *This requirement applies only if previous versions of the payment application stored sensitive authentication data.* ***Aligns with PCI DSS Requirement 3.2***					
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 integrators/resellers: • Historical data must be removed (track data, card verification 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. *(continued on next page)*	▪ **Identify whether** any previous version of the payment application stored magnetic stripe data, card validation values or codes, and/or PINs or PIN block data. **(yes/no)**	<*Report Findings Here*>			
	If "no":				
	▪ **Describe how** it was verified that prior versions do not store magnetic stripe data, card validation values or codes, and/or PINs or PIN block data.	<*Report Findings Here*>			
	If "yes":				
	Identify the page number(s)/section of the *PA-DSS Implementation Guide* **verified** to include the following instructions for customers and integrators/resellers:				
	▪ That historical data must be removed (track data, card verification codes, PINs, or PIN blocks stored by previous versions of the payment application).	<*Report Findings Here*>			
	▪ Detailed procedures for removing historical data.	<*Report Findings Here*>			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not In Place
	▪ That such removal is absolutely necessary for PCI DSS compliance**.**	*<Report Findings Here>*			
1.1.4.b Examine payment application software files and configuration documentation to verify the vendor provides a secure wipe tool or procedure to remove the data.	▪ **Describe** the secure wipe tool or procedure the vendor provides to remove the data.	*<Report Findings Here>*			
	▪ **Identify** the payment application software files reviewed to verify the vendor provides a secure wipe tool or procedure to remove the data.	*<Report Findings Here>*			
	▪ **Identify** the configuration documentation reviewed to verify the vendor provides a secure wipe tool or procedure to remove the data.	*<Report Findings Here>*			
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.	▪ **Identify** the forensic tools and/or methods used to verify the tool or procedure securely removes the data.	*<Report Findings Here>*			
	▪ **Identify** the industry-accepted standard(s) for secure deletion of data.	*<Report Findings Here>*			
	▪ **Describe how** the tool or procedure was observed to verify secure removal of the data, in accordance with the industry-accepted standards.	*<Report Findings Here>*			
1.1.5 Do not store sensitive authentication data on vendor systems. If any sensitive authentication data (pre-authorization data) must be used for debugging or troubleshooting purposes, ensure the following: • Sensitive authentication data is collected only when needed to solve a specific problem • Such data is stored in a specific, known location with limited access • The minimum amount of data is collected as needed to solve a specific problem • Sensitive authentication data is encrypted with strong cryptography while stored • Data is securely deleted immediately after use, including from: – Log files – Debugging files – Other data sources received from customers. ***Aligns with PCI DSS Requirement 3.2***.					

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not In Place
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 *(continued on next page)*	▪ **Identify** the document that contains the software vendor's procedures for troubleshooting customers' problems.	*<Report Findings Here>*			
	▪ **Identify** whether the software vendor's procedures for troubleshooting customers' problems allow any collection of sensitive authentication data (pre-authorization). **(yes/no)** *If "no," mark the remainder of 1.1.5.a as "not applicable."*	*<Report Findings Here>*			
	*If "yes," briefly **describe how** the documented procedures for troubleshooting customers' problems ensure the following:*				
	▪ Collection of sensitive authentication data only when needed to solve a specific problem.	*<Report Findings Here>*			
	▪ Storage of such data in a specific, known location with limited access.	*<Report Findings Here>*			
	▪ Collection of only a limited amount of data needed to solve a specific problem**.**	*<Report Findings Here>*			
	▪ Encryption of sensitive authentication data while stored.	*<Report Findings Here>*			
	▪ Secure deletion of such data immediately after use**.**	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not In Place
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.	▪ **Identify the sample** of customer troubleshooting requests observed for this testing procedure.	*<Report Findings Here>*			
	▪ If collection of SAD is prohibited for troubleshooting, **describe how** actual events related to the sample of recent troubleshooting requests from customers were examined to verify there is no collection of SAD. ***Note:*** *If collection of SAD is prohibited, 1.1.5.c can be marked "not applicable."*	*<Report Findings Here>*			
	If collection of SAD is allowed for troubleshooting, for each troubleshooting request in the sample, ***describe how*** *the documented procedures were observed to be followed for each of the below:*				
	▪ Collection of sensitive authentication data only when needed to solve a specific problem**.**	*<Report Findings Here>*			
	▪ Storage of such data in a specific, known location with limited access.	*<Report Findings Here>*			
	▪ Collection of only a limited amount of data needed to solve a specific problem**.**	*<Report Findings Here>*			
	▪ Encryption of sensitive authentication data while stored.	*<Report Findings Here>*			
	▪ Secure deletion of such data immediately after use.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not In Place
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 integrators/resellers: • 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.	**Identify** the page number(s)/section of the *PA-DSS Implementation Guide* **verified** to include the following instructions for customers and integrators/resellers:				
	▪ Collection of sensitive authentication data only when needed to solve a specific problem	*<Report Findings Here>*			
	▪ Storage of such data in a specific, known location with limited access	*<Report Findings Here>*			
	▪ Collection of only a limited amount of data needed to solve a specific problem	*<Report Findings Here>*			
	▪ Encryption of sensitive authentication data while stored	*<Report Findings Here>*			
	▪ Secure deletion of such data immediately after use	*<Report Findings Here>*			

Requirement 2: Protect stored cardholder data

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not In Place
2.1 Software vendor must provide guidance to customers regarding secure deletion of cardholder data after expiration of customer-defined retention period. ***Aligns with PCI DSS Requirement 3.1***					
2.1 Review the *PA-DSS Implementation Guide* prepared by the vendor and verify the documentation includes the following guidance for customers and integrators/resellers: • Cardholder data exceeding the customer-defined retention period must be securely deleted • 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) • Instructions that customers need to securely delete cardholder data when no longer required for legal, regulatory, or business purposes *(Continued on next page)*	**Identify** the page number(s)/section of the *PA-DSS Implementation Guide* **verified** to include the following instructions for customers and integrators/resellers:				
	▪ Guidance that cardholder data exceeding the customer-defined retention period must be securely deleted	*<Report Findings Here>*			
	▪ 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)	*<Report Findings Here>*			
	▪ Instructions that customers need to securely delete cardholder data when no longer required for legal, regulatory, or business purposes	*<Report Findings Here>*			
	▪ Instructions on how to securely delete cardholder data stored by the payment application, including data stored on underlying software or systems (such as OS, databases, etc.).	*<Report Findings Here>*			
	▪ Instructions for configuring the underlying software or systems (such as OS, databases, etc.) to prevent inadvertent capture or retention of cardholder data, for example, system backup or restore points.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not In Place
• Instructions on how to securely delete cardholder data stored by the payment application, including data stored on underlying software or systems (such as OS, databases, etc.). • Instructions for configuring the underlying software or systems (such as OS, databases, etc.) to prevent inadvertent capture or retention of cardholder data—for example, system backup or restore points.	▪ Describe how all locations where the payment application stores cardholder data were observed to confirm that the list provided in the *PA-DSS Implementation Guide* is complete.	*<Report Findings Here>*			
	▪ Describe how the instructions provided in the PA-DSS Implementation Guide for securely deleting cardholder data stored by the payment application, including data stored on underlying software or systems (such as OS, databases, etc.) were observed to be effective.	*<Report Findings Here>*			
	▪ Describe how the instructions provided in *the PA-DSS Implementation Guide* for configuring underlying software or systems to prevent inadvertent capture or retention of cardholder data were observed to be effective.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not In Place
2.2 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN. ***Note:*** *This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.* ***Aligns with PCI DSS Requirement 3.3***					
2.2.a Review the *PA-DSS Implementation Guide* prepared by the vendor to verify the documentation includes the following guidance for customers and integrators/resellers: • Details of all instances where PAN is displayed, including but not limited to POS devices, screens, logs, and receipts. • Confirmation that the payment application masks PAN by default on all displays • Instructions for how to configure the payment application such that only personnel with a legitimate business need can see the full PAN.	**Identify** the page number(s)/section of the *PA-DSS Implementation Guide* **verified** to include the following instructions for customers and integrators/resellers:				
	▪ Details of all instances where PAN is displayed, including but not limited to POS devices, screens, logs, and receipts.	*<Report Findings Here>*			
	▪ Confirmation that the payment application masks PAN by default on all displays.	*<Report Findings Here>*			
	▪ Instructions for how to configure the payment application such that only personnel with a legitimate business need can see the full PAN.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not In Place
2.2.b Install the payment application and examine all displays of PAN data, including but not limited to POS devices, screens, logs, and receipts. For each instance where PAN is displayed, verify that PAN is masked when displayed.	▪ **List all displays of PAN data present and examined** (including but not limited to POS devices, screens, logs and receipts) to verify PAN is masked when displayed.	*<Report Findings Here>*			
	▪ For each instance where PAN is displayed, **describe how** observed PAN displays were masked.	*<Report Findings Here>*			
	▪ **Provide the name** of the PA-QSA who attests that the installed application was tested to confirm that the details of all instances where PAN is displayed documented in the *PA-DSS Implementation Guide* are complete and accurate.	*<Report Findings Here>*			
2.2.c Configure the payment application according to the *PA-DSS Implementation Guide* to allow only personnel with a legitimate business need to see the full PAN. For each instance where PAN is displayed, examine application configurations and displays of PAN to verify that instructions for masking PAN are accurate, and that only personnel with a legitimate business need can see the full PAN.	*For each instance where PAN is displayed:*				
	▪ **Describe the application configurations examined** to verify that instructions in the IG for masking PAN are accurate and that only personnel with a legitimate business need can see the full PAN.	*<Report Findings Here>*			
	▪ **Describe the displays of PAN examined** to verify that instructions in the IG for masking PAN are accurate and that only personnel with a legitimate business need can see the full PAN.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not In Place
2.3 Render PAN 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 (hash must be of the entire PAN) ▪ Truncation (hashing cannot be used to replace the truncated segment of PAN) ▪ Index tokens and pads (pads must be securely stored) ▪ Strong cryptography with associated key-management processes and procedures. ***Notes:*** • *It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are generated by a payment application, additional controls should be in place to ensure that hashed and truncated versions cannot be correlated to reconstruct the original PAN.* • *The PAN must be rendered unreadable anywhere it is stored, even outside the payment application (for example, log files output by the application for storage in the merchant environment).* ***Aligns with PCI DSS Requirement 3.4***					
2.3.a Review the *PA-DSS Implementation Guide* prepared by the vendor to verify the documentation includes the following guidance for customers and integrators/resellers: • Details of any configurable options for each method used by the application to render cardholder data unreadable, and instructions on how to configure each method for all locations where cardholder data is stored by the payment application (per PA-DSS Requirement 2.1). • A list of all instances where cardholder data may be output for the merchant to store outside of the payment application, and instructions that the merchant is responsible for rendering PAN unreadable in all such instances.	**Identify** the page number(s)/section of the *PA-DSS Implementation Guide* **verified** to include the following instructions for customers and integrators/resellers:				
	▪ Details of any configurable options for each method used by the application to render cardholder data unreadable.	*<Report Findings Here>*			
	▪ Instructions on how to configure each method for all locations where cardholder data is stored by the payment application (per PA-DSS Requirement 2.1).	*<Report Findings Here>*			
	▪ A list of all instances where cardholder data may be output for the merchant to store outside of the payment application.	*<Report Findings Here>*			
	▪ Instructions that the merchant is responsible for rendering PAN unreadable in all such instances.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not In Place
2.3.b Examine the method used to protect the PAN, including the encryption algorithms (if applicable). Verify that the PAN is rendered unreadable using any of the following methods: • One-way hashes based on strong cryptography. • Truncation • Index tokens and pads, with the pads being securely stored • Strong cryptography, with associated key-management processes and procedures	▪ **Identify the method(s)** below used to protect PAN: • One-way hashes based on strong cryptography • Truncation • Index tokens and pads, with the pads being securely stored • Strong cryptography, with associated key-management processes and procedures	*<Report Findings Here>*			
	▪ **Identify** the encryption algorithms (algorithm and key length) used (if applicable).	*<Report Findings Here>*			
	▪ **Describe** the processes observed to verify PAN is rendered unreadable using any of the following methods: • One-way hashes based on strong cryptography • Truncation • Index tokens and pads, with the pads being securely stored • Strong cryptography, with associated key-management processes and procedures	*<Report Findings Here>*			
2.3.c Examine several tables or files from data repositories created or generated by the application to verify the PAN is rendered unreadable.	▪ **Identify the sampled tables or files from data repositories** created or generated by the application observed to verify the PAN is rendered unreadable.	*<Report Findings Here>*			
	▪ For each item in the sample, **describe how** the tables or files were observed to confirm that PAN is rendered unreadable.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not In Place
2.3.d If the application creates or generates files for use outside the application (for example, files generated for export or backup), including for storage on removable media, examine a sample of generated files, including those generated on removable media (for example, back-up tapes), to confirm that the PAN is rendered unreadable.	▪ **Identify whether** there are instances where the application creates or generates files for use outside the application (for example, files generated for export or backup), including for storage on removable media. **(yes/no)** *If "no," mark the remainder of 2.3.d as "not applicable."*	*<Report Findings Here>*			
	If "yes," complete the following:				
	▪ **Provide the name of the PA-QSA who attests that** the list in the *PA-DSS Implementation Guide* of all instances where cardholder data may be output for the merchant to store outside of the payment application was observed to be accurate.	*<Report Findings Here>*			
	▪ **Identify the sample** of generated files observed.	*<Report Findings Here>*			
	▪ **Describe how** the generated files were observed to confirm that PAN is rendered unreadable. OR ▪ **Describe how** the generated files were observed to confirm that PAN is removed.	*<Report Findings Here>*			
2.3.e Examine a sample of audit logs created or generated by the application to confirm that the PAN is rendered unreadable or removed from the logs.	▪ **Identify the sample of audit logs** observed.	*<Report Findings Here>*			
	▪ **Describe how** the sample of audit logs was observed to confirm that PAN is rendered unreadable. OR ▪ **Describe how** the sample of audit logs was observed to confirm that PAN is removed from the logs.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not In Place
2.3.f 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 Requirements 2.3.b through 2.3.e, above.	▪ Identify whether the software vendor stores the PAN for any reason. **(yes/no)** *If "no," mark the remainder of 2.3.f as "not applicable"*	*<Report Findings Here>*			
	*If "yes," **describe how** it was verified that the PAN is rendered unreadable in accordance with Requirements 2.3.a through 2.3.e, as follows:*				
	▪ **Describe** the processes observed to confirm PAN is rendered unreadable using any of the methods defined in PA-DSS Requirement 2.3.b.	*<Report Findings Here>*			
	▪ **Describe** the processes observed to confirm PAN is rendered unreadable in several tables or files from data repositories, per PA-DSS Requirement 2.3.c.	*<Report Findings Here>*			
	▪ **Describe** the processes observed to confirm PAN is rendered unreadable in files generated for export or backup, including for storage on removable media, per PA-DSS Requirement 2.3.d.	*<Report Findings Here>*			
	▪ **Describe** the processes observed to confirm PAN is rendered unreadable or removed from audit logs, per PA-DSS Requirement 2.3.e.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not In Place
2.4 Payment application must protect keys used to secure cardholder data against disclosure and misuse. ***Note:*** *This requirement applies to keys used to encrypt stored cardholder data, as well as to key-encrypting keys used to protect data-encrypting keys. Such key-encrypting keys must be at least as strong as the data-encrypting key.* ***Aligns with PCI DSS Requirement 3.5***					
2.4.a Examine product documentation and interview responsible personnel to verify that controls are in place that restrict access to cryptographic keys used by the application.	▪ **Identify the product documentation** reviewed to verify that controls are in place to restrict access to cryptographic keys used by the application.	*<Report Findings Here>*			
	▪ **Identify** the responsible personnel interviewed for this testing procedure who confirm that controls are in place that restrict access to cryptographic keys used by the application.	*<Report Findings Here>*			
2.4.b Examine system configuration files to verify that: • Keys are stored in encrypted format. • Key-encrypting keys are stored separately from data-encrypting keys. • Key-encrypting keys are at least as strong as the data encrypting keys they protect.	▪ **Describe** the system configuration files observed.	*<Report Findings Here>*			
	▪ **Describe how** keys were observed to be stored in encrypted format.	*<Report Findings Here>*			
	▪ **Describe how** key-encrypting keys were observed to be stored separately from data-encrypting keys.	*<Report Findings Here>*			
	▪ **Describe how** key-encrypting keys were verified to be at least as strong as the data-encrypting keys they protect.	*<Report Findings Here>*			
2.4.c Review the *PA-DSS Implementation Guide* prepared by the vendor and verify that customers and integrators/resellers are instructed to: • Restrict access to keys to the fewest number of custodians necessary. • Store keys securely in the fewest possible locations and forms.	**Identify** the page number(s)/section of the *PA-DSS Implementation Guide* **verified** to include the following instructions for customers and integrators/resellers:				
	▪ Restrict access to keys to the fewest number of custodians necessary.	*<Report Findings Here>*			
	▪ Store keys securely in the fewest possible locations and forms.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not In Place
2.5 Payment application must implement key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including at least the following: ***Aligns with PCI DSS Requirement 3.6***					
2.5.a Review the *PA-DSS Implementation Guide* prepared by the vendor and verify the documentation includes the following instructions for customers and integrators/resellers: • How to securely generate, distribute, protect, change, store, and retire/replace encryption keys, where customers or integrators/resellers are involved in these key-management activities. • A sample Key Custodian form for key custodians to acknowledge that they understand and accept their key-custodian responsibilities.	▪ **Identify** whether customers or integrators/resellers are involved in key-management activities for this payment application/able to perform the following key functions. **(yes/no)** *If "no," mark the remainder of 2.5.x as "not applicable."*	*<Report Findings Here>*			
	Identify the page number(s)/section of the *PA-DSS Implementation Guide* **verified** to include the following instructions for customers and integrators/resellers:				
	▪ How to securely generate, distribute, protect, change, store, and retire/replace encryption keys, where customers or integrators/resellers are involved in these key-management activities.	*<Report Findings Here>*			
	▪ A sample Key Custodian form for key custodians to acknowledge that they understand and accept their key-custodian responsibilities.	*<Report Findings Here>*			
2.5.1 Generation of strong cryptographic keys					
2.5.1.a Review the *PA-DSS Implementation Guide* and verify it includes instructions for customers and integrators/resellers on how to securely generate cryptographic keys.	▪ **Identify** the page number(s)/section of the *PA-DSS Implementation Guide* verified to include instructions for customers and integrators/resellers on how to securely generate cryptographic keys.	*<Report Findings Here>*			
2.5.1.b Test the application, including the methods used to generate cryptographic keys, to verify that the instructions in the *PA-DSS Implementation Guide* result in the generation of strong cryptographic keys.	▪ **Describe the application testing performed** to confirm that the instructions in the *PA-DSS Implementation Guide* result in the generation of strong cryptographic keys.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not In Place
2.5.2 Secure cryptographic key distribution					
2.5.2.a Review the *PA-DSS Implementation Guide* and verify it includes instructions for customers and integrators/resellers on how to securely distribute cryptographic keys.	▪ **Identify** the page number(s)/section of the *PA-DSS Implementation Guide* **verified** to include instructions for customers and integrators/resellers on how to securely distribute cryptographic keys.	*<Report Findings Here>*			
2.5.2.b Test the application, including the methods used to distribute cryptographic keys, to verify that the instructions in the *PA-DSS Implementation Guide* result in the secure distribution of cryptographic keys.	▪ **Describe the application testing performed** to confirm that the instructions in the *PA-DSS Implementation Guide* result in the secure distribution of cryptographic keys.	*<Report Findings Here>*			
2.5.3 Secure cryptographic key storage					
2.5.3.a Review the *PA-DSS Implementation Guide* and verify it includes instructions for customers and integrators/resellers on how to securely store cryptographic keys.	▪ **Identify** the page number(s)/section of the *PA-DSS Implementation Guide* **verified** to include instructions for customers and integrators/resellers on how to securely store cryptographic keys.	*<Report Findings Here>*			
2.5.3.b Test the application, including the methods used to store cryptographic keys, to verify that the instructions in the *PA-DSS Implementation Guide* result in the secure storage of cryptographic keys.	▪ **Describe the application testing performed** to confirm that the instructions in the *PA-DSS Implementation Guide* result in the secure storage of cryptographic keys.	*<Report Findings Here>*			
2.5.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).					
2.5.4.a Review the PA-DSS Implementation Guide and verify it	**Identify** the page number(s)/section of the *PA-DSS Implementation Guide* **verified** to include the following instructions for customers and integrators/resellers:				

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not In Place
includes the following instructions for customers and integrators/resellers: • Defined cryptoperiod for each key type used by the application. • Procedures for enforcing key changes at the end of the defined cryptoperiod.	▪ Instructions for customers and integrators/resellers on defined cryptoperiod for each key type used by the applications.	*<Report Findings Here>*			
	▪ Procedures for enforcing key changes at the end of the defined cryptoperiod.	*<Report Findings Here>*			
2.5.4.b Test the application, including the methods for changing cryptographic keys, to verify the instructions in the PA-DSS Implementation *Guide* result in key changes at the end of the defined cryptoperiod.	▪ **Describe the application testing performed** to confirm that the instructions in the *PA-DSS Implementation Guide* result in key changes at the end of the defined cryptoperiod.	*<Report Findings Here>*			
2.5.5 Retirement or replacement of keys (for example: by archiving, destruction, and/or revocation as applicable) as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component, etc.) or keys are suspected of being compromised. ***Note:*** *If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encrypting key). Archived cryptographic keys should be used only for decryption/verification purposes.*					
2.5.5.a Review the *PA-DSS* Implementation Guide and verify it includes the following for customers and integrators/resellers: *(continued on next page)*	**Identify** the page number(s)/section of the *PA-DSS Implementation Guide* **verified** to include the following instructions for customers and integrators/resellers:				
	▪ Instructions that keys must be retired or replaced when the integrity of the key has been weakened, or there is a known or suspected compromise of a key.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not In Place
• Instructions that keys must be retired or replaced when the integrity of the key has been weakened, or there is a known or suspected compromise of a key. • Procedures for retiring or replacing keys (for example: by archiving, destruction, and/or revocation as applicable). • Procedures for ensuring that retired or replaced cryptographic keys are not used for encryption operations.	▪ Procedures for retiring or replacing keys.	*<Report Findings Here>*			
	▪ Procedures for ensuring that retired or replaced cryptographic keys are not used for encryption operations.	*<Report Findings Here>*			
2.5.5.b Test the application, including the methods for retiring or replacing cryptographic keys, to verify that the instructions in the *PA-DSS Implementation Guide* result the retirement or replacement of keys (for example: by archiving, destruction, and/or revocation as applicable).	▪ **Describe the application testing performed** to confirm that the instructions in the *PA-DSS Implementation Guide* result in the retirement or replacement of keys.	*<Report Findings Here>*			
2.5.5.c Test the application with the retired/replaced keys to verify that the instructions in the *PA-DSS Implementation Guide* ensure the application does not use retired or replaced keys for encryption operations.	▪ **Describe the application testing performed** to confirm that the instructions in the *PA-DSS Implementation Guide* ensure the application does not use retired or replaced keys for encryption operations.	*<Report Findings Here>*			
2.5.6 If the payment application supports manual clear-text cryptographic key-management operations, these operations must enforce split knowledge and dual control. ***Note:*** *Examples of manual key-management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.*					

