



Payment Card Industry (PCI) **Payment Application Data Security Standard**

Attestation of Validation

Version 2.0

October 2010

Attestation of Validation

Instructions for Submission

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

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

Part 1. Payment Application Vendor and Qualified Security Assessor Information

Part 1a. Payment Application Vendor Information

Company Name:		DBA(s):	
Contact Name:		Title:	
Telephone:		E-mail:	
Business Address:		City:	
State/Province:		Country:	
URL:		Zip:	

Part 1b. Payment Application Qualified Security Assessor (PA-QSA) Company Information

Company Name:	
Lead QSA Contact Name:	
Telephone:	
Business Address:	
State/Province:	
URL:	

Part 2. Payment Application Information

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

Payment Application Functionality (check all that apply):

<input type="checkbox"/> POS Suite	<input type="checkbox"/> POS Admin	<input type="checkbox"/> Shopping Cart & Store Front
<input type="checkbox"/> POS Face-to-Face	<input type="checkbox"/> Payment Middleware	<input type="checkbox"/> Others (please specify):
<input type="checkbox"/> POS Kiosk	<input type="checkbox"/> Payment Back Office	
<input type="checkbox"/> POS Specialized	<input type="checkbox"/> Payment Gateway/Switch	

Target Market for Application:

Part 3. PCI PA-DSS Validation

Based on the results noted in the PA-DSS ROV dated *(date of ROV)*, *(QSA Name)* asserts the following validation status for the application(s) and version(s) identified in Part 2 of this document as of *(date)* *(Complete either Part 3a or Part 3b)*:

Part 3a. Confirmation of Validated Status: (each item to be confirmed)

- Fully Validated:** All requirements in the ROV are marked “in place,” thereby *(Payment Application Name(s) and Version(s))* has achieved full validation with the Payment Application Data Security Standard.
- The ROV was completed according to the PA-DSS, version *(insert version number)*, in adherence with the instructions therein.
- All information within the above-referenced ROV and in this attestation represents the results of the assessment fairly in all material respects.
- No evidence of magnetic stripe (i.e., track) data¹, CAV2, CVC2, CID, or CVV2 data², or PIN data³ storage after transaction authorization on ANY files or functionalities generated by the application during this PA-DSS assessment.

Part 3b. Annual Re-Validation Confirmation:

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

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

Part 3c. PA-QSA and Application Vendor Acknowledgments

<i>Signature of Application Vendor Executive Officer</i> ↑		<i>Date</i> ↑	
<i>Application Vendor Executive Officer Name</i> ↑		<i>Title</i> ↑	
<i>Application Vendor Company Represented</i> ↑			
<i>Signature of Lead PA-QSA</i> ↑		<i>Date</i> ↑	
<i>Lead PA-QSA Name</i> ↑		<i>Title</i> ↑	

¹ Magnetic Stripe Data (Track Data) – Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full magnetic stripe data after authorization. The only elements of track data that may be retained are account number, expiration date, and name.

² The three- or four-digit value printed on the signature panel or face of a payment card used to verify card-not-present transactions.

³ PIN Data – Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.