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not In Place
2.5.6.a Review the *PA-DSS* Implementation Guide and verify it includes the following for customers and integrators/resellers: • Details of any manual clear-text cryptographic key-management operations supported by the application. • Instructions for enforcing split knowledge and dual control for all such operations.	▪ **Identify whether** the payment application supports manual clear-text cryptographic key-management operations. **(yes/no)** *If "no," mark the remainder of 2.5.6.a and 2.5.6.b as "not applicable."*	*<Report Findings Here>*			
	*If "yes," **identify** the page number(s)/section of the PA-DSS Implementation Guide **verified** to include the following instructions for customers and integrators/resellers:*				
	▪ Details of any manual clear-text cryptographic key-management operations supported by the application for customers and integrators/resellers.	*<Report Findings Here>*			
	▪ Instructions for enforcing split knowledge and dual control for all such operations.	*<Report Findings Here>*			
2.5.6.b Test the application, including all manual clear-text cryptographic key-management operations, to verify that the instructions in the *PA-DSS Implementation Guide* result in split knowledge and dual control of keys being required for all manual clear-text key-management procedures.	▪ **Describe the application testing performed** to confirm that the instructions in the *PA-DSS Implementation Guide* result in split knowledge and dual control of keys being required for all manual clear-text key-management procedures.	*<Report Findings Here>*			
2.5.7 Prevention of unauthorized substitution of cryptographic keys					
2.5.7.a Review the PA-DSS Implementation Guide and verify it includes instructions for customers and integrators/resellers on how to prevent unauthorized substitution of cryptographic keys	▪ **Identify** the page number(s)/section of the PA-DSS Implementation Guide **verified** to include instructions for customers and integrators/resellers on how to prevent unauthorized substitution of cryptographic keys.	*<Report Findings Here>*			
2.5.7.b Test the application, including all methods for substituting keys, to verify that the instructions in the *PA-DSS Implementation Guide* prevent unauthorized substitution of cryptographic keys.	▪ **Describe the application testing performed** to confirm that the instructions in the *PA-DSS Implementation Guide* result in the prevention of unauthorized substitution of cryptographic keys.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not In Place
2.6 Provide a mechanism to render irretrievable any cryptographic key material or cryptogram stored by the payment application, in accordance with industry-accepted standards. These are cryptographic keys used to encrypt or verify cardholder data. ***Note:*** *This requirement applies only if the payment application uses or previous versions of the payment application used cryptographic key materials or cryptograms to encrypt cardholder data.* ***Aligns with PCI DSS Requirement 3.6***					
2.6.a Review the *PA-DSS Implementation Guide* prepared by the vendor and verify the documentation includes the following instructions for customers and integrators/resellers: • Procedures detailing how to use the tool or procedure provided with the application to render cryptographic material irretrievable. • That cryptographic key material should be rendered irretrievable whenever keys are no longer used and in accordance with key-management requirements in PCI DSS. • Procedures for re-encrypting historic data with new keys, including procedures for maintaining security of clear-text data during the decryption /re-encryption process.	▪ **Identify** whether the application uses, or previous versions of the payment application used, cryptographic key materials or cryptograms to encrypt cardholder data. **(yes/no)** *If "no," mark the remainder of 2.6 as "not applicable."*	*<Report Findings Here>*			
	▪ **Identify** the page number(s)/section of the *PA-DSS Implementation Guide* **verified** to include the following instructions for customers and integrators/resellers:				
	• Procedures detailing how to use the tool or procedure provided with the application to render cryptographic material irretrievable.	*<Report Findings Here>*			
	• That cryptographic key material should be rendered irretrievable whenever keys are no longer used and in accordance with key-management requirements in PCI DSS.	*<Report Findings Here>*			
	• Procedures for re-encrypting historic data with new keys, including procedures for maintaining security of clear-text data during the decryption /re-encryption process.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not In Place
2.6.b Examine final application product to verify the vendor provides a tool and/or procedure with the application to render cryptographic material irretrievable.	▪ **Describe how** the final application product was examined to verify the vendor provides a tool and/or procedure with the application to render cryptographic material irretrievable	*<Report Findings Here>*			
	▪ **Describe the tool or procedure** provided by the vendor for rendering cryptographic material irretrievable.	*<Report Findings Here>*			
2.6.c Test the application, including the methods provided for rendering cryptographic key material irretrievable. Verify, through use of forensic tools and/or methods, that the secure wipe tool or procedure provided by the vendor renders the cryptographic material irretrievable, in accordance with industry-accepted standards.	▪ **Identify the forensic tools and/or methods** used to confirm that the secure wipe tool or procedure renders the cryptographic material irretrievable.	*<Report Findings Here>*			
	▪ **Describe the application testing performed** to confirm the vendor-provided tool or procedure renders the cryptographic material irretrievable.	*<Report Findings Here>*			
	▪ **Identify** the industry-accepted standards.	*<Report Findings Here>*			
2.6.d Test the methods for re-encrypting historic data with new keys, to verify the instructions in the *PA-DSS Implementation Guide* result in successful re-encryption of historic data with new keys.	▪ **Describe the testing performed** to confirm that the instructions in the *PA-DSS Implementation Guide* result in successful re-encryption of historic data with new keys.	*<Report Findings Here>*			

Requirement 3: Provide secure authentication features

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
3.1 The payment application must support and enforce the use of unique user IDs and secure authentication for all administrative access and for all access to cardholder data. Secure authentication must be enforced to all accounts generated or managed by the application by the completion of installation and for subsequent changes after installation. The application must enforce 3.1.1 through 3.1.11 below: ***Note:*** *The term "subsequent changes" as used throughout Requirement 3 refers to any application changes that result in user accounts reverting to default settings, changes to existing account configurations, and changes that generate new accounts or recreate existing accounts.* ***Note:*** *These password controls are not intended to apply to personnel who only have access to one card number at a time to facilitate a single transaction. These controls are applicable for access by personnel with administrative capabilities, for access to systems 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.* ***Aligns with PCI DSS Requirements 8.1 and 8.2***					
3.1.a Examine *PA-DSS Implementation Guide* created by the vendor to verify that customers and integrators/resellers are: • Provided clear and unambiguous directions on how the payment application enforces strong authentication for all authentication credentials that the application generates or manages, by: – Enforcing secure changes to authentication credentials by the completion of installation per Requirements 3.1.1 through 3.1.11. – Enforcing secure changes for any subsequent changes (after installation) to authentication credentials per Requirements 3.1.1 through 3.1.11. *(continued on next page)*	**Provide the name of the PA-QSA who attests** that review of the *PA-DSS Implementation Guide* confirmed that customers and integrators/resellers are provided clear and unambiguous directions on how the payment application enforces strong authentication for all authentication credentials that the application generates or manages, as follows: ▪ The payment application enforces strong authentication for all authentication credentials that the application generates by enforcing secure changes to authentication credentials by the completion of installation per Requirements 3.1.1 through 3.1.11. ▪ The payment application enforces strong authentication for all authentication credentials that the application generates by enforcing secure changes for any subsequent changes (after installation) to authentication credentials per Requirements 3.1.1 through 3.1.11.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
• Advised that, to maintain PCI DSS compliance, any changes made to authentication configurations would need to be verified as providing authentication methods that are at least as rigorous as PCI DSS requirements. • Advised to assign secure authentication to any default accounts (even if they won't be used), and then disable or do not use that accounts. • Provided clear and unambiguous directions for all authentication credentials used by the payment application (but which are not generated or managed by the application), on how, by the completion of installation and for any changes after installation, to change authentication credentials and create strong authentication per Requirements 3.1.1 through 3.1.11 below, for all application level and user accounts with administrative access and for all accounts with access to cardholder data.	▪ Customers and integrators/resellers are advised that, to maintain PCI DSS compliance, any changes made to authentication configurations would need to be verified as providing authentication methods that are at least as rigorous as PCI DSS requirements. ▪ Secure authentication should be assigned to any default accounts (even if they won't be used). ▪ Default accounts that won't be used should be disabled or deleted.	*<Continue Findings Here>*			
	▪ **Identify whether** there are any authentication credentials used by the payment application but that are not generated or managed by the application. **(yes/no)** *If "no," mark the rest of 3.1 as "not applicable."*	*<Report Findings Here>*			
	*If "yes," **provide the name of the PA-QSA who attests** that review of the* PA-DSS Implementation Guide *confirmed that that customers and integrators/resellers are provided clear and unambiguous directions on how to change authentication credentials and create strong authentication per Requirements 3.1.1 through 3.1.11 below for all application level and user accounts with administrative access and for all accounts with access to cardholder data, as follows:*				
	▪ How to change authentication credentials and create strong authentication per Requirements 3.1.1 through 3.1.11 for all application level accounts with administrative access by the completion of installation. ▪ How to change authentication credentials and create strong authentication per Requirements 3.1.1 through 3.1.11 for all for all access to cardholder data for any changes after installation.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
3.1.1 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 database default administrative account). ***Aligns with PCI DSS Requirement 2.1***					
3.1.1 Install and configure the payment application in accordance with the *PA-DSS Implementation Guide,* including configuring any administrative accounts for all necessary software. Test the payment application to verify the payment application does not use (or require the use of) default administrative accounts for necessary software.	▪ **Describe the testing performed** to verify that the payment application does not use default administrative accounts for other necessary software	*<Report Findings Here>*			
	▪ **Describe the testing performed** to verify that the payment application does not require the use of default administrative accounts for other necessary software	*<Report Findings Here>*			
3.1.2 The application must enforce the changing of all default application passwords for all accounts that are generated or managed by the application, by the completion of installation and for subsequent changes after installation. This applies to all accounts, including user accounts, application and service accounts, and accounts used by the vendor for support purposes. ***Note:*** *This requirement cannot be met through specifying a user process or via instructions in the PA-DSS Implementation Guide. At the completion of installation, and upon subsequent changes, the application must technically prevent any default or built-in accounts from being used until the default password has been changed.* ***Aligns with PCI DSS Requirement 2.1***					
3.1.2 For all accounts generated or managed by the application, test the application as follows:					
3.1.2.a Install the application in accordance with the *PA-DSS Implementation Guide*, examine account and password settings and attempt to use all default passwords to verify that the application enforces changes to any default payment application passwords by completion of the installation process.	▪ **Identify** account and password settings examined.	*<Report Findings Here>*			
	▪ **Describe how** attempts to use all default payment application passwords verified the application enforces changes to all default passwords by completion of the installation process.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
3.1.2.b Test all application functionality that results in user accounts reverting to default settings, changes to existing account configurations, generation of new accounts and recreation of existing accounts. For all types of changes performed, examine account and password settings and attempt to use all default passwords to verify that the application enforces changes to all default passwords upon completion of the change.	▪ **Identify** the application functionality present that results in user accounts reverting to default settings, changes to existing account configurations, generation of new accounts and recreation of existing accounts.	*<Report Findings Here>*			
	▪ **Identify** account and password settings examined for all type of changes performed.	*<Report Findings Here>*			
	▪ **Describe how** attempts to use all default payment application passwords verified the application enforces changes to all default passwords upon completion of the change.	*<Report Findings Here>*			
3.1.3 The payment application assigns unique IDs for user accounts. ***Aligns with PCI DSS Requirements 8.1.1***					
3.1.3 For all accounts that are generated or managed by the application, test the application as follows:					
3.1.3.a Install the payment application in accordance with the *PA-DSS Implementation Guide* and attempt to create different application accounts with the same user ID to verify that the payment application only assigns unique user IDs by completion of the installation process.	▪ **Describe how** attempts to create different application accounts with the same user ID verified the payment application only assigns unique user IDs by completion of the installation process.	*<Report Findings Here>*			
3.1.3.b Test all application functionality that results in user accounts reverting to default settings, changes to existing account configurations, generation of new accounts and recreation of existing accounts. *(continued on next page)*	▪ For the testing of all types of changes performed (as identified in 3.1.2.b), **identify** the account settings examined.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
For all types of changes performed, examine account settings and test application functionality to verify that unique user IDs are assigned for all accounts upon completion of the change.	▪ **Describe how** account settings were tested to verify that unique user IDs are assigned for all accounts upon completion of the change.	*<Report Findings Here>*			
	▪ **Describe** the application functionality testing performed to verify that unique user IDs are assigned for all accounts upon completion of the change.	*<Report Findings Here>*			
3.1.4 The payment application employs at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric ***Aligns with PCI DSS Requirements 8.2***					
3.1.4 For all accounts generated or managed by the application, test the application as follows:					
3.1.4.a Install the payment application in accordance with the *PA-DSS Implementation Guide* and test authentication methods to verify that the application requires at least one of the defined authentication methods for all accounts by completion of the installation process.	▪ **Identify** the authentication methods examined.	*<Report Findings Here>*			
	▪ **Describe the testing of authentication methods performed** to verify that the application requires at least one of the defined authentication methods for all accounts by completion of the installation process.	*<Report Findings Here>*			
3.1.4.b Test all application functionality that results in user accounts reverting to default settings, changes to existing account configurations, generation of new accounts and recreation of existing accounts. *(continued on next page)*	▪ For the testing of all types of changes performed (as identified in 3.1.2.b), **identify** the authentication methods examined.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
For all types of changes performed, test authentication methods to verify that the application requires at least one of the defined authentication methods for all accounts, upon completion of the change.	▪ **Describe how** authentication methods were tested to verify that the application requires at least one of the defined authentication methods for all accounts, upon completion of the change.	*<Report Findings Here>*			
	▪ **Describe** the application functionality testing performed to verify that the application requires at least one of the defined authentication methods for all accounts, upon completion of the change.	*<Report Findings Here>*			
3.1.5 The payment application does **not** require or use any group, shared, or generic accounts and passwords. ***Aligns with PCI DSS Requirement 8.5***					
3.1.5 For all accounts generated or managed by the application, test the application as follows:					
3.1.5.a Install the payment application in accordance with the *PA-DSS Implementation Guide*, examine account settings and test application functionality to verify that, by completion of the installation process, the application does not require or use any group, shared, or generic accounts and passwords.	▪ **Identify** the account settings examined.	*<Report Findings Here>*			
	▪ **Describe the testing of account settings performed** to verify that, by completion of the installation process, the application does not require or use:				
	• Any group accounts and passwords.	*<Report Findings Here>*			
	• Shared account s and passwords.	*<Report Findings Here>*			
	• Generic accounts and passwords.	*<Report Findings Here>*			
	▪ **Describe the testing of application functionality performed** to verify that, by completion of the installation process, the application does not require or use:				
	• Any group accounts and passwords.	*<Report Findings Here>*			
	• Shared account s and passwords.	*<Report Findings Here>*			
	• Generic accounts and passwords.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
3.1.5.b Test all application functionality that results in user accounts reverting to default settings, changes to existing account configurations, generation of new accounts and recreation of existing accounts. For all types of changes performed, examine account settings and test application functionality to verify that the application does not rely on or use any group, shared, or generic accounts and passwords upon completion of the change.	▪ For the testing of all types of changes performed (as identified in 3.1.2.b), **identify** the account settings examined.	*<Report Findings Here>*			
	▪ **Describe how** account settings were tested to verify that, upon completion of the change, the application does not rely on or use:				
	• Any group accounts and passwords.	*<Report Findings Here>*			
	• Shared account s and passwords.	*<Report Findings Here>*			
	• Generic accounts and passwords.	*<Report Findings Here>*			
	▪ **Describe the application functionality testing performed** to verify that, upon completion of the change, the application does not rely on or use:				
	• Any group accounts and passwords.	*<Report Findings Here>*			
	• Shared accounts and passwords.	*<Report Findings Here>*			
	• Generic accounts and passwords.	*<Report Findings Here>*			
3.1.6 The payment application requires that passwords meet the following: • Require a minimum length of at least seven characters • Contain both numeric and alphabetic characters Alternatively, the passwords/phrase must have complexity and strength at least equivalent to the parameters specified above.					

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
3.1.6 For all accounts generated or managed by the application, test the application as follows:					
3.1.6.a Install the payment application in accordance with the *PA-DSS Implementation Guide* and examine account settings to verify that by completion of the installation process, the application requires passwords to require a minimum of the following complexity and strength: • Be at least seven characters in length. • Contain both numeric and alphabetic characters.	▪ **Identify** the account settings examined.	*<Report Findings Here>*			
	▪ **Describe the testing of account settings performed** to verify that by completion of the installation process, the application requires:				
	• Passwords to be at least seven characters in length.	*<Report Findings Here>*			
	• Passwords to contain both numeric and alphabetic characters.	*<Report Findings Here>*			
3.1.6.b Test all application functionality that results in user accounts reverting to default settings, changes to existing account configurations, generation of new accounts and recreation of existing accounts. For all types of changes performed, examine account settings and test application functionality to verify that, upon completion of the change, the application requires passwords to require a minimum of the following complexity and strength: • Be at least seven characters in length. • Contain both numeric and alphabetic characters.	▪ For the testing of all types of changes performed (as identified in 3.1.2.b), **identify** the account settings examined.	*<Report Findings Here>*			
	▪ **Describe how** account settings were tested to verify that upon completion of the change, the application requires:				
	• Passwords to be at least seven characters in length.	*<Report Findings Here>*			
	• Passwords to contain both numeric and alphabetic characters.	*<Report Findings Here>*			
	▪ **Describe the application functionality testing performed** to verify that upon completion of the change, the application requires:				
	• Passwords to be at least seven characters in length.	*<Report Findings Here>*			
	• Passwords to contain both numeric and alphabetic characters.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
3.1.6.c If the application uses a different minimum character set and length for passwords, calculate the entropy of the passwords required by the application, and verify that it is at least equivalent to the parameters specified above (that is, at least as strong as seven characters in length with numeric and alphabetic characters).	▪ **Identify** whether the application uses a different minimum character set and length for passwords. **(yes/no)** *If "no," mark the rest of 3.1.6.c as "not applicable."*	*<Report Findings Here>*			
	If "yes":				
	▪ **Describe how** the entropy of the passwords required by the application was calculated.	*<Report Findings Here>*			
	▪ **Describe how** the calculated entropy was compared to the parameters specified above (at least as strong as seven characters in length with numeric and alphabetic character) and verified to be at least equivalent.	*<Report Findings Here>*			
3.1.7 The payment application requires changes to user passwords at least every 90 days. ***Aligns with PCI DSS Requirement 8.2.4***					
3.1.7 For all accounts generated or managed by the application, test the application as follows:					
3.1.7.a Install the payment application in accordance with the *PA-DSS Implementation Guide* and examine account settings to verify that the application requires user passwords to be changed at least every 90 days by completion of the installation process.	▪ **Identify** the account settings examined.	*<Report Findings Here>*			
	▪ **Describe the testing of account settings performed** to verify that the application requires user passwords to be changed at least every 90 days by completion of the installation process.	*<Report Findings Here>*			
3.1.7.b Test all application functionality that results in user accounts reverting to default settings, changes to existing account configurations, generation of new accounts and recreation of existing accounts. *(continued on next page)*	▪ For the testing of all types of changes performed (as identified in 3.1.2.b), **identify** the account settings examined.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
For all types of changes performed, examine account settings and test application functionality to verify that the application requires user passwords to be changed at least every 90 days upon completion of the change.	▪ **Describe how** account settings were tested to verify that the application requires user passwords to be changed at least every 90 days upon completion of the change.	*<Report Findings Here>*			
	▪ **Describe the application functionality testing performed** to verify that the application requires user passwords to be changed at least every 90 days upon completion of the change.	*<Report Findings Here>*			
3.1.8 The payment application keeps password history and requires that a new password is different than any of the last four passwords used. ***Aligns with PCI DSS Requirement 8.2.5***					
3.1.8 For all accounts generated or managed by the application, test the application as follows:					
3.1.8.a Install the payment application in accordance with the *PA-DSS Implementation Guide* and examine account settings to verify that, by completion of the installation process, the application keeps password history and requires that a new password is different than any of the last four passwords used.	▪ **Identify** the account settings examined.	*<Report Findings Here>*			
	▪ **Describe the testing of account settings performed** to verify that, by completion of the installation process, the application keeps password history.	*<Report Findings Here>*			
	▪ **Describe the testing of account settings performed** to verify that, by completion of the installation process, the application requires that a new password is different than any of the last four passwords used.	*<Report Findings Here>*			
3.1.8.b Test all application functionality that results in user accounts reverting to default settings, changes to existing account configurations, generation of new accounts and recreation of existing accounts. *(continued on next page)*	▪ For the testing of all types of changes performed (as identified in 3.1.2.b), **identify** the account settings examined.	*<Report Findings Here>*			
	Describe how account settings were tested to verify that, upon completion of the change, the application:				
	▪ Keeps password history.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
For all types of changes performed, examine account settings and test application functionality to verify that the application keeps password history and requires that a new password is different than any of the last four passwords used, upon completion of the change.	▪ Requires that a new password is different than any of the last four passwords used.	*<Report Findings Here>*			
	Describe the application functionality testing performed to verify that, upon completion of the change, the application:				
	▪ Keeps password history.	*<Report Findings Here>*			
	▪ Requires that a new password is different than any of the last four passwords used.	*<Report Findings Here>*			
3.1.9 The payment application limits repeated access attempts by locking out the user account after not more than six logon attempts. ***Aligns with PCI DSS Requirement 8.1.6***					
3.1.9 For all accounts generated or managed by the application, test the application as follows:					
3.1.9.a Install the payment application in accordance with the *PA-DSS Implementation Guide* and examine account settings to verify that, by completion of the installation process, the application locks out user accounts after not more than six invalid logon attempts.	▪ **Identify** the account settings examined.	*<Report Findings Here>*			
	▪ **Describe the testing of account settings performed** to verify that, by completion of the installation process, the application locks out user accounts after not more than six invalid logon attempts.	*<Report Findings Here>*			
3.1.9.b Test all application functionality that results in user accounts reverting to default settings, changes to existing account configurations, generation of new accounts and recreation of existing accounts. For all types of changes performed, examine account settings and test application functionality to verify that the application locks out user accounts after not more than six invalid logon attempts, upon completion of the change.	▪ For the testing of all types of changes performed (as identified in 3.1.2.b), **identify** the account settings examined.	*<Report Findings Here>*			
	▪ **Describe how** account settings were tested to verify that the application locks out user accounts after not more than six invalid logon attempts, upon completion of the change.	*<Report Findings Here>*			
	▪ **Describe the application functionality testing performed** to verify that the application locks out user accounts after not more than six invalid logon attempts, upon completion of the change.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
3.1.10 The payment application sets the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. ***Aligns with PCI DSS Requirement 8.1.7***					
3.1.10 For all accounts generated or managed by the application, test the application as follows:					
3.1.10.a Install the payment application in accordance with the *PA-DSS Implementation Guide* and examine account settings to verify that, by completion of the installation process, the application sets the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.	▪ **Identify** the account settings examined.	*<Report Findings Here>*			
	▪ **Describe the testing of account settings performed** to verify that by completion of the installation process, the application sets the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.	*<Report Findings Here>*			
3.1.10.b Test all application functionality that results in user accounts reverting to default settings, changes to existing account configurations, generation of new accounts and recreation of existing accounts. For all types of changes performed, examine account settings and test application functionality to verify that the application sets the lockout duration to a minimum of 30 minutes or until administrator enables the user ID, upon completion of the change.	▪ For the testing of all types of changes performed (as identified in 3.1.2.b), **identify** the account settings examined.	*<Report Findings Here>*			
	▪ **Describe how** account settings were tested to verify that the application sets the lockout duration to a minimum of 30 minutes or until administrator enables the user ID, upon completion of the change.	*<Report Findings Here>*			
	▪ **Describe the application functionality testing performed** to verify that the application sets the lockout duration to a minimum of 30 minutes or until administrator enables the user ID, upon completion of the change.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
3.1.11 If a payment application session has been idle for more than 15 minutes, the application requires the user to re-authenticate to re-activate the session. ***Aligns with PCI DSS Requirement 8.1.8***					
3.1.11 For all accounts generated or managed by the application, test the application as follows:					
3.1.11.a Install the payment application in accordance with the *PA-DSS Implementation Guide* and examine account settings to verify that, by completion of the installation process, the application sets a session idle time out to 15 minutes or less.	▪ **Identify** the account settings examined.	*<Report Findings Here>*			
	▪ **Describe the testing of account settings performed** to verify that, by completion of the installation process, the application sets a session idle time out to 15 minutes or less.	*<Report Findings Here>*			
3.1.11.b Test all application functionality that results in user accounts reverting to default settings, changes to existing account configurations, generation of new accounts and recreation of existing accounts. For all types of changes performed, examine account settings and test application functionality to verify that the application sets a session idle time out to 15 minutes or less, upon completion of the change.	▪ For the testing of all types of changes performed (as identified in 3.1.2.b), **identify** the account settings examined.	*<Report Findings Here>*			
	▪ **Describe how** account settings were tested to verify that the application sets a session idle time out to 15 minutes or less, upon completion of the change.	*<Report Findings Here>*			
	▪ **Describe the application functionality testing performed** to verify that the application sets a session idle time out to 15 minutes or less, upon completion of the change.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
3.2 Software vendor must provide guidance to customers that all access to PCs, servers, and databases with payment applications must require a unique user ID and secure authentication. ***Aligns with PCI DSS Requirements 8.1 and 8.2***					
3.2 Examine *PA-DSS Implementation Guide* created by vendor to verify customers and integrators/resellers are instructed 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.	**Identify** the page number(s)/section of the *PA-DSS Implementation Guide* **verified** to include the following instructions for customers and integrators/resellers:				
	▪ Control access to any PCs, servers, and databases with payment applications via unique user ID and PCI DSS-compliant secure authentication.	*<Report Findings Here>*			
	▪ Control access to any PCs, servers, and databases with cardholder data via unique user ID and PCI DSS-compliant secure authentication.	*<Report Findings Here>*			
3.3 Secure all payment application passwords (including passwords for user and application accounts) during transmission and storage. *Aligns with PCI DSS Requirement 8.2.1*					
3.3 Perform the following:					
3.3.1 Use strong cryptography to render all payment application passwords unreadable during transmission.					
3.3.1.a Examine vendor documentation and application configurations to verify that strong cryptography is used to render all passwords unreadable at all times during transmission.	▪ **Identify** the vendor documentation reviewed to verify it defines that strong cryptography is used to render all passwords unreadable at all times during transmission.	*<Report Findings Here>*			
	▪ **Identify** the application configurations examined to verify that strong cryptography is used to render all passwords unreadable at all times during transmission.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
3.3.1.b For all types of application passwords, examine transmissions of passwords (for example, by logging into the application from another system, and authenticating the application to other systems) to verify strong cryptography is used to render all passwords unreadable at all times during transmission.	▪ **Identify** the types of application passwords examined during transmission.	*<Report Findings Here>*			
	▪ **Identify** the strong cryptography verified to be used to render passwords unreadable at all times during transmission.	*<Report Findings Here>*			
	▪ **Describe how** strong cryptography was observed to render passwords unreadable at all times during transmission.	*<Report Findings Here>*			
3.3.2 Use a strong, one-way cryptographic algorithm, based on approved standards to render all payment application passwords unreadable during storage. Each password must have a unique input variable that is concatenated with the password before the cryptographic algorithm is applied. Note: The input variable does not need to be unpredictable or secure.					
3.3.2.a Examine vendor documentation and application configurations to verify that**:** • Stored passwords are rendered unreadable using a strong, one-way cryptographic algorithm, based on approved standards. • A unique input variable is concatenated with each password before the cryptographic algorithm is applied.	▪ **Identify** the vendor documentation reviewed and verified to define that: • Stored passwords are rendered unreadable using a strong, one-way cryptographic algorithm, based on approved standards. • A unique input variable is concatenated with each password before the cryptographic algorithm is applied.	*<Report Findings Here>*			
	▪ **Identify** the application configurations examined to verify that stored passwords are rendered unreadable using a strong, one-way cryptographic algorithm, based on approved standards.	*<Report Findings Here>*			
	▪ **Identify** the application configurations examined to verify that a unique input variable is concatenated with each password before the cryptographic algorithm is applied.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
3.3.2.b For all types of application passwords, identify all locations where the application may store passwords, including within the application itself, on underlying systems, log files, registry settings, etc. For all locations and types of passwords, examine stored password files during storage to verify that passwords are rendered unreadable using a strong, one-way cryptographic algorithm, with a unique input variable at all times when stored.	▪ **Identify** all locations where the application may store passwords.	*<Report Findings Here>*			
	▪ For all locations and types of passwords, **describe how** payment application password files were observed during storage to verify passwords are unreadable at all times during storage.	*<Report Findings Here>*			
	▪ **Identify** the strong cryptography verified to be used to render passwords unreadable at all times during storage.	*<Report Findings Here>*			
3.4 Payment application must limit access to required functions/resources and enforce least privilege for built-in accounts: • By default, all application/service accounts have access to only those functions/resources specifically needed for purpose of the application/service account. • By default, all application/service accounts have minimum level of privilege assigned for each function/resource as needed for the application/service account. ***Aligns with PCI DSS Requirement 7***					
3.4.1.a Install the payment application in accordance with the *PA-DSS Implementation Guide* and examine settings for built-in accounts to verify that, by completion of the installation process: • All application/service accounts have access to only those functions/resources specifically needed for purpose of the application/service account. • All application/service accounts have minimum level of privilege assigned for each function/resource as needed for the application/service account.	▪ **Identify** the settings for built-in accounts examined.	*<Report Findings Here>*			
	Describe how settings for built-in accounts were examined to verify that by completion of the installation process, all application/service accounts have:				
	▪ Access to only those functions/resources specifically needed for purpose of the application/service account.	*<Report Findings Here>*			
	▪ Minimum level of privilege assigned for each function/resource as needed for the application/service account.	*<Report Findings Here>*			
3.4.1.b Test all application functionality that results in changes to built-in	For all types of changes performed, **describe the account settings tested** to verify that, upon completion of the change, all application/service accounts have:				

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
accounts, including those that result in user accounts reverting to default settings, changes to existing account settings, generation of new accounts and recreation of existing accounts. For all types of changes performed, examine settings for built-in accounts and test application functionality to verify that upon completion of the change: • All application/service accounts have access to only those functions/resources specifically needed for purpose of the application/service account. • All application/service accounts have minimum level of privilege assigned for each function/resource as needed for the application/service account.	▪ Access to only those functions/resources specifically needed for purpose of the application/service account.	*<Report Findings Here>*			
	▪ Minimum level of privilege assigned for each function/resource as needed for the application/service account.	*<Report Findings Here>*			
	Describe the application functionality testing performed to verify that, upon completion of the change, all application/service accounts have:				
	▪ Access to only those functions/resources specifically needed for purpose of the application/service account.	*<Report Findings Here>*			
	▪ Minimum level of privilege assigned for each function/resource as needed for the application/service account.	*<Report Findings Here>*			

Requirement 4: Log payment application activity

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
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 and be able to link all activities to individual users. ***Aligns with PCI DSS Requirement 10.1***					
4.1.a Install the payment application. Test the application to verify that payment application audit trails are automatically enabled upon installation.	▪ **Describe the testing performed** on the installed application to verify that payment application audit trails are automatically enabled upon installation.	*<Report Findings Here>*			
4.1.b Examine the *PA-DSS Implementation Guide* prepared by the vendor to verify the following instructions are included: • How to install the application so that logs are configured and enabled by default upon completion of the installation process. • How to set PCI DSS-compliant log settings, per PA-DSS Requirements 4.2, 4.3 and 4.4 below, for any logging options that are configurable by the customer after installation. • Logs should not be disabled and doing so will result in non-compliance with PCI DSS. • How to configure PCI DSS-compliant log settings for any third-party software components packaged with or required by the payment application, for any logging options that are configurable by the customer after installation. *(continued on next page)*	**Identify** the page number(s)/section of the *PA-DSS Implementation Guide* **verified** to include the following instructions for customers and integrators/resellers:				
	▪ How to install the application so that logs are configured and enabled by default upon completion of the installation process.	*<Report Findings Here>*			
	▪ How to set PCI DSS-compliant log settings, per PA-DSS Requirements 4.2, 4.3 and 4.4 below, for any logging options that are configurable by the customer after installation.	*<Report Findings Here>*			
	▪ Logs should not be disabled and doing so will result in non-compliance with PCI DSS.	*<Report Findings Here>*			
	▪ How to configure PCI-compliant log settings for any third-party software components packaged with or required by the payment application, for any logging options that are configurable by the customer after installation.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
	▪ **Describe** how the *PA-DSS Implementation Guide* includes instructions on how to set PCI DSS-compliant log settings to reconstruct the events defined in PA-DSS Requirements 4.2.1-4.2.7.	*<Report Findings Here>*			
	▪ **Describe** how the *PA-DSS Implementation Guide* includes instructions on how to record at least the audit trail entries identified in PA-DSS Requirements 4.3.1-4.3.6, for each audited event.	*<Report Findings Here>*			
	▪ **Describe** how the *PA-DSS Implementation Guide* includes instructions on how to facilitate centralized logging, as defined in PA-DSS Requirement 4.4.	*<Report Findings Here>*			
4.2 Payment application must provide automated audit trails to reconstruct the following events: ***Aligns with PCI DSS Requirement 10.2***					
4.2 Test the payment application by examining payment application audit log settings and audit log output, and perform the following:					
4.2.1 All individual user accesses to cardholder data from the application					
4.2.1 Verify all individual access to cardholder data through the payment application is logged.	▪ **Identify** the payment application audit log settings examined.	*<Report Findings Here>*			
	▪ **Describe** the audit log output examined.	*<Report Findings Here>*			
	▪ **Describe the testing performed,** including examination of audit log settings and audit log output, to verify that all individual access to cardholder data through the payment application is logged.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
4.2.2 All actions taken by any individual with administrative privileges as assigned in the application					
4.2.2 Verify actions taken by any individual with administrative privileges to the payment application are logged.	▪ **Identify** the payment application audit log settings examined.	*<Report Findings Here>*			
	▪ **Describe** the audit log output examined.	*<Report Findings Here>*			
	▪ **Describe the testing performed**, including examination of audit log settings and audit log output, to verify that actions taken by any individual with administrative privileges to the payment application are logged.	*<Report Findings Here>*			
4.2.3 Access to application audit trails managed by or within the application					
4.2.3 Verify access to application audit trails managed by or within the application is logged.	▪ **Identify** the payment application audit log settings examined.	*<Report Findings Here>*			
	▪ **Describe** the audit log output examined.	*<Report Findings Here>*			
	▪ **Describe the testing performed**, including examination of audit log settings and audit log output, to verify that access to application audit trails managed by or within the application is logged.	*<Report Findings Here>*			
4.2.4 Invalid logical access attempts					
4.2.4 Verify invalid logical access attempts are logged.	▪ **Identify** the payment application audit log settings examined.	*<Report Findings Here>*			
	▪ **Describe** the audit log output examined.	*<Report Findings Here>*			
	▪ **Describe the testing performed**, including examination of audit log settings and audit log output, to verify that invalid logical access attempts are logged.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
4.2.5 Use of, and changes to the application's identification and authentication mechanisms (including but not limited to creation of new accounts, elevation of privileges, etc.), and all changes, additions, deletions to application accounts with root or administrative privileges					
4.2.5 Verify use of and changes to the payment application's identification and authentication mechanisms (including but not limited to creation of new accounts, elevation of privileges, etc.), and all changes, additions, deletions to application accounts with root or administrative privileges are logged.	▪ **Identify** the payment application audit log settings examined.	*<Report Findings Here>*			
	▪ **Describe** the audit log output examined.	*<Report Findings Here>*			
	▪ **Describe the testing performed**, including examination of audit log settings and audit log output, to verify that use of the payment application's identification mechanisms and all changes, additions, deletions to application accounts with root or administrative privileges are logged.	*<Report Findings Here>*			
	▪ **Describe the testing performed**, including examination of audit log settings and audit log output, to verify that changes to the payment application's authentication mechanisms and all changes, additions, deletions to application accounts with root or administrative privileges are logged.	*<Report Findings Here>*			
4.2.6 Initialization, stopping or pausing of the application audit logs					
4.2.6 Verify the following are logged: • Initialization of application audit logs. • Stopping or pausing of application audit logs. *(continued on next page)*	▪ **Identify** the payment application audit log settings examined.	*<Report Findings Here>*			
	▪ **Describe** the audit log output examined.	*<Report Findings Here>*			
	▪ **Describe the testing performed**, including examination of audit log settings and audit log output, to verify that initialization of application audit logs is logged.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
	▪ **Describe the testing performed**, including examination of audit log settings and audit log output, to verify that stopping or pausing of application audit logs is logged.	*<Report Findings Here>*			
4.2.7 Creation and deletion of system-level objects within or by the application					
4.2.7 Verify the creation and deletion of system-level objects within or by the application is logged.	▪ **Identify** the payment application audit log settings examined.	*<Report Findings Here>*			
	▪ **Describe** the audit log output examined.	*<Report Findings Here>*			
	▪ **Describe the testing performed,** including examination of audit log settings and audit log output, to verify that creation of system-level objects within or by the application is logged.	*<Report Findings Here>*			
4.3 Payment application must record at least the following audit trail entries for each event: ***Aligns with PCI DSS Requirement 10.3***					
4.3 Test the payment application by examining the payment application's audit log settings and audit log output, and, for each auditable event (from 4.2), perform the following:					
4.3.1 User identification					
4.3.1 Verify user identification is included in log entries.	▪ **Identify** the payment application audit log settings examined.	*<Report Findings Here>*			
	▪ **Describe** the audit log output examined.	*<Report Findings Here>*			
	▪ For each auditable event from 4.2.1-4.2.7, **describe the testing performed**, including examination of audit log settings and audit log output, to verify that user identification is included in log entries.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
4.3.2 Type of event					
4.3.2 Verify type of event is included in log entries.	▪ **Identify** the payment application audit log settings examined.	*<Report Findings Here>*			
	▪ **Describe** the audit log output examined.	*<Report Findings Here>*			
	▪ For each auditable event from 4.2.1-4.2.7, **describe the testing performed**, including examination of audit log settings and audit log output, to verify that type of event is included in log entries.	*<Report Findings Here>*			
4.3.3 Date and time					
4.3.3 Verify date and time stamp is included in log entries.	▪ **Identify** the payment application audit log settings examined.	*<Report Findings Here>*			
	▪ **Describe** the audit log output examined.	*<Report Findings Here>*			
	▪ For each auditable event from 4.2.1-4.2.7, **describe the testing performed**, including examination of audit log settings and audit log output, to verify that date and time stamp is included in log entries.	*<Report Findings Here>*			
4.3.4 Success or failure indication					
4.3.4 Verify success or failure indication is included in log entries.	▪ **Identify** the payment application audit log settings examined.	*<Report Findings Here>*			
	▪ **Describe** the audit log output examined.	*<Report Findings Here>*			
	▪ For each auditable event from 4.2.1-4.2.7, **describe the testing performed**, including examination of audit log settings and audit log output, to verify that success or failure indication is included in log entries.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
4.3.5 Origination of event					
4.3.5 Verify origination of event is included in log entries.	▪ **Identify** the payment application audit log settings examined.	*<Report Findings Here>*			
	▪ **Describe** the audit log output examined.	*<Report Findings Here>*			
	▪ For each auditable event from 4.2.1-4.2.7, **describe the testing performed,** including examination of audit log settings and audit log output, to verify that origination of event is included in log entries.	*<Report Findings Here>*			
4.3.6 Identity or name of affected data, system component, or resource					
4.3.6 Verify identity or name of affected data, system component, or resources is included in log entries.	▪ **Identify** the payment application audit log settings examined.	*<Report Findings Here>*			
	▪ **Describe** the audit log output examined.	*<Report Findings Here>*			
	▪ For each auditable event from 4.2.1-4.2.7, **describe the testing performed,** including examination of audit log settings and audit log output, to verify that identity or name of affected data, system component, or resources is included in log entries.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
4.4. Payment application must facilitate centralized logging. ***Note*:** Examples of this functionality may include, but are not limited to: • Logging via industry standard log file mechanisms such as Common Log File System (CLFS), Syslog, delimited text, etc. • Providing functionality and documentation to convert the application's proprietary log format into industry standard log formats suitable for prompt, centralized logging. ***Aligns with PCI DSS Requirement 10.5.3***					
4.4.a Examine the *PA-DSS Implementation Guide* prepared by the vendor to verify that customers and integrators/resellers are provided with: • A description of which centralized logging mechanisms are supported. • Instructions and procedures for incorporating the payment application logs into a centralized logging environment.	**Identify** the page number(s)/section of the *PA-DSS Implementation Guide* **verified** to include the following instructions for customers and integrators/resellers:				
	▪ A description of which centralized logging mechanisms are supported.	*<Report Findings Here>*			
	▪ Instructions and procedures for incorporating the payment application logs into a centralized logging environment.	*<Report Findings Here>*			
4.4.b Install and configure the payment application according to the *PA-DSS Implementation Guide* to verify that the instructions are accurate, and that functionality that facilitates a merchant's ability to assimilate logs into their centralized log server is provided.	Provide the name of the PA-QSA who attests that after installing and configuring the payment application according to the *PA-DSS Implementation Guide,* the following was verified to be true:				
	▪ The instructions in the *PA-DSS Implementation Guide* are accurate.	*<Report Findings Here>*			
	▪ Functionality that facilitates a merchant's ability to assimilate logs into their centralized log server is provided.	*<Report Findings Here>*			

Requirement 5: Develop secure payment applications

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
5.1 The software vendor has defined and implemented a formal process for secure development of payment applications, which includes: • Payment applications are developed in accordance with PCI DSS and PA-DSS (for example, secure authentication and logging). • Development processes are based on industry standards and/or best practices. • Information security is incorporated throughout the software development life cycle. • Security reviews are performed prior to release of an application or application update. ***Aligns with PCI DSS Requirement 6.3***					
5.1.a Examine documented software-development processes and verify that processes are based on industry standards and/or best practices.	▪ **Identify** the document that defines vendor software-development processes.	*<Report Findings Here>*			
	▪ **Identify** the industry standards and/or best practices the processes are verified to be based upon.	*<Report Findings Here>*			
5.1.b Verify documented software-development processes include procedures for the following: • Incorporating information security throughout the software development life cycle. • Developing payment applications in accordance with PCI DSS and PA-DSS Requirements.	▪ **Identify** the documented software-development processes reviewed and verified to include procedures for the following: • Incorporating information security throughout the software-development life cycle. • Developing payment applications in accordance with PCI DSS Requirements. • Developing payment applications in accordance with PA-DSS Requirements.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
5.1.c Verify documented software-development processes include: • Defined security reviews prior to release of an application or application update. • Procedures for security reviews to be performed to ensure the security objectives of PCI DSS and PA-DSS are being met.	▪ **Identify** the documented software development processes **reviewed and verified** to include procedures for the following: • Defined security reviews during the development process and prior to release of an application or application update. • Procedures for security reviews to be performed, to ensure the security objectives of PCI DSS and PA-DSS are being met.	*<Report Findings Here>*			
5.1.d Interview software developers to confirm that documented processes are followed such that: • Information security is incorporated throughout the software development life cycle. • Payment applications are developed in accordance with PCI DSS and PA-DSS Requirements. • Security reviews are performed at defined intervals throughout the development process and prior to release, to ensure that security objectives, including PCI DSS and PA-DSS requirements, are being met.	▪ **Identify** the software developers interviewed for this testing procedure who confirm that documented software development processes from 5.1.a, 5.1.b, and 5.1.c are followed such that: • Information security is incorporated throughout the software development life cycle. • Payment applications are developed in accordance with PCI DSS Requirements. • Payment applications are developed in accordance with PA-DSS Requirements. • Security reviews are performed prior to release, to ensure that security objectives, including PCI DSS and PA-DSS requirements, are being met.	*<Report Findings Here>*		

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
5.1.1 Live PANs are not used for testing or development. ***Aligns with PCI DSS Requirement 6.4.3***					
5.1.1.a Review software development processes to verify that they include procedures to ensure live PANs are not used for testing or development.	▪ **Identify** the documented software development processes **reviewed and verified** to include procedures for the following: • Procedures to ensure live PANs are not used for testing. • Procedures to ensure live PANs are not used for development.	*<Report Findings Here>*			
5.1.1.b Observe testing processes and interview personnel to verify live PANs are not used for testing or development.	**Describe the testing processes observed** to verify that:				
	▪ Live PANs are not used for testing.	*<Report Findings Here>*			
	▪ Live PANs are not used for development.	*<Report Findings Here>*			
	▪ **Identify** the personnel interviewed for this testing procedure who confirm that live PANS are not used for • Testing • Development	*<Report Findings Here>*			
5.1.1.c Examine samples of test data to verify live PANs are not used for testing or development.	**Describe** the samples of test data examined to verify that:				
	▪ Live PANs are not used for testing.	*<Report Findings Here>*			
	▪ Live PANs are not used for development.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
5.1.2 Test data and accounts are removed before release to customer. ***Aligns with PCI DSS Requirement 6.4.4***					
5.1.2.a Review software-development processes to verify they include procedures to ensure test data and accounts are removed before payment application is released to customers.	▪ **Identify** the documented software development processes reviewed and verified to include procedures for the following: • To ensure test data is removed before the payment application is released to customers. • To ensure accounts are removed before the payment application is released to customers.	*<Report Findings Here>*			
5.1.2.b Observe testing processes and interview personnel to verify test data and accounts are removed before release to customer.	**Describe the testing processes observed to verify that:**				
	▪ Test data is removed before the payment application is released to customers.	*<Report Findings Here>*			
	▪ Test accounts are removed before the payment application is released to customers.	*<Report Findings Here>*			
	▪ **Identify** the personnel interviewed for this testing procedure who confirm that: • Test data is removed before the payment application is released to customers. • Test accounts are removed before the payment application is released to customers.	*<Report Findings Here>*			
5.1.2.c Examine the final payment application product to verify test data and accounts are removed before release to customer.	**Describe** the final payment application product examined to verified that:				
	▪ Test data is removed before the payment application is released to customers.	*<Report Findings Here>*			
	▪ Test accounts are removed before the payment application is released to customers.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
5.1.3 Custom payment application accounts, user IDs, and passwords are removed before payment applications are released to customers ***Aligns with PCI DSS Requirement 6.3.1***					
5.1.3.a Review software-development processes to verify they include procedures to ensure custom payment application accounts, user IDs, and passwords are removed before payment application is released to customers.	▪ **Identify** the documented software-development processes **reviewed and verified** to include procedures for the following: • To ensure custom payment application accounts are removed before payment application is released to customers. • To ensure user IDs are removed before payment application is released to customers. • To ensure passwords are removed before payment application is released to customers.	*<Report Findings Here>*			
5.1.3.b Observe testing processes and interview personnel to verify that custom payment application accounts, user IDs, and passwords are removed before payment application is released to customers. *(continued on next page)*	**Describe the testing processes observed to verify that:**				
	▪ Custom payment application accounts are removed before the payment application is released to customers.	*<Report Findings Here>*			
	▪ User IDs are removed before the payment application is released to customers.	*<Report Findings Here>*			
	▪ Passwords are removed before the payment application is released to customers.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
	▪ **Identify** the personnel interviewed for this testing procedure who confirm that: • Custom payment application accounts are removed before the payment application is released to customers. • User IDs are removed before the payment application is released to customers. • Passwords are removed before the payment application is released to customers.	*<Report Findings Here>*			
5.1.3.c Examine the final payment application product to verify that custom payment application accounts, user IDs, and passwords are removed before payment application is released to customers.	**Describe** the final payment application product examined to verify that:				
	▪ Custom payment application accounts are removed before the payment application is released to customers.	*<Report Findings Here>*			
	▪ User IDs are removed before the payment application is released to customers.	*<Report Findings Here>*			
	▪ Passwords are removed before the payment application is released to customers.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
5.1.4 Payment application code is reviewed prior to release to customers after any significant change, to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: • 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. (See PA-DSS Requirement 5.2.) • Appropriate corrections are implemented prior to release. • Code-review results are reviewed and approved by management prior to release. • Documented code-review results include management approval, code author, and code reviewer, and what corrections were implemented prior to release. ***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. Code reviews can be conducted by knowledgeable internal personnel or third parties.* ***Aligns with PCI DSS Requirement 6.3.2***					

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
5.1.4.a Examine written software-development procedures and interview responsible personnel to verify the vendor performs code reviews for all significant application code changes (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. • Code reviews ensure code is developed according to secure coding guidelines. (See PA-DSS Requirement 5.2.) • Appropriate corrections are implemented prior to release. • Code-review results are reviewed and approved by management prior to release. • Code-review results are documented including management approval, code author and code reviewer, and what corrections were implemented prior to release. *(continued on next page)*	▪ **Identify** whether the vendor uses a manual or automated process to perform code reviews for all significant application code changes.	*<Report Findings Here>*			
	▪ **Identify** the documented software-development processes reviewed and verified to include procedures for the following: • Code changes are reviewed by individuals other than the originating code author. • Code changes are reviewed by individuals who are knowledgeable in code review techniques. • Code changes are reviewed by individuals who are knowledgeable in secure coding practices. • Code reviews ensure code is developed according to secure coding guidelines. • Appropriate corrections are implemented prior to release. • Code-review results are reviewed by management prior to release. • Code-review results are approved by management prior to release.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
	▪ **Identify** the responsible personnel interviewed for this testing procedure who confirm that vendor performs code reviews for all significant application code changes (either using manual or automated processes) as follows: • Whether the vendor uses a manual or automated process to perform code reviews for all significant application code changes. • Code changes are reviewed by individuals other than the originating code author. • Code changes are reviewed by individuals who are knowledgeable in code review techniques. • Code changes are reviewed by individuals who are knowledgeable in secure coding practices. • Code reviews ensure code is developed according to secure coding guidelines. • Appropriate corrections are implemented prior to release. • Code-review results are reviewed by management prior to release. • Code-review results are approved by management prior to release.	*<Report Findings Here>*			
5.1.4.b Examine code-review results for a sample of code changes to verify: • Code reviews were performed by a knowledgeable individual other than the code author. *(continued on next page)*	▪ **Identify the sample** of code changes examined.	*<Report Findings Here>*			
	Describe the code-review results for the sample of code changes observed to verify:				
	▪ Code changes are reviewed by individuals other than the originating code author.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
• Code reviews were developed according to secure coding guidelines. • Appropriate corrections were implemented prior to release. • Code-review results were reviewed and approved by management prior to release.	▪ Code changes are reviewed by individuals who are knowledgeable in code review techniques.	*<Report Findings Here>*			
	▪ Code changes are reviewed by individuals who are knowledgeable in secure coding practices.	*<Report Findings Here>*			
	▪ Code reviews ensure code is developed according to secure coding guidelines.	*<Report Findings Here>*			
	▪ Appropriate corrections are implemented prior to release.	*<Report Findings Here>*			
	▪ Code-review results are reviewed by management prior to release.	*<Report Findings Here>*			
5.1.5 Secure source-control practices are implemented to verify integrity of source code during the development process.					
5.1.5.a Examine written software-development procedures and interview responsible personnel to verify the vendor maintains secure source control practices to verify integrity of source code during the development process.	▪ **Identify** the written software-development procedures **reviewed** to confirm that the vendor maintains secure source control practices to verify integrity of source code during the development process.	*<Report Findings Here>*			
	▪ **Identify** the responsible personnel interviewed for this testing procedure who confirm that the vendor maintains secure source control practices to verify integrity of source code during the development process.	*<Report Findings Here>*			
5.1.5.b Examine mechanisms and observe procedures for securing source code to verify integrity of source code is maintained during the development process.	▪ **Identify** the mechanisms for securing source code examined to verify that the integrity of source code is maintained during the development process.	*<Report Findings Here>*			
	▪ **Describe the procedures for securing source code observed** to verify that the integrity of source code is maintained during the development process.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
5.1.6 Payment applications are developed according to industry best practices for secure coding techniques, including: • Developing with least privilege for the application environment. • Developing with fail-safe defaults (all execution is by default denied unless specified within initial design). • Developing for all access point considerations, including input variances such as multi-channel input to the application.					
5.1.6.a Examine software-development processes to verify that secure coding techniques are defined and include: • Developing with least privilege for the application environment. • Developing with fail-safe default (all execution is by default denied unless specified within initial design). • Developing for all access point considerations, including input variances such as multi-channel input to the application.	▪ **Identify** the software development processes **reviewed and verified** as having secure coding techniques defined that include: • Developing with least privilege for the application environment. • Developing with fail-safe default (all execution is by default denied unless specified within initial design). • Developing for all access point considerations, including input variances such as multi-channel input to the application.	*<Report Findings Here>*			
5.1.6.b Interview developers to verify that applications are developed according to industry best practices for secure coding techniques, including: • Developing with least privilege for the application environment. • Developing with fail-safe defaults (all execution is by default denied unless specified within initial design). • Developing for all access point considerations, including input variances such as multi-channel input to the application.	▪ **Identify** the developers interviewed for this testing procedure.	*<Report Findings Here>*			
	For the interview, **summarize the relevant details discussed** that verify that applications are developed according to industry best practices for secure coding techniques, including:				
	▪ Developing with least privilege for the application environment.	*<Report Findings Here>*			
	▪ Developing with fail-safe defaults (all execution is by default denied unless specified within initial design).	*<Report Findings Here>*			
	▪ Developing for all access point considerations, including input variances such as multi-channel input to the application.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
5.1.6.1 Coding techniques include documentation of how PAN and/or SAD are handled in memory.					
5.1.6.1.a Examine coding techniques to verify they include documentation of how PAN and/or SAD are handled in memory.	▪ **Identify** the documented coding techniques **reviewed to verify** coding techniques document how PAN and/or SAD are handled in memory.	*<Report Findings Here>*			
5.1.6.1.b Interview developers to verify that they consider how PAN/SAD is handled in memory during the application-development process.	▪ **Identify** the developers interviewed for this testing procedure.	*<Report Findings Here>*			
	▪ For the interview, **summarize the relevant details discussed** that verify that developers consider how PAN/SAD is handled in memory during the application-development process.	*<Report Findings Here>*			
5.1.7 Provide training in secure development practices for application developers, as applicable for the developer's job function and technology used, for example: • Secure application design • Secure coding techniques to avoid common coding vulnerabilities (for example, vendor guidelines, OWASP Top 10, SANS CWE Top 25, CERT Secure Coding, etc.) • Managing sensitive data in memory • Code reviews • Security testing (for example, penetration-testing techniques) • Risk-assessment techniques ***Note:*** *Training for application developers may be provided in-house or by third parties. Examples of how training may be delivered include on-the-job, instructor-led, and computer-based.*					
5.1.7a Verify documented software-development processes require training in secure development practices for application developers as applicable for the developer's job function and technology used.	▪ **Identify** the documented software-development processes reviewed to verify that processes require training in secure development practices for application developers as applicable for the developer's job function and technology used.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
5.1.7.b Interview a sample of developers to verify that they are knowledgeable in secure development practices and coding techniques, as applicable to the technology used.	▪ **Identify** the developers interviewed for this testing procedure.	*<Report Findings Here>*			
	For the interview, **summarize the relevant details discussed** that verify that:				
	▪ Interviewed developers are knowledgeable in secure development practices, as applicable to the technology used.	*<Report Findings Here>*			
	▪ Interviewed developers are knowledgeable in coding techniques, as applicable to the technology used.	*<Report Findings Here>*			
5.1.7.c Examine records of training to verify that all application developers receive training as applicable for their job function and technology used.	▪ **Identify** the sample of records of training examined	*<Report Findings Here>*			
	▪ **Describe how** the sample of records of training was examined to verify that all application developers receive training as applicable for their job function and technology used.	*<Report Findings Here>*			
5.1.7.1 Update training as needed to address new development technologies and methods used.					
5.1.7.1 Examine training materials and interview a sample of developers to verify that training is updated as needed to address new development technologies and methods used.	▪ **Identify** the training material examined to verify that training is updated as needed to address new development technologies and methods used.	*<Report Findings Here>*			
	▪ **Identify** the developers interviewed for this testing procedure.	*<Report Findings Here>*			
	▪ For the interview, **summarize the relevant details discussed** that verify that training is updated as needed to address new development technologies and methods used.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
5.2 Develop all payment applications to prevent common coding vulnerabilities in software-development processes: ***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 with industry best practices when this version of PA-DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Top 10, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.* ***Aligns with PCI DSS Requirement 6.5***					
5.2 Verify that 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:					
Note: *Requirements 5.2.1 through 5.2.6, below, apply to all payment applications (internal or external):*					
5.2.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.					
5.2.1 Injection flaws, particularly SQL injection, are addressed by coding techniques that include: • Validating input to verify user data cannot modify meaning of commands and queries. • Utilizing parameterized queries.	▪ For 5.2.1–5.2.10, **describe the penetration testing** techniques used, including whether manual or automated testing was used.	*<Report Findings Here>*			
	▪ **Describe how** the penetration testing results verified that coding techniques have addressed injection flaws, particularly SQL injection.	*<Report Findings Here>*			
5.2.2 Buffer Overflow					
5.2.2 Buffer Overflows are addressed by coding techniques that include: • Validating buffer boundaries. • Truncating input strings.	**Describe how** the penetration testing results verified that buffer overflows are addressed by coding techniques that include				
	▪ Validating buffer boundaries.	*<Report Findings Here>*			
	▪ Truncating input strings.	*<Report Findings Here>*			
5.2.3 Insecure cryptographic storage					
5.2.3 Insecure cryptographic storage is addressed by coding techniques that: • Prevent cryptographic flaws. • Use strong cryptographic algorithms and keys.	**Describe how** the penetration testing results verified that insecure cryptographic storage is addressed by coding techniques that:				
	▪ Prevent cryptographic flaws.	*<Report Findings Here>*			
	▪ Use strong cryptographic algorithms and keys.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
5.2.4 Insecure communications					
5.2.4 Insecure communications are addressed by coding techniques that properly authenticate and encrypt all sensitive communications.	**Describe how** the penetration testing results verified that insecure communications are addressed by coding techniques that:				
	▪ Properly authenticate all sensitive communications.	*<Report Findings Here>*			
	▪ Properly encrypt all sensitive communications.	*<Report Findings Here>*			
5.2.5 Improper error handling					
5.2.5 Improper error handling is addressed by coding techniques that do not leak information via error messages (for example, by returning generic rather than specific error details).	▪ **Describe how** the penetration testing results verified that improper error handling is addressed by coding techniques that do not leak information via error messages.	*<Report Findings Here>*			
5.2.6 All "high risk" vulnerabilities as identified in the vulnerability identification process at PA-DSS Requirement 7.1					
5.2.6 Coding techniques address any "high risk" vulnerabilities that could affect the application, as identified in PA-DSS Requirement 7.1	▪ **Describe how** the penetration testing results verified that coding techniques address any "high risk" vulnerabilities that could affect the application, as identified in PA-DSS Requirement 7.1.	*<Report Findings Here>*			
Note: *Requirements 5.2.7 through 5.2.10, below, apply to web-based applications and application interfaces (internal or external):*					
5.2.7 Cross-site scripting (XSS)					
5.2.7 Cross-site scripting (XSS) is addressed by coding techniques that include: • Validating all parameters before inclusion • Utilizing context-sensitive escaping	▪ Identify whether the payment application is web-based and/or includes web-based application interfaces (internal or external). (yes/no) *If "no," mark 5.2.7-5.2.10 as "not applicable."*	*<Report Findings Here>*			
	Describe how the penetration testing results verified that cross-site scripting (XSS) is addressed by coding techniques that include:				
	▪ Validating all parameters before inclusion.	*<Report Findings Here>*			
	▪ Utilizing context-sensitive escaping.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
5.2.8 Improper access control such as insecure direct object references, failure to restrict URL access, and directory traversal					
5.2.8 Improper access control, such as insecure direct object references, failure to restrict URL access, and directory traversal is addressed by coding technique that include: • Proper authentication of users. • Sanitizing input. • Not exposing internal object. references to users. • User interface does not permit. access to unauthorized functions.	**Describe how** the penetration testing results verified that improper access control, such as insecure direct object references, failure to restrict URL access, and directory traversal is addressed by coding technique that include:				
	▪ Proper authentication of users.	*<Report Findings Here>*			
	▪ Sanitizing input.	*<Report Findings Here>*			
	▪ Not exposing internal object references to users.	*<Report Findings Here>*			
	▪ User interface does not permit access to unauthorized functions.	*<Report Findings Here>*			
5.2.9 Cross-site request forgery (CSRF)					
5.2.9 Cross-site request forgery (CSRF) is addressed by coding techniques that ensure applications do not rely on authorization credentials and tokens automatically submitted by browsers.	▪ **Describe how** the penetration testing results verified that cross-site request forgery (CSRF) is addressed by coding techniques that ensure applications do not rely on authorization credentials and tokens automatically submitted by browsers.	*<Report Findings Here>*			
5.2.10 Broken Authentication and session management					
5.2.10 Broken authentication and session management is addressed via coding techniques that commonly include: • Flagging session tokens (for example cookies) as "secure." • Not exposing session IDs in the URL. • Incorporating appropriate time-outs and rotation of session IDs after a successful login.	▪ **Describe how** the penetration testing results verified that broken authentication and session management is addressed.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
5.3 Software vendor must follow change-control procedures for all application changes. Change-control procedures must follow the same software development processes as new releases (as defined in PA-DSS Requirement 5.1), and include the following: ***Aligns with PCI DSS Requirement 6.4.5***					
5.3.a Examine the vendor's change-control procedures for software modifications, and: • Verify the procedures follow documented software-development processes as defined in Requirement 5.1. • Verify that the procedures require items 5.3.1–5.3.4 below.	▪ **Identify** the document that defines the vendor's change-control procedures for software modifications, and which was verified to follow documented software-development processes as defined in Requirement 5.1: • Payment applications are developed in accordance with PCI DSS and PA-DSS. • Development processes are based on industry standards and/or best practices. • Information security is incorporated throughout the software development life cycle. • Security reviews are performed prior to release of an application or application update.	*<Report Findings Here>*			
	▪ **Identify** the document that defines the vendor's change-control procedures for software modifications, and which was verified to require items 5.3.1-5.3.4: • Documentation of impact. • Documented approval of change by appropriate authorized parties. • Functionality testing to verify that the change does not adversely impact the security of the system. • Back-out or product de-installation procedures.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
5.3.b Interview developers to determine recent payment application changes. Examine recent payment application changes and trace them back to related change-control documentation. For each change examined, verify the following was documented according to the change-control procedures:	▪ **Identify** recent payment application changes.	*<Report Findings Here>*			
	▪ **Identify the** recent payment application changes observed for 5.3.1-5.3.4.	*<Report Findings Here>*			
	▪ **Describe** how each of the recent payment application changes were traced back to **related change-control documentation.**	*<Report Findings Here>*			
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.	▪ For each payment application change examined, identify the related change-control documentation that includes customer impact.	*<Report Findings Here>*			
5.3.2 Documented approval of change by appropriate authorized parties					
5.3.2 Verify that documented approval by appropriate authorized parties is present for each change.	▪ For each payment application change examined, identify the related change-control documentation that includes documented approval by appropriate authorized parties.	*<Report Findings Here>*			
5.3.3 Functionality testing to verify that the change does not adversely impact the security of the system					
5.3.3.a For each sampled change, verify that functionality testing was performed to verify that the change does not adversely impact the security of the system.	▪ **For each payment application change examined, identify the related change-control documentation** that includes that functionality testing was performed to verify that the change did not adversely impact the security of the system.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
5.3.3.b Verify that all changes (including patches) are tested for compliance with 5.2 before being released.	▪ **For each payment application change examined, identify the related change-control documentation** that includes that the change was tested for compliance with 5.2 (that the vulnerabilities in 5.2.1–5.2.9 are addressed) prior to release.	*<Report Findings Here>*			
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.	▪ For each payment application change examined, identify the related change-control documentation that includes that back-out or product de-installation procedures are prepared for each change.	*<Report Findings Here>*			
5.4 The payment application vendor must document and follow a software-versioning methodology as part of their system development lifecycle. The methodology must follow the procedures in the *PA-DSS Program Guide* for changes to payment applications and include at least the following:					
5.4 Examine documented software development processes to verify they include the software vendor's versioning methodology, and that the versioning methodology must be in accordance with the *PA-DSS Program Guide.* Verify that the documented versioning methodology is required to be followed for the payment application, including all changes to the payment application.	▪ **Identify** the documented software development processes which were **verified** to: • Include the software vendor's versioning methodology. • Be in accordance with the *PA-DSS Program Guide.* • Be required to be followed for the payment application, including all changes to the payment application.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
5.4.1 The versioning methodology must define the specific version elements used, as follows: • Details of how the elements of the version scheme are in accordance with requirements specified in the *PA-DSS Program Guide.* • The format of the version scheme, including number of elements, separators, character set, etc. (consisting of alphabetic, numeric, and/or alphanumeric characters) • Definition of what each element represents in the version scheme (for example, type of change, major, minor, or maintenance release, wildcard, etc.) • Definition of elements that indicate use of wildcards ***Note:*** *Wildcards may only be substituted for elements of the version number that represent non-security impacting changes. Refer to 5.4.3 for additional requirements on the use of wildcards.*					
5.4.1.a Examine the documented versioning methodology to verify it includes the following: • Details of how the elements of the version numbering scheme are in accordance with requirements specified in the *PA-DSS Program Guide.* • The format of the version numbering scheme is specified and includes details of number of elements, separators, character set, etc. (e.g., 1.1.1.N, consisting of alphabetic, numeric, and/or alphanumeric characters). • A definition of what each element represents in the version-numbering scheme (e.g., type of change, major, minor, or maintenance release, wildcard, etc.). • Definition of elements that indicate use of wildcards.	**Identify the document reviewed** that verified the documented versioning methodology **includes**				
	▪ Details of how the elements of the version numbering scheme are in accordance with requirements specified in the *PA-DSS Program Guide.*	*<Report Findings Here>*			
	▪ The format of the version numbering scheme is specified and includes details of number of elements, separators, character set, etc.	*<Report Findings Here>*			
	▪ A definition of what each element represents in the version numbering scheme.	*<Report Findings Here>*			
	▪ Definition of elements that indicate use of wildcards.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
5.4.1.b Verify the elements of the version scheme are in accordance with the types of changes specified in the *PA-DSS Program Guide.*	▪ **Identify the version of the *PA-DSS Program Guide*** that the elements of the version scheme were verified to be in accordance with.	*<Report Findings Here>*			
5.4.1.c Examine recent payment application changes, the version number assigned, and the change-control documentation that specifies the type of application change, and verify that the elements in the version number match the applicable change and the parameters defined in the documented versioning methodology.	▪ **Describe** the types of recent payment application changes examined.	*<Report Findings Here>*			
	▪ **Identify** the associated change control documentation that specifies the type of application change.	*<Report Findings Here>*			
	▪ For each change examined, describe how the change to the version number is in accordance with their defined methodology.	*<Report Findings Here>*			
5.4.1.d Interview a sample of developers and verify that they are knowledgeable in the version scheme, including the acceptable use of wildcards in the version number.	▪ **Identify** the developers interviewed for this testing procedure.	*<Report Findings Here>*			
	For the interview, **summarize the relevant details discussed** that verify that they are knowledgeable in:				
	▪ The version scheme.	*<Report Findings Here>*			
	▪ The acceptable use of wildcards in the version number.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
5.4.2 The versioning methodology must indicate the type and impact of all application changes in accordance with the *PA-DSS Program Guide,* including: • Descriptions of all types and impacts of application changes • Specific identification and definition of changes that: – Have no impact on functionality of the application or its dependencies – Have impact on application functionality but no impact on security or PA-DSS requirements – Have impact to any security functionality or PA-DSS requirement. • How each type of change ties to a specific version number					
5.4.2.a Examine the software vendor's documented versioning methodology to verify the version methodology includes: • Description of all types and impacts of application changes (for example, changes that have no impact, low impact, or high impact to the application) • Specific identification and definition for changes that: – Have no impact on functionality of the application or its dependencies. – Have impact on application functionality but no impact on security or PA-DSS requirements. – Have impact to any security functionality or PA-DSS requirement. • How each type of change ties to a specific version number.	▪ **Identify** the software vendor's documented versioning methodology **that was verified** to include: • Description of all types and impacts of application changes. • Specific identification and definition for changes that: – Have no impact on functionality of the application or its dependencies. – Have impact on application functionality but no impact on security or PA-DSS requirements. – Have impact to any security functionality or PA-DSS requirement. • How each type of change ties to a specific version number.	*<Report Findings Here>*			
5.4.2.b Verify the versioning methodology is in accordance with the *PA-DSS Program Guide* requirements.	▪ Provide the name of the PA-QSA attesting that the documented versioning methodology is in accordance with the *PA-DSS Program Guide.*	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
5.4.2.c Interview personnel and observe processes for each type of change to verify that the documented methodology is being followed for all types of changes.	▪ **Identify** the responsible personnel interviewed who confirm that the documented methodology is followed for all types of changes.	*<Report Findings Here>*			
	▪ **Describe the processes observed** to verify that the documented methodology is followed for all types of changes.	*<Report Findings Here>*			
5.4.2.d Select a sample of recent payment application changes and review the change control documentation that specifies the type of application change to verify that the version assigned to the change matches the type of change according to the documented methodology.	▪ **Describe** the types of recent payment application changes examined.	*<Report Findings Here>*			
	▪ For each change examined, **identify** the category of change for each one, per the *PA-DSS Program Guide.*	*<Report Findings Here>*			
	▪ **Identify** the associated change control documentation that specifies the type of application change.	*<Report Findings Here>*			
	▪ For each change examined, describe: • How the version number changed (what the version number was and what it changed to). • How that version number change matches the category of change made to the payment application, according to the documented methodology.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
5.4.3 The versioning methodology must specifically identify if wildcards are used, and if so, how they are used. The following must be included: • Details of how wildcards are used in the versioning methodology • Wildcards are never used for any change that has an impact on security or any PA-DSS requirements • Any element of the version number used to represent a non-security-impacting change (including a wildcard element) must never be used to represent a security impacting change • Wildcard elements must not precede version elements that could represent security-impacting changes. Any version elements that appear after a wildcard element must not be used to represent security-impacting changes. ***Note:*** *Wildcards may only be used in accordance with the PA-DSS Program Guide.*					
5.4.3.a Examine the software vendor's documented versioning methodology to verify that it includes specific identification of how wildcards are used, including: • Details of how wildcards are used in the versioning methodology. • Wildcards are never used for any change that has an impact on security or any PA-DSS requirements. • Any element of the version number used to represent a non-security-impacting change (including a wildcard element) must never be used to represent a security impacting change. • Any elements to the right of a wildcard cannot be used for a security impacting change. • Security-impacting change requires a change to other version-number element that appears "to the left of" the first wildcard element.	▪ **Identify** the software vendor's documented versioning methodology that was verified to include: • Details of how wildcards are used in the versioning methodology. • Wildcards are never used for any change that has an impact on security or any PA-DSS requirements. • Any element of the version number used to represent a non-security-impacting change (including a wildcard element) must never be used to represent a security impacting change. • Any elements to the right of a wildcard cannot be used for a security impacting change. • Security-impacting change requires a change to other version-number element that appears "to the left of" the first wildcard element.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
5.4.3.b Verify that any use of wildcards is in accordance with the *PA-DSS Program Guide* requirements; For example, elements that appear after a wildcard element cannot be used for a security impacting change.	▪ **Identify whether** there is any use of wildcards in the vendor's version methodology. **(yes/no)** *If "no," mark the rest of 5.4.3.b as "not applicable."*	*<Report Findings Here>*			
	▪ *If "yes,"* **describe how** use of wildcards is in accordance with the *PA-DSS Program Guide* requirements.	*<Report Findings Here>*			
5.4.3.c Interview personnel and observe processes for each type of change to verify that: • Wildcards are never used for any change that has an impact on security or any PA-DSS requirements. • Elements of the version number used to represent non-security-impacting changes (including a wildcard element) are never be used to represent a security impacting change.	▪ **Identify** the responsible personnel interviewed for this testing procedure who confirm that for each type of change: • Wildcards are never used for any change that has an impact on security or any PA-DSS requirements. • Elements of the version number used to represent non-security-impacting changes (including a wildcard element) are never used to represent a security impacting change.	*<Report Findings Here>*			
	Describe the processes observed for each type of change to verify that:				
	▪ Wildcards are never used for any change that has an impact on security or any PA-DSS requirements.	*<Report Findings Here>*			
	▪ Elements of the version number used to represent non-security-impacting changes (including a wildcard element) are never used to represent a security impacting change.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
5.4.3.d Select a sample of recent payment application changes and review the change control documentation that specifies the type of application change. Verify that: • Wildcards are not used for any change that has an impact on security or any PA-DSS requirements. • Elements of the version number used to represent non-security-impacting changes (including a wildcard element) are not used to represent a security impacting change.	▪ **Identify** the sample of recent payment application changes examined.	*<Report Findings Here>*			
	▪ **Identify** the associated change-control documentation that specifies the type of application change.	*<Report Findings Here>*			
	Describe how the recent payment application changes and the change-control documentation were examined to verify that:				
	▪ Wildcards are never used for any change that has an impact on security or any PA-DSS requirements.	*<Report Findings Here>*			
	▪ Elements of the version number used to represent non-security-impacting changes (including a wildcard element) are never used to represent a security impacting change.	*<Report Findings Here>*			
5.4.4 The vendor's published versioning methodology must be communicated to customers and integrators/resellers.					
5.4.4 Verify the *PA-DSS Implementation Guide* includes a description of the vendor's published versioning methodology for customers and integrators/resellers, and includes the following: • Details of versioning scheme, including the format of the version scheme (number of elements, separators, character set, etc.). • Details of how security-impacting changes will be indicated by the version scheme. • Details of how other types of changes will affect the version. *(continued on next page)*	**Identify** the page number(s)/section of the *PA-DSS Implementation Guide* that include:				
	▪ Details of versioning scheme, including the format of the version scheme (number of elements, separators, character set, etc.).	*<Report Findings Here>*			
	▪ Details of how security-impacting changes will be indicated by the version scheme.	*<Report Findings Here>*			
	▪ Details of how other types of changes will affect the version.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
• Details of any wildcard elements that are used, including confirmation that they will never be used to represent a security-impacting change.	▪ Details of any wildcard elements that are used, including confirmation that they will never be used to represent a security-impacting change.	*<Report Findings Here>*			
5.4.5 If an internal version mapping to published versioning scheme is used, the versioning methodology must include mapping of internal versions to the external versions.					
5.4.5.a Examine the documented version methodology to verify it includes a mapping of internal versions to published external versions.	▪ **Identify** the software vendor's documented versioning methodology reviewed to verify it includes a mapping of internal versions to published external versions.	*<Report Findings Here>*			
5.4.5.b Examine recent changes to confirm internal version mapping to published versioning scheme, match according to the type of change.	▪ **Identify** recent payment application changes examined.	*<Report Findings Here>*			
	▪ **Describe how** examination of recent changes verified that mapping of internal and external version numbers was updated according to the documented methodology.	*<Report Findings Here>*			
5.4.6 Software vendor must have a process in place to review application updates for conformity with the versioning methodology prior to release.					
5.4.6.a Examine documented software-development processes and the versioning methodology to verify there is a process in place to review application updates for conformity with the versioning methodology prior to release.	▪ **Identify the** document that includes the process to review application updates for conformity with the versioning methodology prior to release.	*<Report Findings Here>*			
5.4.6.b Interview software developers and observe processes to verify that application updates are reviewed for conformity with the versioning methodology prior to release.	▪ **Identify** the software developers interviewed who confirm application updates are reviewed for conformity with the versioning methodology prior to release.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
	▪ **Describe the processes observed** to verify that application updates are reviewed for conformity with the versioning methodology prior to release.	*<Report Findings Here>*			
5.5 Risk assessment techniques (for example, application threat-modeling) are used to identify potential application security design flaws and vulnerabilities during the software-development process. Risk assessment processes include the following: • Coverage of all functions of the payment application, including but not limited to, security-impacting features and features that cross trust-boundaries. • Assessment of application decision points, process flows, data flows, data storage, and trust boundaries. • Identification of all areas within the payment application that interact with PAN and/or SAD or the cardholder data environment (CDE), as well as any process-oriented outcomes that could lead to the exposure of cardholder data. • A list of potential threats and vulnerabilities resulting from cardholder data-flow analyses and assign risk ratings (for example, high, medium, or low priority) to each. • Implementation of appropriate corrections and countermeasures during the development process. • Documentation of risk assessment results for management review and approval.					

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
5.5 Examine written software-development procedures and interview responsible personnel to verify the vendor uses risk assessment techniques as part of the software-development process, and that the processes include: • Coverage of all functions of the payment application, including but not limited to, security-impacting features and features that cross trust boundaries. • Assessment of application decision points, process flows, data flows, data storage, and trust boundaries. • Identification of all areas within payment applications that interact with PAN/SAD or the cardholder data environment (CDE), as well as any process-oriented outcomes that could lead to the exposure of cardholder data. • A list of potential threats and vulnerabilities resulting from cardholder data-flow analyses, and assign risk ratings (e.g., high, medium, or low priority) to each. • Implementation of appropriate corrections and countermeasures during the development process. • Documentation of risk assessment results for management review and approval. *(continued on next page)*	▪ **Identify** the documented software-development procedures verified to contain risk assessment techniques, and verified to include processes for: • Coverage of all functions of the payment application, including but not limited to, security-impacting features and features that cross trust boundaries. • Assessment of application decision points, process flows, data flows, data storage, and trust boundaries. • Identification of all areas within payment applications that interact with PAN/SAD or the cardholder data environment (CDE), as well as any process-oriented outcomes that could lead to the exposure of cardholder data. • A list of potential threats and vulnerabilities resulting from cardholder data-flow analyses, and assign risk ratings (e.g., high, medium, or low priority) to each. • Implementation of appropriate corrections and countermeasures during the development process. • Documentation of risk assessment results for management review and approval.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
	▪ **Identify** the software developers interviewed who confirm the vendor uses risk assessment techniques as part of the software-development process, and that the processes include: • Coverage of all functions of the payment application, including but not limited to, security-impacting features and features that cross trust boundaries. • Assessment of application decision points, process flows, data flows, data storage, and trust boundaries. • Identification of all areas within payment applications that interact with PAN/SAD or the cardholder data environment (CDE), as well as any process-oriented outcomes that could lead to the exposure of cardholder data. • A list of potential threats and vulnerabilities resulting from cardholder data-flow analyses, and assign risk ratings (e.g., high, medium, or low priority) to each. • Implementation of appropriate corrections and countermeasures during the development process. • Documentation of risk assessment results for management review and approval.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
5.6 Software vendor must implement a process to document and authorize the final release of the application and any application updates. Documentation includes: • Signature by an authorized party to formally approve release of the application or application update • Confirmation that secure development processes were followed by the vendor.					
5.6.a Examine documented processes to verify that final release of the application and any application updates must be formally approved and documented, including a signature by an authorized party to formally approve the release and confirmation that all SDLC processes were followed.	▪ **Identify** the documented processes reviewed to verify that final release of the application and any application updates must be formally approved and documented, and must include: • Formal approval and signature by an authorized party. • Confirmation that all SDLC processes were followed.	*<Report Findings Here>*			
5.6.b For a sample of recent releases of application and application updates, review approval documentation to verify it includes • Formal approval and signature by an authorized party. • Confirmation that that all secure development processes were followed.	▪ **Identify** the sample of recent releases of application and application updates reviewed for this testing procedure.	*<Report Findings Here>*			
	For each item in the sample of recent releases of application and application updates, **identify** the corresponding approval documentation that includes:				
	▪ Formal approval and signature by an authorized party.	*<Report Findings Here>*			
	▪ Confirmation that that all secure development processes were followed.	*<Report Findings Here>*			

Requirement 6: Protect wireless transmissions

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
6.1 For payment applications using wireless technology, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. The wireless technology must be implemented securely. ***Aligns with PCI DSS Requirements 1.2.3 & 2.1.1***					
6.1 For payment applications developed for use with wireless technology, and for all wireless applications bundled with the payment application, verify that the wireless applications do not use vendor default settings, as follows:					
6.1.a Examine the *PA-DSS Implementation Guide* prepared by the vendor to verify it includes the following instructions for customers and integrators/resellers: • The payment application enforces changes of default encryption keys, passwords and SNMP community strings at installation for all wireless components controlled by the application. • Procedures for changing wireless encryption keys and passwords, including SNMP strings, anytime anyone with knowledge of the keys/passwords leaves the company or changes positions. • Instructions for changing default encryption keys, passwords and SNMP community strings on any wireless components provided with, but not controlled by, the payment application. *(continued on next page)*	▪ **Identify** whether the payment application uses wireless technologies. **(yes/no)**	*<Report Findings Here>*			
	▪ **Identify** whether other applications bundled with the payment application use wireless technologies. **(yes/no)**	*<Report Findings Here>*			
	▪ *If both are "no,"* **describe testing performed** to verify the application is not developed for use with wireless technology. *If both are "no," mark the remainder of 6.1 and 6.2 as "not applicable" and proceed to 6.3.* *If either are "yes," complete the below.*	*<Report Findings Here>*			
	Identify the page number(s)/section of the *PA-DSS Implementation Guide* **verified** to include the following instructions for customers and integrators/resellers:				
	▪ The payment application enforces changes of default encryption keys, passwords and SNMP community strings at installation for all wireless components controlled by the application.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
• Instructions to install a firewall between any wireless networks and systems that store cardholder data. • Details of any wireless traffic (including specific port information) that the wireless function of the payment application would use. • Instructions to configure firewalls to deny or—if such traffic is necessary for business purposes—permit only authorized traffic between the wireless environment and the cardholder data environment.	▪ Procedures for changing wireless encryption keys and passwords, including SNMP strings, anytime anyone with knowledge of the keys/passwords leaves the company or changes positions.	*<Report Findings Here>*			
	▪ Instructions for changing default encryption keys, passwords and SNMP community strings on any wireless components provided with, but not controlled by, the payment application.	*<Report Findings Here>*			
	▪ Instructions to install a firewall between any wireless networks and systems that store cardholder data.	*<Report Findings Here>*			
	▪ Details of any wireless traffic (including specific port information) that the wireless function of the payment application would use.	*<Report Findings Here>*			
	▪ Instructions to configure firewalls to deny or—if such traffic is necessary for business purposes—permit only authorized traffic between the wireless environment and the cardholder data environment.	*<Report Findings Here>*			
6.1.b Install the application according to the *PA-DSS Implementation Guide* and test application and wireless settings to verify the following, for all wireless functionality managed by the payment application: • Encryption keys were changed from default at installation. • Default SNMP community strings on wireless devices were changed at installation. *(continued on next page)*	After installing the application according to the PA-DSS Implementation Guide**, describe the testing of the application and wireless settings** to verify the following for all wireless functionality managed by the payment application:				
	▪ Encryption keys were changed from default at installation	*<Report Findings Here>*			
	▪ Default SNMP community strings on wireless devices were changed at installation.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
• Default passwords/passphrases on access points were changed at installation. • Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks. • Other security-related wireless vendor defaults were changed, if applicable.	▪ Default passwords/passphrases on access points were changed at installation.	*<Report Findings Here>*			
	▪ Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks.	*<Report Findings Here>*			
	▪ Other security-related wireless vendor defaults were changed, if applicable.	*<Report Findings Here>*			
6.1.c For all wireless functionality managed by the payment application, follow instructions in the *PA-DSS Implementation Guide* for changing wireless encryption keys, passwords/passphrases and SNMP strings. Verify that the *PA-DSS Implementation Guide* instructions are accurate and result in changed wireless encryption keys, passwords and SNMP strings.	▪ *If wireless functionality is managed by the payment application*, **provide the name of the PA-QSA who attests that** the instructions in the *PA-DSS Implementation Guide* were followed to verify that the instructions are accurate and result in the required change for the following: • Change of wireless encryption keys • Change of passwords/passphrases • Change of SNMP strings	*<Report Findings Here>*			
6.1.d For all wireless components provided with, but not controlled by, the payment application, follow instructions in the *PA-DSS Implementation Guide* for changing default encryption keys, passwords/passphrases and SNMP community strings. Verify the *PA-DSS Implementation Guide* instructions are accurate and result in changed wireless encryption keys, passwords and SNMP strings.	▪ *If there are wireless components provided with, but not controlled by, the payment application*, **provide the name of the PA-QSA who attests that** the instructions in the *PA-DSS Implementation Guide* were followed to verify that the instructions are accurate and result in the required change for the following: • Change of wireless encryption keys • Change of passwords/passphrases • Change of SNMP strings	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
6.1.e Install the application and test wireless functions to verify the wireless traffic and ports used by the application are in accordance with those documented in the *PA-DSS Implementation Guide*.	**Describe the testing of the application and wireless settings on the installed application** to verify the following are in accordance with those documented in the *PA-DSS Implementation Guide*:				
	▪ Wireless traffic	*<Report Findings Here>*			
	▪ Wireless ports	*<Report Findings Here>*			
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. ***Note:*** *The use of WEP as a security control is prohibited.* ***Aligns with PCI DSS Requirement 4.1.1***					
6.2.a For payment applications developed for use with wireless technology, test all wireless functionality to verify the application uses industry best practices (for example, IEEE 802.11.i) to provide strong encryption for authentication and transmission.	*For payment applications developed for use with wireless technology*, **describe how** wireless functionality was tested to verify the use of industry best practices and use of strong encryption for:				
	▪ Strong encryption for authentication	*<Report Findings Here>*			
	▪ Strong encryption for transmission	*<Report Findings Here>*			
	▪ **Identify** the industry best practice(s) used for authentication.	*<Report Findings Here>*			
	▪ **Identify** the industry best practice(s) used for transmission.	*<Report Findings Here>*			
6.2.b For all wireless applications bundled with the payment application, test wireless functionality to verify that industry best practices (for example, IEEE 802.11.i) are used to provide strong encryption for authentication and transmission.	*For all wireless applications bundled with the payment application*, **describe how** wireless functionality was tested to verify the use of industry best practices and use of strong encryption for:				
	▪ Strong encryption for authentication	*<Report Findings Here>*			
	▪ Strong encryption for transmission	*<Report Findings Here>*			
	▪ **Identify** the industry best practice(s) used for authentication.	*<Report Findings Here>*			
	▪ **Identify** the industry best practice(s) used for transmission.	*<Report Findings Here>*			
6.2.c Examine the *PA-DSS Implementation Guide* prepared by the vendor to verify it includes the following instructions for customers and integrators/resellers:	**Identify** the page number(s)/section of the *PA-DSS Implementation Guide* **verified** to include the following instructions for customers and integrators/resellers:				
	▪ How to configure the application to use industry best practices for strong encryption for authentication**.**	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
• How to configure the application to use industry best practices (for example, IEEE 802.11.i) for strong encryption for authentication and transmission, and/or • How to configure all wireless applications bundled with the payment application to use industry best practices for strong encryption for authentication and transmission.	▪ How to configure the application to use industry best practices for strong encryption for transmission**.**	*<Report Findings Here>*			
	And/or:				
	Identify the page number(s)/section of the *PA-DSS Implementation Guide* **verified** to include the following instructions for customers and integrators/resellers:				
	▪ How to configure all wireless applications bundled with the payment application to use industry best practices for strong encryption for authentication**.**	*<Report Findings Here>*			
	▪ How to configure all wireless applications bundled with the payment application to use industry best practices for strong encryption for transmission.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
6.3 Provide instructions for customers about secure use of wireless technology. ***Note:*** *This requirement applies to all payment applications, regardless of whether the application is developed for use with wireless technologies.* ***Aligns with PCI DSS Requirements 1.2.3, 2.1.1 & 4.1.1***					
6.3 Examine *PA-DSS Implementation Guide* prepared by the vendor to verify customers and integrators/resellers are instructed on PCI DSS-compliant wireless settings, including changing wireless vendor defaults and using industry best practices to implement strong encryption for authentication and transmission of cardholder data, as follows: • Instructions to change all wireless default encryption keys, passwords and SNMP community strings upon installation. • Instructions to change wireless encryption keys, passwords and SNMP strings anytime anyone with knowledge of the keys/passwords leaves the company or changes positions. • Instructions to install a firewall between any wireless networks and systems that store cardholder data, and to configure firewalls to deny or, if such traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment. • Instructions to use industry best practices (for example, IEEE 802.11.i) to provide strong encryption for authentication and transmission.	▪ **Identify** the page number(s)/section of the PA-DSS Implementation Guide **verified** to include the following instructions for customers and integrators/resellers on PCI DSS-compliant wireless settings, as follows:				
	▪ Instructions to change all wireless default encryption keys, passwords and SNMP community strings upon installation.	*<Report Findings Here>*			
	▪ Instructions to change wireless encryption keys, passwords and SNMP strings anytime anyone with knowledge of the keys/passwords leaves the company or changes positions.	*<Report Findings Here>*			
	▪ Instructions to install a firewall between any wireless networks and systems that store cardholder data, and to configure firewalls to deny or, if such traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	*<Report Findings Here>*			
	▪ Instructions to use industry best practices (for example, IEEE 802.11.i) to provide strong encryption for authentication and transmission.	*<Report Findings Here>*			

Requirement 7: Test payment applications to address vulnerabilities and maintain application updates

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
7.1 Software vendors must establish a process to identify and manage vulnerabilities, as follows: ***Note:*** *Any underlying software or systems that are provided with or required by the payment application (for example, web servers, third-party libraries and programs) must be included in this process.* ***Aligns with PCI DSS Requirement 6.1***					
7.1.a Examine vulnerability management process documentation to verify procedures are defined to: • Identify new security vulnerabilities using reputable sources for obtaining security vulnerability information. • Assign a risk ranking to all identified vulnerabilities. • Test payment applications and updates for the presence of vulnerabilities prior to release.	▪ **Identify** the vulnerability management process documentation **verified** to define the following procedures: • Identify new security vulnerabilities using reputable sources for obtaining security vulnerability information. • Assign a risk ranking to all identified vulnerabilities. • Test payment applications for the presence of vulnerabilities prior to release. • Test updates for the presence of vulnerabilities prior to release	*<Report Findings Here>*			
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).	▪ **Identify** the vulnerability management process documentation **verified** to include processes to identify new vulnerabilities and implement corrections for all software: • Provided with the payment application. • Required by the payment application.	*<Report Findings Here>*			
	Describe the processes observed to identify new vulnerabilities for:				
	▪ All software provided with the payment application.	*<Report Findings Here>*			
	▪ All software required by the payment application.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
	Describe the processes observed to implement corrections for:				
	▪ All software provided with the payment application.	*<Report Findings Here>*			
	▪ All software required by the payment application.	*<Report Findings Here>*			
7.1.1 Identify new security vulnerabilities using reputable sources for obtaining security vulnerability information.					
7.1.1 Interview responsible personnel and observe processes to verify new security vulnerabilities are identified: • In both the payment application and any underlying software or systems provided with or required by the payment application. • Using reputable sources (such as software/systems vendor websites, NIST's NVD, MITRE's CVE, and the DHS's US-CERT websites).	▪ **Identify** the responsible personnel interviewed who confirm new security vulnerabilities are identified: • In both the payment application and any underlying software or systems provided with or required by the payment application. • Using reputable sources.	*<Report Findings Here>*			
	▪ **Identify** the outside sources identified as used for security vulnerability information via interview.	*<Report Findings Here>*			
	Describe the processes observed to verify that new security vulnerabilities are identified:				
	▪ In both the payment application and in any underlying software or systems provided with or required by the payment application.	*<Report Findings Here>*			
	▪ Using reputable sources.	*<Report Findings Here>*			
7.1.2 Assign a risk ranking to all identified vulnerabilities, including vulnerabilities involving any underlying software or systems provided with or required by the payment application. ***Note:*** *Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or impact to application functionality.* *Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the application. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat, impact critical application components, or would result in a potential compromise if not addressed.*					

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
7.1.2 Interview responsible personnel and observe processes to verify new security vulnerabilities are assigned a risk ranking, including vulnerabilities involving any underlying software or systems provided with or required by the payment application.	▪ **Identify** the responsible personnel interviewed who confirm that: • New security vulnerabilities are assigned a risk ranking. • Processes include ranking vulnerabilities in any underlying software or systems provided with or required by the payment application.	*<Report Findings Here>*			
	Describe the processes observed to verify that:				
	▪ New security vulnerabilities are assigned a risk ranking.	*<Report Findings Here>*			
	▪ Processes include ranking vulnerabilities in any underlying software or systems provided with or required by the payment application.	*<Report Findings Here>*			
7.1.3 Test payment applications and updates for the presence of vulnerabilities prior to release.					
7.1.3 Interview responsible personnel and observe processes to verify that payment applications are tested for the presence of vulnerabilities prior to release.	▪ **Identify** the responsible personnel interviewed who confirm that payment applications are tested for the presence of vulnerabilities prior to release.	*<Report Findings Here>*			
	▪ **Describe** the processes observed to verify that payment applications are tested for the presence of vulnerabilities prior to release.	*<Report Findings Here>*			
7.2 Software vendors must establish a process for timely development and deployment of security patches and upgrades.					

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
7.2 Examine process documentation for the development and distribution of security patches and upgrades to verify the process include procedures for 7.2.1 through 7.2.2:	▪ **Identify** the vulnerability management process documentation verified to include procedures for the development and distribution of security patches and upgrades, as follows: • Patches and updates are delivered to customers in a secure manner with a known chain of trust**.** • Patches and updates are delivered to customers in a manner that maintains the integrity of the patch and update code**.**	*<Report Findings Here>*			
7.2.1 Patches and updates are delivered to customers in a secure manner with a known chain of trust.					
7.2.1 Interview responsible personnel and observe processes to verify patches and updates are delivered to customers in a secure manner with a known chain of trust.	▪ **Identify** the responsible personnel interviewed who confirm that patches and updates are delivered to customers in a secure manner with a known chain of trust.	*<Report Findings Here>*			
	▪ **Describe the processes observed** to verify that patches and updates are delivered to customers in a secure manner with a known chain of trust.	*<Report Findings Here>*			
7.2.2 Patches and updates are delivered to customers in a manner that maintains the integrity of the patch and update code.					
7.2.2.a Interview responsible personnel and observe processes to verify patches and updates are delivered to customers in a manner that maintains the integrity of the patch and update code.	▪ **Identify** the responsible personnel interviewed who confirm that patches and updates are delivered to customers in a manner that maintains the integrity of the patch and update code.	*<Report Findings Here>*			
	▪ **Describe the processes observed** to verify that patches and updates are delivered to customers in a manner that maintains the integrity of the patch and update code.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
7.2.2.b Interview responsible personnel and observe application update processes to verify patches and updates are integrity-tested on the target system prior to installation.	▪ **Identify** the responsible personnel interviewed who confirm that patches and updates are integrity-tested on the target system prior to installation.	*<Report Findings Here>*			
	▪ **Describe the processes observed** to verify that patches and updates are integrity-tested on the target system prior to installation.	*<Report Findings Here>*			
7.2.2.c Verify that the integrity of patch and update code is maintained by running the update process with arbitrary code, and determine that the system will not allow the update to occur.	▪ **Describe how** the update process was run with arbitrary code.	*<Report Findings Here>*			
	▪ **Describe how** the testing was run to verify that the system will not allow the update to occur.	*<Report Findings Here>*			
7.3 Include release notes for all application updates, including details and impact of the update, and how the version number was changed to reflect the application update.					
7.3.a Examine processes for releasing updates and interview personnel to verify release notes are prepared for all updates, including details and impact of the update, and how the version number was changed to reflect the application update.	▪ **Identify** the process documentation **reviewed** to verify release notes are prepared for all updates, including details and impact of the update, and how the version number was changed to reflect the application update.	*<Report Findings Here>*			
	▪ **Identify** the responsible personnel interviewed who confirm release notes are prepared for all updates, including details and impact of the update, and how the version number was changed to reflect the application update.	*<Report Findings Here>*			
7.3.b Examine release notes for a sample of application updates and verify they were provided with the update.	▪ **Describe the sample** of application updates examined.	*<Report Findings Here>*			
	▪ **Identify** the release notes provided with each of the updates examined in the sampling.	*<Report Findings Here>*			
	▪ **Describe how** the release notes were verified to be provided with the update.	*<Report Findings Here>*			

Requirement 8: Facilitate secure network implementation

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
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 installation of patches, anti-malware protection, firewall configurations, or any other device, application, or configuration required for PCI DSS compliance.* ***Aligns with PCI DSS Requirements 1, 3, 4, 5, and 6***					
8.1.a Install the application in a PCI DSS compliant laboratory environment according to the *PA-DSS Implementation Guide*. Test the payment application to obtain evidence that it can run in a network that is fully compliant with PCI DSS.	▪ **Describe the testing performed** to verify that the payment application can run in a network that is fully compliant with PCI DSS.	*<Report Findings Here>*			
	▪ **Provide the name of the PA-QSA who attests that** the application was installed in a PCI DSS compliant laboratory environment, according to the *PA-DSS Implementation Guide,* consistent with Appendix B for confirmation of the configuration and setup of the lab.	*<Report Findings Here>*			
8.1.b Test the application and underlying systems to verify that the payment application does not preclude the use of or interfere with PCI DSS functions on underlying systems—for example, the application does not inhibit installation of patches or anti-malware updates—or interfere with the operation of other PCI DSS functions.	▪ **Describe** the testing performed on the application and underlying systems to verify that the payment application does not preclude the use of PCI DSS functions on underlying systems.	*<Report Findings Here>*			
	▪ **Describe** the testing performed on the application and underlying systems to verify that the payment application does not interfere with the use of PCI DSS functions on underlying systems.	*<Report Findings Here>*			
8.2 The payment application must only use or require use of necessary and secure services, protocols, daemons, components, and dependent software and hardware, including those provided by third parties, for any functionality of the payment application. *For example, if NetBIOS, file-sharing, Telnet, FTP, etc., are required by the application, they are secured via SSH, S-FTP, SSL, IPSec, or other technology.* ***Aligns with PCI DSS Requirement 2.2.2***					

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
8.2.a Examine system services, protocols, daemons, components, and dependent software and hardware enabled or required by the payment application. Verify that only necessary and secure services, protocols, daemons, components, dependent software and hardware are enabled by default "out of the box."	▪ **Identify** the system services, protocols, daemons, components, dependent hardware, and dependent software enabled or required by the payment application.	*<Report Findings Here>*			
	▪ **Describe the testing performed** to verify that only necessary and secure services, protocols, daemons, components, dependent software and hardware are enabled by default "out of the box."	*<Report Findings Here>*			
8.2.b Install the application and test application functions to verify that if the application supports any insecure services, daemons, protocols or components, they are securely configured by default "out of the box."	▪ **Provide the name** of the assessor who attests that the application was installed and application functions tested to verify that if the application supports any insecure services, daemons, protocols or components, they are securely configured by default "out of the box."	*<Report Findings Here>*			
8.2.c Verify that the *PA-DSS Implementation Guide* documents all required protocols, services, components, and dependent software and hardware that are necessary for any functionality of the payment application, including those provided by third parties.	**Identify** the page number(s)/section of the *PA-DSS Implementation Guide* **verified** to include documentation of the following required or necessary for the functionality of the payment application, including those provided by third parties:				
	▪ System services	*<Report Findings Here>*			
	▪ Protocols	*<Report Findings Here>*			
	▪ Components	*<Report Findings Here>*			
	▪ Dependent hardware	*<Report Findings Here>*			
	▪ Dependent software	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
8.3 The payment application must not require use of services or protocols that preclude the use of or interfere with normal operation of two-factor authentication technologies for secure remote access (network-level access originating from outside the network) to network resources residing within the CDE). ***Note:*** *Two-factor authentication requires that two of the three authentication methods (see below) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication. The authentication methods, also known as a factors, are:* • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric *Examples of two-factor technologies include RADIUS with tokens, TACACS with tokens, or other technologies that facilitate two-factor authentication.* ***Aligns with PCI DSS Requirement 8.3***					
8.3 Examine payment application functionality to verify it does not require use of any services or protocols that preclude the use of or interfere with the normal operation of two-factor authentication technologies for remote access.	▪ **Describe the payment application functionality examined** to verify that the payment application does not require use of services or protocols that preclude the use of or interfere with normal operation of two-factor authentication technologies for remote access.	*<Report Findings Here>*			
8.3.b Identify remote access mechanisms supported by the application and verify that the mechanisms do not prevent two-factor authentication.	▪ **Identify** remote access mechanisms (if any) supported by the application.	*<Report Findings Here>*			
	▪ **Describe testing performed** to verify the remote access mechanisms do not prevent two-factor authentication.	*<Report Findings Here>*			

Requirement 9: Cardholder data must never be stored on a server connected to the Internet

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
9.1 The payment application must be developed such that any web server and any cardholder data storage component (for example, a database server) are not required to be on the same server, nor is the data storage component required to be on the same network zone (such as a DMZ) with the web server. ***Aligns with PCI DSS Requirement 1.3.7***					
9.1.a Identify all payment application data storage components (for example, databases) and all web servers. Install data storage components and web servers on different servers and test application functionality across the different servers. Verify the payment application does not require any data storage component (such as a database) to be installed on the same server as a web server in order to function.	▪ **Identify** all data storage components.	*<Report Findings Here>*			
	▪ **Identify** all web servers.	*<Report Findings Here>*			
	▪ After installing data storage components and web servers on different servers, **describe the testing of application functionality across the different servers** that verified that the payment application does not require any data storage component to be installed on the same server as a web server.	*<Report Findings Here>*			
9.1.b Install data storage components and web servers on different network zones. Test all application functions across the network zones to verify that the payment application does not require any data storage component (such as a database) to be installed on the same network zone as a web server in order to function.	▪ After installing data storage components and web servers on different network zones, **describe the testing of application functionality across the different network zones** that verified that the payment application does not require any data storage component to be installed on the same network zone as a web server.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
9.1.c Examine *PA-DSS Implementation Guide* prepared by vendor to verify it includes the following instructions for customers and integrators/resellers: • Instructions not to store cardholder data on public-facing systems (for example, web server and database server must not be on same server). • Instructions on how to configure the payment application to use a DMZ to separate the Internet from systems storing cardholder data (for example, installing a web server component in a DMZ and installing a data storage component on an internal different network zone). • A list of services/ports that the application needs to use in order to communicate across two network zones (so the merchant can configure their firewall to open only required ports).	**Identify** the page number(s)/section of the *PA-DSS Implementation Guide* **verified** to include the following instructions for customers and integrators/resellers:				
	▪ Instructions not to store cardholder data on public-facing systems.	*<Report Findings Here>*			
	▪ Instructions on how to configure the payment application to use a DMZ to separate the Internet from systems storing cardholder data.	*<Report Findings Here>*			
	▪ A list of services/ports that the application needs to use in order to communicate across two network zones.	*<Report Findings Here>*			

Requirement 10: Facilitate secure remote access to payment application

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
10.1 Two-factor authentication must be used for all remote access to the payment application that originates from outside the customer environment. ***Note:*** *Two-factor authentication requires that two of the three authentication methods be used for authentication (see PA-DSS Requirement 3.1.4 for descriptions of authentication methods).* ***Aligns with PCI DSS Requirement 8.3***					
10.1.a Examine *PA-DSS Implementation Guide* prepared by the vendor to verify it contains the following instructions for customers and integrators/resellers: • Instructions that all remote access originating from outside the customer's network to the payment application must use two-factor authentication in order to meet PCI DSS requirements. • A description of two-factor authentication mechanisms supported by the application. • Instructions for configuring the application to support two-factor authentication (two of the three authentication methods described in PA DSS Requirement 3.1.4).	**Identify** the page number(s)/section of the *PA-DSS Implementation Guide* **verified** to include the following instructions for customers and integrators/resellers:				
	▪ Instructions that all remote access originating from outside the customer's network to the payment application must use two-factor authentication in order to meet PCI DSS requirements.	*<Report Findings Here>*			
	▪ A description of two-factor authentication mechanisms supported by the application**.**	*<Report Findings Here>*			
	▪ Instructions for configuring the application to support two-factor authentication (two of the three authentication methods described in PA DSS Requirement 3.1.4).	*<Report Findings Here>*			
10.1.b If the application vendor has remote access to a customer's payment application that originates from outside the customer environment, examine vendor policies to verify that the vendor supports customer requirements for two-factor authentication, for all such access. *(continued on next page)*	▪ **Identify whether** the application vendor has remote access to a customer's payment application that originates from outside the customer environment. **(yes/no)**	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
	If "yes:"				
	▪ **Identify** the vendor policy documentation examined to verify that the vendor supports customer requirements for two-factor authentication for all remote access that originates from outside the customer environment.	*<Report Findings Here>*			
	▪ **Describe** the two-factor technologies supported by the vendor including which factors are used (something you know, something you are, something you have).	*<Report Findings Here>*			
	If "no:"				
	▪ **Describe how** it was verified that the vendor does not have remote access to a customer payment application that originates from outside the customer environment.	*<Report Findings Here>*			
10.2 Any remote access into the payment application must be performed securely, as follows.					
10.2 Verify that any remote access is performed as follows:					
10.2.1 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 virtual private network (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. ***Aligns with PCI DSS Requirements 1 and 12.3.9***					

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
10.2.1.a If payment application updates are delivered via remote access into customers' systems, examine *PA-DSS Implementation Guide* prepared by vendor, and verify it contains: • Instructions for customers and integrators/resellers regarding secure use of remote-access technologies, specifying that remote-access technologies used by vendors and business partners should be activated only when needed and immediately deactivated after use. • Recommendation for customers and integrators/resellers to use a securely configured 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.	▪ **Identify whether** payment application updates are delivered via remote access into customers' systems. **(yes/no)** *If "no," mark 10.2.1 as not applicable above and proceed to 10.2.2.*	*<Report Findings Here>*			
	*If "yes," **identify** the page number(s)/section of the* PA-DSS Implementation Guide ***verified*** *to include the following instructions for customers and integrators/resellers:*				
	▪ Instructions regarding secure use of remote-access technologies, specifying that when used by vendors and business partners, it should be activated only when needed.	*<Report Findings Here>*			
	▪ Instructions regarding secure use of remote-access technologies, specifying that when used by vendors and business partners, it should be immediately deactivated after use.	*<Report Findings Here>*			
	▪ Recommendation for customers and resellers/ integrators to use a securely configured 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.	*<Report Findings Here>*			
10.2.1.b If the vendor delivers payment application and/or updates via remote access to customer networks, observe the vendor's methods for delivering payment application and/or updates via remote access to customer networks, and verify the vendor method includes: • Activation of remote-access	**Describe the methods observed** to verify that:				
	▪ Remote-access technologies to customer networks are activated only when needed.	*<Report Findings Here>*			
	▪ Remote-access technologies to customer networks are immediately deactivated after use.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
technologies to customer networks only when needed and immediate deactivation after use. • If remote access is via VPN or other high-speed connection, the connection is secured according to PCI DSS Requirement 1.	▪ The connection is secured according to PCI DSS Requirement 1 (if remote access is via VPN or other high-speed connection).	*<Report Findings Here>*			
10.2.2 If vendors or integrators/resellers can access customers' payment applications remotely, a unique authentication credential (such as a password/phrase) must be used for each customer environment. ***Aligns with PCI DSS Requirements 8.5.1***					
10.2.2 If vendors or integrators/resellers can access customers' payment applications remotely, examine vendor processes and interview personnel to verify that a unique password is used for each customer environment they have access to.	▪ Identify whether vendors, integrators/resellers, or customers can access customer's payment applications remotely. **(yes/no)** *If "no," mark 10.2.2 and 10.2.3 "not applicable."*	*<Report Findings Here>*			
	▪ *If "yes,"* **identify** the vendor policy documentation **verified** to include that a unique password to be used for each customer environment they have access to.	*<Report Findings Here>*			
	▪ **Identify** the responsible personnel interviewed who verify that a unique password is used for each customer environment the vendor has access to.	*<Report Findings Here>*			
	▪ Describe how processes observed verify that a unique password is used for each customer environment the vendor has access to.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
10.2.3 Remote access to customers' payment applications by vendors, integrators/resellers, or customers must be implemented securely, for example: • 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 (See PA-DSS Requirements 3.1.1 through 3.1.11). • Enable encrypted data transmission according to PA-DSS Requirement 12.1 • Enable account lockout after a certain number of failed login attempts (See PA-DSS Requirement 3.1.9 through 3.1.10.) • Establish a VPN connection via a firewall before access is allowed. • Enable the logging function. • Restrict access to customer environments to authorized integrator/resellers personnel. ***Aligns with PCI DSS Requirements 2, 8 and 10***					
10.2.3.a Examine PA-DSS Implementation Guide prepared by the vendor, and verify that customers and integrators/resellers are instructed that all remote access to the payment application must be implemented securely for example: • 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 (See PA-DSS Requirements 3.1.1 through 3.1.11) *(continued on next page)*	▪ **Identify** the page number(s)/section of the *PA-DSS Implementation Guide* **verified** to include instructions for customers and integrators/resellers that all remote access to the payment application must be implemented securely.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
• Enable encrypted data transmission according to PA-DSS Requirement 12.1 • Enable account lockout after a certain number of failed login attempts (See PA-DSS Requirement 3.1.9-3.1.10) • Establish a VPN connection via a firewall before access is allowed. • Enable the logging function. • Restrict access to customer environments to authorized personnel.	▪ **Describe** the PA-DSS Implementation Guide's instructions for customers and integrators/resellers for secure implementation of remote access to the payment application.	*<Report Findings Here>*			
10.2.3.b If the software vendor can access customers' payment applications remotely, observe the vendor's remote-access methods and interview personnel to verify the remote access is implemented securely.	▪ **Identify** whether the software vendor can access customers' payment applications remotely. **(yes/no)** *If "no," mark the remainder of 10.2.3.b as "not applicable."*	*<Report Findings Here>*			
	If "yes":				
	▪ **Describe** the software vendor's remote-access methods observed verify that remote access is implemented securely.	*<Report Findings Here>*			
	▪ **Identify** the responsible personnel interviewed who confirm that remote access is implemented securely.	*<Report Findings Here>*			

Requirement 11: Encrypt sensitive traffic over public networks

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
11.1 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 (for example, SSL/TLSIPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including at least the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use *Examples of open, public networks include but are not limited to:* • *The Internet* • *Wireless technologies, including but not limited to 802.11 and Bluetooth* • *Cellular technologies, for example, Global System for Mobile Communications (GSM), Code division multiple access (CDMA)* • *General Packet Radio Service (GPRS)* • *Satellite communications* ***Aligns with PCI DSS Requirement 4.1***					
11.1.a If the payment application sends, or facilitates sending, cardholder data over public networks, verify that strong cryptography and security protocols are provided with the application, or that use thereof is specified. *(continued on next page)*	▪ **Identify** whether the payment application sends or facilitates sending cardholder data over public networks. **(yes/no)**	*<Report Findings Here>*			
	▪ *If "no,"* **describe** the testing performed to verify the application cannot facilitate such transmissions.	*<Report Findings Here>*			
	If "yes:"				
	▪ **Identify** the strong cryptography provided with the payment application.	*<Report Findings Here>*			
	▪ **Identify** the security protocols provided with the payment application.	*<Report Findings Here>*			
	OR if "yes":				
	▪ **Identify** the strong cryptography specified for use.	*<Report Findings Here>*			
	▪ **Identify** the security protocols specified for use.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
	▪ **Describe how** the use of strong cryptography is specified.	*<Report Findings Here>*			
	▪ **Describe how** the use of security protocols is specified.	*<Report Findings Here>*			
11.1.b Examine *PA-DSS Implementation Guide* prepared by the vendor, and verify the vendor includes directions for customers and integrators/resellers to use the strong cryptography and security protocols provided by or specified for use with the application, including: • Instructions that strong cryptography and security protocols must be used if cardholder data is ever transmitted over public networks. • Instructions for verifying that only trusted keys and/or certificates are accepted. • How to configure the payment application to use only secure versions and secure implementations of security protocols. • How to configure the payment application to use the proper encryption strength for the encryption methodology in use.	**Identify** the page number(s)/section of the *PA-DSS Implementation Guide* **verified** to include the following directions for customers and integrators/resellers:				
	▪ Instructions that strong cryptography and security protocols must be used if cardholder data is ever transmitted over public networks.	*<Report Findings Here>*			
	▪ Instructions for verifying that only trusted keys and/or certificates are accepted.	*<Report Findings Here>*			
	▪ How to configure the payment application to use only secure versions and secure implementations of security protocols.	*<Report Findings Here>*			
	▪ How to configure the payment application to use the proper encryption strength for the encryption methodology in use.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
11.1.c If strong cryptography and security protocols are provided with the payment application, install and test the application according to instructions in the *PA-DSS Implementation Guide*, and verify: • The protocol is implemented by default to use only trusted keys and/or certificates. • The protocol is implemented by default to use only secure configurations and does not support insecure versions or configurations. • Proper encryption strength is implemented for the encryption methodology in use.	*If it was noted in 11.1.a that strong cryptography and security protocols are provided with the payment application*: After installing the application according to instructions in the PA-DSS Implementation Guide, **describe testing performed** to verify the following**:**				
	▪ The protocol is implemented by default to use only trusted keys and/or certificates.	*<Report Findings Here>*			
	▪ The protocol is implemented by default to use only secure configurations.	*<Report Findings Here>*			
	▪ The protocol is implemented by default to not support insecure versions or configurations.	*<Report Findings Here>*			
	▪ Proper encryption strength is implemented for the encryption methodology in use.	*<Report Findings Here>*			
11.2 If the payment application facilitates sending of PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat), the payment application must provide a solution that renders the PAN unreadable or implements strong cryptography, or specify use of strong cryptography to encrypt the PANs. ***Aligns with PCI DSS Requirement 4.2***					
11.2.a If the payment application allows and/or facilitates sending of PANs by end-user messaging technologies, verify that a solution that renders the PAN unreadable or implements strong cryptography is provided, or that use thereof is specified. *(continued on next page)*	▪ Identify whether the payment application allows and/or facilitates the sending of PANs by end-user messaging technologies. **(yes/no)**	*<Report Findings Here>*			
	▪ *If "no,"* **describe how** the application was observed to prevent such action.	*<Report Findings Here>*			
	If "yes," either: ▪ **Identify and describe** the solution provided with the application that:				
	• Renders the PAN unreadable; OR	*<Report Findings Here>*			
	• Implements strong cryptography.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
	OR (if "yes"): ▪ **Identify and describe** the solution specified for use that:				
	• Renders the PAN unreadable; OR	*<Report Findings Here>*			
	• Implements strong cryptography.	*<Report Findings Here>*			
	▪ **Describe how** use of the solution is specified.	*<Report Findings Here>*			
11.2.b Examine *PA-DSS Implementation Guide* prepared by the vendor, and verify the vendor includes directions for customers and integrators/resellers to use a solution provided with or specified for use with the application, including: • Procedures for using the defined solution to render the PAN unreadable or secure the PAN with strong cryptography. • Instruction that PAN must always be rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies.	**Identify** the page number(s)/section of the PA-DSS Implementation Guide **verified** to include directions for customers and integrators/resellers to use a solution provided with or specified for use with the application, including:				
	▪ Procedures for using the defined solution to render the PAN unreadable or secure the PAN with strong cryptography.	*<Report Findings Here>*			
	▪ Instruction that PAN must always be rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies.	*<Report Findings Here>*			
11.2.c If a solution is provided with the payment application, install and test the application to verify that the solution renders the PAN unreadable or implements strong cryptography.	*If the payment application provides the solution:* After installing the payment application, **describe testing performed** to verify that:				
	▪ The solution renders the PAN unreadable; OR	*<Report Findings Here>*			
	▪ The solution implements strong cryptography.	*<Report Findings Here>*			

Requirement 12: Encrypt all non-console administrative access

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
12.1 If the payment application facilitates non-console administrative access, encrypt all such access with strong cryptography using technologies such as SSH, VPN, or SSL/TLS, for web-based management and other non-console administrative access. ***Note:*** *Clear-text protocols such as Telnet or rlogin must never be used for administrative access.* ***Aligns with PCI DSS Requirement 2.3***					
12.1.a Install the payment application in a lab and test non-console administration connections to verify that a strong encryption method is invoked before the administrator's password is requested.	▪ **Identify** whether the payment application allows non-console administration. **(yes/no)**	*<Report Findings Here>*			
	▪ *If "no,"* **describe testing performed** to verify the payment application does not allow non-console administration.	*<Report Findings Here>*			
	▪ *If "yes,"* after installing the payment application in the lab, **describe the testing** of the non-console administrative connections performed to verify that a strong encryption method is invoked before the administrator's password is requested.	*<Report Findings Here>*			
12.1.b Examine payment application configuration settings to verify that clear-text protocols, such as Telnet and rlogin, are not used by the payment application for non-console administrative access.	▪ **Describe** payment application configuration settings examined.	*<Report Findings Here>*			
	▪ **Describe** payment application configuration settings examined to verify that clear-text protocols are not used by the payment application for non-console administrative access.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
12.1.c Examine the *PA-DSS Implementation Guide* prepared by vendor, and verify it includes instructions for customers and integrators/resellers how to configure the application to use strong cryptography, using technologies such as SSH, VPN, or SSL/TLS, for encryption of non-console administrative access.	▪ **Identify** the page number(s)/section of the *PA-DSS Implementation Guide* **verified** to include directions for customers and integrators/resellers that define how to configure the application to use strong cryptography for encryption of non-console administrative access.	*<Report Findings Here>*			
12.2 Instruct customers to encrypt all non-console administrative access with strong cryptography, using technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access. ***Note:*** *Clear-text protocols such as Telnet or rlogin must never be used for administrative access.* ***Aligns with PCI DSS Requirement 2.3***					
12.2 Examine the *PA-DSS Implementation Guide* prepared by vendor and verify it includes instructions for customers and integrators/resellers to implement strong cryptography, using technologies such as SSH, VPN, or SSL/TLS, for encryption of all non-console administrative access.	▪ **Identify** the page number(s)/section of the *PA-DSS Implementation Guide* **verified** to include instructions for customers and integrators/resellers to implement strong cryptography for encryption of all non-console administrative access.	*<Report Findings Here>*			

Requirement 13: Maintain a PA-DSS Implementation Guide for customers, resellers, and integrators

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
13.1 Develop, maintain, and disseminate a *PA-DSS Implementation Guide(s)* for customers, resellers, and integrators that accomplishes the following:					
13.1 Examine the *PA-DSS Implementation Guide* and related vendor processes, and interview personnel to verify: • The *PA-DSS Implementation Guide* is disseminated to all customers, resellers, and integrators with the application. • The vendor has a mechanism in place to provide the *PA-DSS Implementation Guide* to customers, resellers, and integrators upon request.	▪ **Identify** the related vendor process documents reviewed to verify processes define that: • The *PA-DSS Implementation Guide* is disseminated to all customers, resellers, and integrators with the application. • The vendor has a mechanism in place to provide the *PA-DSS Implementation Guide* to customers, resellers, and integrators upon request.	*<Report Findings Here>*			
	▪ **Identify** the mechanism in place to provide the *PA-DSS Implementation Guide* to customers, resellers, and integrators upon request.	*<Report Findings Here>*			
	▪ **Identify** the personnel interviewed for this testing procedure.	*<Report Findings Here>*			
	For the interview, **summarize the relevant details discussed** that verify that:				
	▪ The *PA-DSS Implementation Guide* is disseminated to all customers, resellers, and integrators with the application.	*<Report Findings Here>*			
	▪ The vendor has a mechanism in place to provide the *PA-DSS Implementation Guide* to customers, resellers, and integrators upon request.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
13.1.1 Provides relevant information specific to the application for customers, resellers, and integrators to use.					
13.1.1 Examine the PA-DSS Implementation Guide and verify it: • Clearly identifies the payment application name and version to which it applies. • Provides details of all application dependencies that are required in order for the application to be configured in a PCI DSS compliant manner.	**Identify** the page number(s)/section of the *PA-DSS Implementation Guide* **verified** to include the following:				
	▪ Clearly identifies the payment application name and version to which it applies.	*<Report Findings Here>*			
	▪ Provides details of all application dependencies that are required in order for the application to be configured in a PCI DSS compliant manner.	*<Report Findings Here>*			
13.1.2 Addresses all requirements in this document wherever the *PA-DSS Implementation Guide* is referenced.					
13.1.2 Examine the *PA-DSS Implementation Guide* and, using Appendix A as a reference, verify the *PA-DSS Implementation Guide* covers all related requirements in this document.	▪ Provide the name of the PA-QSA who attests that the PA-DSS Implementation Guide was verified to include all related requirements specifically indicated in Appendix A of the PA-DSS 3.0 document.	*<Report Findings Here>*			
13.1.3 Includes a review at least annually and upon changes to the application or to the PA-DSS requirements, and is updated as needed to keep the documentation current with all changes affecting the application, as well as with changes to the requirements in this document.					
13.1.3.a Examine the *PA-DSS* Implementation Guide and interview personnel to verify the *PA-DSS Implementation Guide* is reviewed: • At least annually, • Upon changes to the application • Upon changes to these PA-DSS requirements *(continued on next page)*	▪ **Describe how** the *PA-DSS Implementation Guide* was examined to verify it is reviewed:				
	• At least annually	*<Report Findings Here>*			
	• Upon changes to the application	*<Report Findings Here>*			
	• Upon changes to these PA-DSS requirements	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
	▪ **Identify** the personnel interviewed for this testing procedure who confirm the PA-DSS Implementation Guide is reviewed • At least annually, • Upon changes to the application • Upon changes to these PA-DSS requirements	*<Report Findings Here>*			
13.1.3.b Verify the *PA-DSS Implementation Guide* is updated as needed to keep current with: • Changes to the PA-DSS requirements. • Changes to the application or its dependencies.	**Describe the processes observed** to ensure that the *PA-DSS Implementation Guide* is updated as needed to keep current with:				
	▪ Changes to the PA-DSS requirements.	*<Report Findings Here>*			
	▪ Changes to the application or its dependencies.	*<Report Findings Here>*			
13.1.3.c Examine the *PA-DSS Implementation Guide* and related vendor processes, and interview personnel to verify the vendor has a mechanism in place to communicate updates to customers, resellers, and integrators, and provide updated versions as needed. *(continued on next page)*	▪ **Identify** the related vendor process documents reviewed to verify processes define that the vendor has a mechanism in place to: • Communicate updates to customers, resellers, and integrators. • Provide updated versions as needed.	*<Report Findings Here>*			
	▪ **Describe** the mechanism in place to communicate updates to customers, resellers, and integrators.	*<Report Findings Here>*			
	▪ **Describe** the mechanism in place to provide updated versions as needed.	*<Report Findings Here>*			
	▪ **Identify** the personnel interviewed for this testing procedure.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
	For the interview, **summarize the relevant details discussed** that verify that:				
	▪ The vendor has a mechanism in place to communicate updates to customers, resellers, and integrators.	*<Report Findings Here>*			
	▪ The vendor provides updated versions as needed.	*<Report Findings Here>*			

Requirement 14: Assign PA-DSS responsibilities for personnel and maintain training programs for personnel, customers, resellers, and integrators

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
14.1 Provide training in information security and PA-DSS for vendor personnel with PA-DSS responsibility at least annually.					
14.1 Examine training materials and interview responsible personnel to verify that all vendor personnel with PA-DSS responsibility receive training in PA-DSS and information security at least annually.	**Identify** the training materials examined to verify that all vendor personnel with PA-DSS responsibility:				
	▪ Receive training in PA-DSS at least annually.	*<Report Findings Here>*			
	▪ Receive training in information security at least annually.	*<Report Findings Here>*			
	▪ **Identify** the personnel interviewed for this testing procedure.	*<Report Findings Here>*			
	For the interview, **summarize the relevant details discussed** that verify that vendor personnel with PA-DSS responsibility:				
	▪ Receive training in PA-DSS at least annually.	*<Report Findings Here>*			
	▪ Receive training in information security at least annually.	*<Report Findings Here>*			
14.2 Assign roles and responsibilities to vendor personnel including the following: • Overall accountability for meeting all the requirements in PA-DSS • Keeping up-to-date within any changes in the *PA-DSS Program Guide* • Ensuring secure coding practices are followed • Ensuring integrators/resellers receive training and supporting materials • Ensuring all vendor personnel with PA-DSS responsibilities, including developers, receive training					

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
14.2.a Examine documented responsibilities to verify that responsibility for the following roles is formally assigned: • Overall accountability for meeting all the requirements in PA-DSS. • Keeping up-to-date within any changes in the *PA-DSS Program Guide.* • Ensuring secure coding practices are followed. • Ensuring integrators/resellers receive training and supporting materials. • Ensuring all vendor personnel with PA-DSS responsibilities, including developers, receive training.	▪ Identify the document(s) examined that verify responsibility for the following roles is formally assigned: • Overall accountability for meeting all the requirements in PA-DSS. • Keeping up-to-date within any changes in the *PA-DSS Program Guide.* • Ensuring secure coding practices are followed. • Ensuring integrators/resellers receive training and supporting materials. • Ensuring all vendor personnel with PA-DSS responsibilities, including developers, receive training.	*<Report Findings Here>*			
14.2.b Interview personnel assigned responsibility for the following roles to confirm that roles and responsibilities are defined and understood: • Overall accountability for meeting all the requirements in PA-DSS. • Keeping up-to-date within any changes in the *PA-DSS Program Guide.* • Ensuring secure coding practices are followed. • Ensuring integrators/resellers receive training and supporting materials. • Ensuring all vendor personnel with PA-DSS responsibilities, including developers, receive training.	**Identify** the interviewed personnel assigned responsibility for the following roles who confirmed that their roles and responsibilities are defined and understood:				
	▪ Overall accountability for meeting all the requirements in PA-DSS.	*<Report Findings Here>*			
	▪ Keeping up-to-date within any changes in the *PA-DSS Program Guide.*	*<Report Findings Here>*			
	▪ Ensuring secure coding practices are followed.	*<Report Findings Here>*			
	▪ Ensuring integrators/resellers receive training and supporting materials.	*<Report Findings Here>*			
	▪ Ensuring all vendor personnel with PA-DSS responsibilities, including developers, receive training.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
14.3 Develop and implement training and communication programs for payment application integrators and resellers. Training should include at least the following: • How to implement the payment application and related systems and networks in a PCI DSS-compliant manner • Coverage of all items noted for the *PA-DSS Implementation Guide* throughout this document (and in Appendix A)					
14.3.a Examine the training materials for integrators and resellers, and confirm the materials include the following: • Training on how to implement the payment application and related systems and networks in a PCI DSS-compliant manner. • Coverage of all items noted for the *PA-DSS Implementation Guide* throughout this document (and in Appendix A).	▪ **Identify** the training materials verified to include the following: • Training on how to implement the payment application in a PCI DSS-compliant manner. • Training on how to implement related systems and networks in a PCI DSS-compliant manner. • Coverage of all items noted for the *PA-DSS Implementation Guide* throughout this document (and in Appendix A).	*<Report Findings Here>*			
14.3.b Examine the vendor's communication programs and related vendor processes, and interview vendor personnel to verify: • Training materials are provided to integrators and resellers. • The vendor has a mechanism in place to provide updated materials to integrators and resellers upon request.	**Describe** the vendor's communication programs and related vendor processes examined to verify that:				
	▪ Training materials are provided to integrators and resellers.	*<Report Findings Here>*			
	▪ The vendor has a mechanism in place to provide updated materials to integrators and resellers upon request.	*<Report Findings Here>*			
	▪ **Identify** the vendor personnel interviewed who confirm that • Training materials are provided to integrators and resellers. • The vendor has a mechanism in place to provide updated materials to integrators and resellers upon request.	*<Report Findings Here>*			
14.3.c Interview a sample of integrators and resellers to verify that they received the training and training materials from the application vendor.	▪ **Identify** the sample of integrators and resellers interviewed who confirm that they received the training and training materials from the application vendor.	*<Report Findings Here>*			

PA-DSS Requirements and Testing Procedures	Reporting Instruction	ROV Reporting Details: Assessor's Response	Summary of Findings (check one)		
			In Place	Not Applicable	Not in Place
14.3.d Examine evidence of integrators and resellers receipt of the training materials from the software vendor.	▪ **Describe** evidence examined that verified receipt of the training materials from the software vendor.	*<Report Findings Here>*			
14.3.1 Review training materials at least annually and upon changes to the application or to PA-DSS requirements. Update the training materials as needed to keep the documentation current with new payment application versions and changes to PA-DSS requirements.					
14.3.1.a Examine the training materials for integrators and resellers and verify the materials are: • Reviewed at least annually and upon changes to the application or to PA-DSS requirements. • Updated as needed to keep the documentation current with new payment application versions and changes to PA-DSS requirements.	**Describe** the training materials for integrators and resellers observed to verify the materials are:				
	▪ Reviewed at least annually.	*<Report Findings Here>*			
	▪ Reviewed upon changes to the application.	*<Report Findings Here>*			
	▪ Reviewed upon changes to the PA-DSS requirements.	*<Report Findings Here>*			
	▪ Updated as needed to keep the documentation current with new payment application versions.	*<Report Findings Here>*			
	▪ Updated as needed to keep the documentation current with changes to PA-DSS requirements.	*<Report Findings Here>*			
14.3.1.b Examine the distribution process for new payment application versions and verify that updated documentation is distributed to integrators and resellers with the updated payment application.	▪ **Identify** the document that includes the distribution process to integrators and resellers for new payment application versions.	*<Report Findings Here>*			
	▪ **Describe** the distribution process observed that verified updated documentation is distributed with the updated payment application to integrators and resellers.	*<Report Findings Here>*			
14.3.1.c Interview a sample of integrators and resellers to verify they received updated training materials from the application vendor.	▪ **Identify** the sample of integrators and resellers interviewed who confirm they received updated training materials from the application vendor.	*<Report Findings Here>*			

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* provided to customers and integrators/resellers (see "PA-DSS Implementation Guide" on page 11), and to spell out responsibilities for implementing the related controls.

PA-DSS Requirement	PA-DSS Topic	Required Implementation Guide Content	Control Implementation Responsibility
1.1.4	Delete sensitive authentication data stored by previous payment application versions.	The following instructions must be provided for customers and integrators/resellers: ▪ Historical data must be removed (track data, card verification 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 sensitive authentication data stored by previous versions, per PA-DSS Requirement 1.1.4. **Customers & Integrators/Resellers**: 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.	The following instructions must be provided for customers and integrators/resellers: ▪ 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**: Do not store sensitive authentication data; and perform any troubleshooting of customer's problems according to PA-DSS Requirement 1.1.5.a. **Customers & Integrators/Resellers:** Do not store sensitive authentication data; and troubleshoot any problems per the *PA-DSS Implementation Guide* and PA-DSS Requirement 1.1.5.a.

PA-DSS Requirement	PA-DSS Topic	Required Implementation Guide Content	Control Implementation Responsibility
2.1	Securely delete cardholder data after customer-defined retention period.	The following must be provided for customers and integrators/resellers: ▪ Instructions that cardholder data exceeding the customer-defined retention period must be securely deleted. ▪ A list of all locations where payment application stores cardholder data, so that customer knows the locations of data that needs to be deleted. ▪ Instruction that customers need to securely delete cardholder data when no longer required for legal, regulatory, or business purposes. ▪ How to securely delete cardholder data stored by the payment application, including data stored on underlying software or systems (such as OS, databases, etc.). ▪ How to configure the underlying software or systems (such as OS, databases, etc.) to prevent inadvertent capture or retention of cardholder data.	**Software Vendor**: Provide guidance to customers that cardholder data exceeding customer-defined retention periods must be securely deleted where such data is stored by the payment application and underlying software or systems, and how to securely delete cardholder data stored by the payment application. **Customers & Integrators/Resellers**: Securely delete cardholder data exceeding customer-defined retention period, per the *PA-DSS Implementation Guide* and PA-DSS Requirement 2.1.
2.2	Mask PAN when displayed so only personnel with a business need can see the full PAN.	The following must be provided for customers and integrators/resellers: ▪ Details of all instances where PAN is displayed, including but not limited to POS devices, screens, logs, and receipts. ▪ Confirmation that the payment application masks PAN by default on all displays. ▪ Instructions on how to configure the payment application such that only personnel with a legitimate business need can see the full PAN.	**Software Vendor**: Provide instructions to customers for masking PAN so only personnel with a business need can see the full PAN. **Customers & Integrators/Resellers**: Mask displays of PAN so only personnel with a business need can see the full PAN, per the *PA-DSS Implementation Guide* and PA-DSS Requirement 2.2.

PA-DSS Requirement	PA-DSS Topic	Required Implementation Guide Content	Control Implementation Responsibility
2.3	Render PAN unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs).	The following must be provided for customers and integrators/resellers: ▪ Details of any configurable options for each method used by the application to render cardholder data unreadable, and instructions on how to configure each method for all locations where cardholder data is stored by the payment application (per PA-DSS Requirement 2.1). ▪ A list of all instances where cardholder data may be output for the merchant to store outside of the payment application, and instructions that the merchant is responsible for rendering PAN unreadable in all such instances.	**Software Vendor**: Provide instructions to customers for rendering PAN unreadable anywhere it is stored or output by the application. **Customers & Integrators/Resellers**: Render PAN unreadable anywhere it is stored per the *PA-DSS Implementation Guide* and PA-DSS Requirement 2.3.
2.4	Protect keys used to secure cardholder data against disclosure and misuse.	The following instructions must be provided for customers and integrators/resellers: ▪ Restrict access to keys to the fewest number of custodians necessary. ▪ Store keys securely in the fewest possible locations and forms.	**Software Vendor**: Provide guidance to customers that keys used to secure cardholder data should be stored securely in the fewest possible locations, and access to keys must be restricted to the fewest possible custodians. **Customers & Integrators/Resellers**: Store keys securely in the fewest possible locations, and restrict access to keys to the fewest possible custodians, per the *PA-DSS Implementation Guide* and PA-DSS Requirement 2.4.
2.5	Implement key-management processes and procedures for cryptographic keys used for encryption of cardholder data.	The following must be provided for customers and integrators/resellers: ▪ How to securely generate, distribute, protect, change, store, and retire/replace encryption keys, where customers or integrators/resellers are involved in these key-management activities. ▪ A sample Key Custodian Form for key custodians to acknowledge that they understand and accept their key-custodian responsibilities.	**Software Vendor**: Provide instructions to customers that access cryptographic keys used for encryption of cardholder data to implement key-management processes and procedures. **Customers & Integrators/Resellers**: Implement key-management processes and procedures for cryptographic keys used for encryption of cardholder data per *PA-DSS Implementation Guide* and PA-DSS Requirement 2.5.

PA-DSS Requirement	PA-DSS Topic	Required Implementation Guide Content	Control Implementation Responsibility
2.5.1–2.5.7	Implement secure key-management functions.	Provide instructions for customers and integrators/resellers on how to perform key-management functions including: ▪ Generation of strong cryptographic keys. ▪ Secure cryptographic key distribution. ▪ Secure cryptographic key storage. ▪ Cryptographic key changes for keys that have reached the end of their cryptoperiod. ▪ Retirement or replacement of keys as deemed necessary when the integrity of the key has been weakened or keys are suspected of being compromised. ▪ Split knowledge and dual control for any manual clear-text cryptographic key management operations supported by the payment application. ▪ Prevention of unauthorized substitution of cryptographic keys.	**Software Vendor**: Provide instructions to customers to implement key management secure key-management functions. **Customers & Integrators/Resellers**: Implement secure key management functions for cryptographic keys per *PA-DSS Implementation Guide* and PA-DSS Requirements 2.5.1–2.5.7.
2.6	Provide a mechanism to render irretrievable cryptographic key material or cryptograms stored by the payment application.	The following instructions must be provided for customers and integrators/resellers: ▪ Procedures detailing how to use the tool or procedure provided with the application to render cryptographic material irretrievable. ▪ That cryptographic key material should be rendered irretrievable whenever keys are no longer used and in accordance with key-management requirements in PCI DSS. ▪ Instructions on how to re-encrypt historic data with new keys, including procedures for maintaining security of clear-text data during the decryption /re-encryption process.	**Software Vendor**: Provide tool or procedure to securely remove cryptographic key material or cryptograms stored by the application, and provide tool or procedure to re-encrypt historic data with new keys. **Customers & Integrators/Resellers**: Delete any historical cryptographic material in accordance with key-management requirements per *PA-DSS Implementation Guide* and PA-DSS Requirement 2.6.

PA-DSS Requirement	PA-DSS Topic	Required Implementation Guide Content	Control Implementation Responsibility
3.1	Use unique user IDs and secure authentication for administrative access and access to cardholder data.	The following must be provided for customers and integrators/resellers: ▪ Directions on how the payment application enforces strong authentication for any authentication credentials (for example, users, passwords) that the application generates or manages, by: • Enforcing secure changes to authentication credentials by the completion of installation per PA-DSS requirements 3.1.1 through 3.1.11. • Enforcing secure changes to authentication credentials for any subsequent changes (after installation) per PA-DSS requirements 3.1.1 through 3.1.11. ▪ That, to maintain PCI DSS compliance, any changes made to authentication configurations would need to be verified as providing authentication methods that are at least as rigorous as PCI DSS requirements. ▪ Assign secure authentication to default accounts (even if not used), and disable or do not use the accounts. ▪ How to change and create authentication credentials when such credentials are not generated or managed by the payment application, per PA-DSS Requirements3.1.1 through 3.1.11, by the completion of installation and for subsequent changes after installation, for all application level accounts with administrative access or access to cardholder data.	**Software Vendor**: For all authentication credentials generated or managed by the application, ensure payment application enforces customer's use of unique user IDs and secure authentication for accounts/passwords, per PA-DSS Requirements 3.1.1 through 3.1.11. For authentication credentials not generated or managed by the payment application, ensure the *PA-DSS Implementation Guide* provides clear and unambiguous guidance for customers and integrators/resellers on how to change and create secure authentication credentials per PA-DSS Requirements 3.1.1 through 3.1.11. **Customers & Integrators/Resellers**: Establish and maintain unique user IDs and secure authentication per the *PA-DSS Implementation Guide* and PA-DSS Requirements 3.1.1 through 3.1.11.

PA-DSS Requirement	PA-DSS Topic	Required Implementation Guide Content	Control Implementation Responsibility
3.2	Use unique user IDs and secure authentication for access to PCs, servers, and databases with payment applications.	Instruct customers and integrators/resellers to use unique user names and secure authentication to access any PCs, servers, and databases with payment applications and/or cardholder data, PA-DSS requirements 3.1.1 through 3.1.11.	**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 PA-DSS requirements 3.1.2 through 3.1.9. **Customers & Integrators/Resellers**: Establish and maintain unique user IDs and secure authentication per the *PA-DSS Implementation Guide* and PA-DSS requirements 3.1.1 through 3.1.11.
4.1	Implement automated audit trails.	Provide instructions for implementing automated audit trails to include: ▪ How to install the application so that logs are configured and enabled by default upon completion of the installation process. ▪ How to set PCI DSS-compliant log settings, per PA-DSS Requirements 4.2, 4.3 and 4.4, for any logging options that are configurable by the customer after installation. ▪ Logs must be enabled, and disabling the logs will result in non-compliance with PCI DSS. ▪ How to configure PCI-compliant log settings for any third-party software components packaged with or required by the payment application, for any logging options that are configurable by the customer after installation.	**Software Vendor**: Ensure payment application supports customer's use of compliant logs per PA-DSS Requirements 4.2, 4.3 and 4.4. **Customers & Integrators/Resellers:** Establish and maintain PCI DSS-compliant logs per the *PA-DSS Implementation Guide* and PA-DSS Requirements 4.2, 4.3 and 4.4.
4.4	Facilitate centralized logging.	Provide a description of which centralized logging mechanisms are supported, as well as instructions and procedures for incorporating the payment application logs into a centralized logging server.	**Software Vendor**: Ensure payment application supports centralized logging in customer environments per PA-DSS Requirement 4.4. **Customers & Integrators/Resellers:** Establish and maintain centralized logging per the *PA-DSS Implementation Guide* and PA-DSS Requirement 4.4.

PA-DSS Requirement	PA-DSS Topic	Required Implementation Guide Content	Control Implementation Responsibility
5.5.4	Implement and communicate application versioning methodology.	Provide a description of the vendor's published versioning methodology, and include guidance for the following: ▪ Details of versioning scheme, including the format of the version scheme (number of elements, separators, character set, etc.). ▪ Details of how security-impacting changes will be indicated by the version scheme. ▪ Details of how other types of changes will affect the version. ▪ Details of any wildcard elements that are used, including that they will never be used to represent a security-impacting change.	**Software Vendor**: Document and implement a software-versioning methodology as part of the system development lifecycle. The methodology must follow the procedures in the *PA-DSS Program Guide* for changes to payment applications, per PA-DSS Requirement 5.5. **Customers & Integrators/Resellers:** Understand which version of the payment application they are using, and ensure validated versions are in use.

PA-DSS Requirement	PA-DSS Topic	Required Implementation Guide Content	Control Implementation Responsibility
6.1	Securely implement wireless technology.	For payment applications developed for use with wireless technology, the following instructions must be provided for customers and integrators/resellers: ▪ Instruction that the payment application enforces changes of default encryption keys, passwords and SNMP community strings at installation for all wireless components controlled by the application. ▪ Procedures for changing wireless encryption keys and passwords, including SNMP strings, anytime anyone with knowledge of the keys/passwords leaves the company or changes positions. ▪ Instructions for changing default encryption keys, passwords and SNMP community strings on any wireless components provided with, but not controlled by, the payment application. ▪ Instructions to install a firewall between any wireless networks and systems that store cardholder data. ▪ Details of any wireless traffic (including specific port information) that the wireless function of the payment application would use. ▪ Instructions to configure firewalls to deny or (if such traffic is necessary for business purposes) permit only authorized traffic between the wireless environment and the cardholder data environment.	**Software Vendor**: Instruct customers and integrators/resellers, that if wireless technology is used with the payment application, the wireless vendor default settings must be changed per PA-DSS Requirement 6.1. **Customers & Integrators/Resellers**: For wireless implemented into the payment environment by customers or integrators/resellers, change vendor defaults per PA-DSS Requirement 6.1 and install a firewall per the *PA-DSS Implementation Guide* and PCI DSS Requirement 2.1.1.

PA-DSS Requirement	PA-DSS Topic	Required Implementation Guide Content	Control Implementation Responsibility
6.2	Secure transmissions of cardholder data over wireless networks.	For payment applications developed for use with wireless technology, include instructions for using industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission of cardholder data. This includes: ▪ How to configure the application to use industry best practices (for example, IEEE 802.11.i) for strong encryption for authentication and transmission, and/or ▪ How to configure all wireless applications bundled with the payment application to use industry best practices for strong encryption for authentication and transmission.	**Software Vendor**: Instruct customers and integrators/resellers, that if wireless technology is used with the payment application, secure encrypted transmissions must be implemented, per PA-DSS Requirement 6.2. **Customers & Integrators/Resellers**: For wireless implemented into the payment environment by customers or integrators/resellers, use secure encrypted transmissions per the *PA-DSS Implementation Guide* and PA-DSS Requirement 6.2.
6.3	Provide instructions for secure use of wireless technology.	Provide instructions for PCI DSS-compliant wireless settings, including: ▪ Instructions to change all wireless default encryption keys, passwords and SNMP community strings upon installation. ▪ Instructions to change wireless encryption keys, passwords and SNMP strings anytime anyone with knowledge of the keys/passwords leaves the company or changes positions. ▪ Instructions to install a firewall between any wireless networks and systems that store cardholder data, and to configure firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment. ▪ Instructions to use industry best practices (for example, IEEE 802.11.i) to provide strong encryption for authentication and transmission.	**Software Vendor**: Instruct customers and integrators/resellers, to secure wireless technologies per PA-DSS Requirement 6.3. **Customers & Integrators/Resellers**: Secure wireless technologies per the *PA-DSS Implementation Guide* and PA-DSS Requirement 6.2.

PA-DSS Requirement	PA-DSS Topic	Required Implementation Guide Content	Control Implementation Responsibility
8.2	Use only necessary and secure services, protocols, components, and dependent software and hardware, including those provided by third parties.	Document all required protocols, services, components, and dependent software and hardware that are necessary for any functionality of the payment application.	**Software Vendor:** Ensure payment application supports customer's use of only necessary and secure protocols, services, etc., by 1) having only necessary protocols, services, etc., established "out of the box" by default, 2) having those necessary protocols, services, etc., securely configured by default, and 3) by documenting necessary protocols, services, etc., as a reference for customers and integrators/resellers. **Customers and Integrators/Resellers:** Use the documented list from the *PA-DSS Implementation Guide* to ensure only necessary and secure protocols, services, etc., are used on the system, in accordance with PA-DSS Requirement 5.4.
9.1	Store cardholder data only on servers not connected to the Internet.	The following instructions must be provided for customers and integrators/resellers: ▪ Instructions not to store cardholder data on public-facing systems (for example, web server and database server must not be on same server). ▪ Instructions on how to configure the payment application to use a DMZ to separate the Internet from systems storing cardholder data. ▪ A list of services/ports that the application needs to use in order to communicate across two network zones (so the merchant can configure their firewall to open only required ports).	**Software Vendor**: Ensure payment application does not require cardholder data storage in the DMZ or on Internet-accessible systems, and will allow use of a DMZ per PA-DSS Requirement 9. **Customers & Integrators/Resellers**: Establish and maintain payment applications so that cardholder data is not stored on Internet-accessible systems, per the *PA-DSS Implementation Guide* and PA-DSS Requirement 9
10.1	Implement two-factor authentication for all remote access to payment application that originates from outside the customer environment.	Provide the following for customers and integrators/resellers: ▪ Instruction that all remote access originating from outside the customer's network to the payment application must use two-factor authentication in order to meet PCI DSS requirements. ▪ Describe the two-factor authentication mechanisms supported by the application. ▪ Instructions on how to configure the application to support two-factor authentication (two of the three authentication methods described in PA DSS Req. 3.1.4).	**Software Vendor**: Ensure payment application supports customers' use of two-factor authentication for all remote access to the payment application that originates from outside the customer environment, per PA-DSS Requirement 10.2. **Customers & Integrators/resellers**: Establish and maintain two-factor authentication for all remote access to payment application that originates from outside the customer environment, per the *PA-DSS Implementation Guide* and PA-DSS Requirement 10.2.

PA-DSS Requirement	PA-DSS Topic	Required Implementation Guide Content	Control Implementation Responsibility
10.2.1	Securely deliver remote payment application updates.	If payment application updates are delivered via remote access into customers' systems, provide the following: ▪ Instructions for activation of remote-access technologies for payment application updates only when needed for downloads, and turning access off immediately after download completes, per PCI DSS Requirement 12.3.9. ▪ Instructions that, if computer is connected via VPN or other high-speed connection, receive remote payment application updates via a securely configured firewall or personal firewall per PCI DSS Requirement 1.	**Software Vendor**: Deliver remote payment application updates securely per PA-DSS 10.3 **Customers & Integrators/Resellers**: Receive remote payment application updates from vendor securely, per the *PA-DSS Implementation Guide,* PA-DSS Requirement 10.3 and PCI DSS Requirement 1.
10.2.3	Securely implement remote-access software.	Include instructions that all remote access to the payment application must be implemented securely, for example: ▪ 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 (See PA-DSS Requirements 3.1.1 through 3.1.11). ▪ Enable encrypted data transmission according to PA-DSS Requirement 12.1. ▪ Enable account lockout after a certain number of failed login attempts. (See PA-DSS Requirement 3.1.8.) ▪ Establish a Virtual Private Network ("VPN") connection via a firewall before access is allowed. ▪ Enable the logging function. ▪ Restrict access to customer environments to authorized integrator/reseller personnel.	**Software Vendor**: (1) If vendor can access customers' payment applications remotely, implemented secure remote access such as those specified in PA-DSS Requirement 10.3.2. (2) Ensure payment application supports customers' use of remote access security features. **Customers & Integrators/resellers**: Use remote access security features for all remote access to payment applications, per the *PA-DSS Implementation Guide* and PA-DSS Requirement 10.3.2.

PA-DSS Requirement	PA-DSS Topic	Required Implementation Guide Content	Control Implementation Responsibility
11.1	Secure transmissions of cardholder data over public networks.	If the payment application sends, or facilitates sending, cardholder data over public networks, include instructions for implementing and using strong cryptography and security protocols for secure cardholder data transmission over public networks, including: ▪ Required use of strong cryptography and security protocols if cardholder data is ever transmitted over public networks. ▪ Instructions for verifying that only trusted keys and/or certificates are accepted. ▪ How to configure the payment application to use only secure versions and secure implementations of security protocols. ▪ How to configure the payment application to use the proper encryption strength for the encryption methodology in use.	**Software Vendor**: Ensure payment application supports customer's use of strong cryptography and security protocols for transmissions of cardholder data over public networks, per PA-DSS Requirement 11.1. **Customers & Integrators/Resellers**: Establish and maintain strong cryptography and security protocols for transmissions of cardholder data, per the *PA-DSS Implementation Guide* and PA-DSS Requirement 11.1.
11.2	Encrypt cardholder data sent over end-user messaging technologies.	If the payment application facilitates sending of PANs by end-user messaging technologies, include instructions for implementing and using a solution that renders the PAN unreadable or implements strong cryptography, including: ▪ Procedures for using the defined solution to render the PAN unreadable or secure the PAN with strong cryptography. ▪ Instruction that PAN must always be rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies.	**Software Vendor**: Provide or specify use of a solution that renders the PAN unreadable or implements strong cryptography, and ensure payment application supports the encryption or rendering unreadable of PANs if sent with end-user messaging technologies, per PA-DSS Requirement 11.2. **Customers & Integrators/Resellers**: Render unreadable or encrypt with strong cryptography all PANs sent with end-user messaging technologies, per the *PA-DSS Implementation Guide* and PA-DSS Requirement 11.2.
12.1	Encrypt non-console administrative access.	If the payment application facilitates non-console administrative access, include instructions on how to configure the application to use strong cryptography (such as SSH, VPN, or SSL/TLS) for encryption of all non-console administrative access to payment application or servers in cardholder data environment.	**Software Vendor**: If the payment application facilitates non-console administrative access, ensure payment application implements strong encryption for non-console administrative access, per PA-DSS Requirement 12.1. **Customers & Integrators/Resellers**: Encrypt all non-console administrative access, per the *PA-DSS Implementation Guide* and PA-DSS Requirement 12.1.

PA-DSS Requirement	PA-DSS Topic	Required Implementation Guide Content	Control Implementation Responsibility
12.2	Encrypt non-console administrative access.	Include instructions for customers and integrators/resellers to implement strong cryptography, using technologies such as SSH, VPN, or SSL/TLS, for encryption of all non-console administrative access.	**Software Vendor**: Ensure payment application supports customer's encryption of non-console administrative access, per PA-DSS Requirement 12.2. **Customers & Integrators/Resellers**: Encrypt all non-console administrative access, per the *PA-DSS Implementation Guide* and PA-DSS Requirement 12.2

Appendix B: Testing Laboratory Configuration for PA-DSS Assessments

For each PA-DSS assessment conducted, the PA-QSA must confirm the status and capabilities of the laboratory used to conduct the testing for the PA-DSS assessment. This confirmation must be submitted along with the completed *Report of Validation (ROV)*.

For each Laboratory Validation Procedure, the PA-QSA must indicate whether the laboratory used for the assessment and the laboratory undergoing these validation procedures was the PA-QSA's laboratory or software vendor's laboratory. PA-QSAs are required to maintain a testing laboratory which meets all of the requirements set out below and use their own laboratory to conduct assessments whenever possible. The software vendor's laboratory may only be used when necessary (for example, when the PA-QSA does not have the mainframe, AS400, or Tandem the payment application runs on) and after verifying that all laboratory requirements are met.

The PA-DSS ROV Reporting Template below provides details of the laboratory validation that must be provided for each assessment.

B.1 Testing Laboratory Used for PA-DSS Assessments

▪ Location of the lab(s) used for the PA-DSS review	
▪ Owner of the lab(s) used for the PA-DSS review	
▪ Rationale for use of vendor lab, if applicable *If the vendor lab was used, complete the following:*	
• **Describe how** the PA-QSA validated the clean installation of the remote lab environment to ensure the environment truly simulates a real-world situation.	
• **Describe how** the PA-QSA validated the clean installation of the remote lab environment to ensure the vendor has not modified or tampered with the environment in any way.	

B.2 Details for Testing Laboratory Configurations for PA-DSS Assessments

▪ Description of laboratory testing architecture and environment in place for the PA-DSS review	
▪ Description of how the real-world use of the payment application was simulated in the laboratory for the PA-DSS review	

B.3 Attestation of Laboratory Validation

▪ Provide the name of the PA-QSA who attests that all items in the table below at B.4 for the PA-DSS Laboratory Requirements were validated to be in place in the PA-QSA's lab and/or vendor's lab and all details are consistent with details in the remainder of the Report on Validation. *For the remainder of the table, indicate via a checkmark whether each below was completed in the PA-QSA's lab or the vendor's lab.*	
• If any of the below were not in place or if there are any other comments or details related to the laboratory the PA-QSA would like to note, please indicate that here.	

B.4 PA-DSS Laboratory Validation

PA-DSS Laboratory Requirement	PA-DSS Laboratory Validation Procedure	Completed in: (Check which lab)	
		PA-QSA	Vendor
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 to simulate real-world customer experience.		
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, including all necessary system components and dependencies.		
	2.c Verify that all critical payment application functionalities were tested for each version.		
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.		

PA-DSS Laboratory Requirement	PA-DSS Laboratory Validation Procedure	Completed in: (Check which lab)	
		PA-QSA	Vendor
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.b** The laboratory uses only test card numbers for the simulation/testing—live PANs are not used for testing.* ***Note:** Test cards can usually be obtained from the vendor or a processor or acquirer.*		
	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.		
6. Provide capabilities for and test using the following penetration-testing methodologies:	**6.a Use of forensic tools/methods:** 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.[2]		
	6.b Attempt to exploit application vulnerabilities: Current vulnerabilities (for example, the OWASP Top 10, SANS CWE Top 25, CERT Secure Coding, etc.), were used to attempt to exploit the payment application(s), per PA-DSS Requirement 5.2.		
	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 7.2.2.		

[2] 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 Laboratory Requirement	PA-DSS Laboratory Validation Procedure	Completed in: (Check which lab)	
		PA-QSA	Vendor
7. Use vendor's lab ONLY after verifying all requirements are met. ***Note:*** *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.a** 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.b The PA-QSA validates the clean installation of the remote lab environment to ensure the environment truly simulates a real-world situation and that the vendor has not modified or tampered with the environment in any way.		
	7.c All testing is executed by the PA-QSA (the vendor cannot run tests against their own application).		
	7.d All testing is either (1) performed while onsite 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 verify that all versions and 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.		