Attestation of Compliance – Merchants

Payment Card Industry (PCI)

Data Security Standard

Attestation of Compliance for Onsite Assessments – Merchants

Version 2.0

October 2010

PCI Security Standards Council

Instructions for Submission

This document must be completed by a Qualified Security Assessor (QSA) or merchant (if merchant internal audit performs validation) as a declaration of the merchant's compliance status with the Payment Card Industry Data Security Standard (PCI DSS). Complete all applicable sections and submit to the acquirer or requesting payment brand.

Part 1. Merchant and Qualified Security Assessor Information

Merchant Organization Information

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

Qualified Security Assessor Company Information

Company Name:					
Lead QSA Contact Name:			Title:		
Telephone:			E-mail:		
Business Address:			City:		
State/Province:		Country:		Zip:	
URL:					

Part 2 Type of Merchant Business (check all that apply)

☐ Retailer ☐ Telecommunication ☐ Grocery and Supermarkets

☐ Petroleum ☐ E-Commerce ☐ Mail/Telephone-Order

☐ Travel & Entertainment ☐ Others (please specify):

List facilities and locations included in PCI DSS review:

Part 2b. Relationships

Does your company have a relationship with one or more third-party agents (for example, gateways, web-hosting companies, airline booking agents, loyalty program agents, etc.)? ☐ Yes ☐ No

Does your company have a relationship with more than one acquirer? ☐ Yes ☐ No

Part 2c. Transaction Processing

How and in what capacity does your business store, process and/or transmit cardholder data?

Payment Application in Use	Version Number	Last Validated according to PABP/PA-DSS

Part 3. PCI DSS Validation

Based on the results noted in the Report on Compliance ("ROC") dated *(date of ROC)*, *(QSA Name/Merchant Name)* asserts the following compliance status for the entity identified in Part 2 of this document as of *(date)* (check one):

☐ **Compliant:** All requirements in the ROC are marked "in place[1]," and a passing scan has been completed by the PCI SSC Approved Scanning Vendor *(ASV Name)* thereby *(Merchant Company Name)* has demonstrated full compliance with the PCI DSS *(insert version number).*

☐ **Non-Compliant:** Some requirements in the ROC are marked "not in place," resulting in an overall **NON-COMPLIANT** rating, **or** a passing scan has not been completed by a PCI SSC Approved Scanning Vendor, thereby *(Merchant Company Name)* has not demonstrated full compliance with the PCI DSS.

Target Date for Compliance:

An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with your acquirer or the payment brand(s) before completing Part 4, since not all payment brands require this section.*

Part 3a. Confirmation of Compliant Status

QSA/Merchant confirms:

☐	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *(insert version number)*, and was completed according to the instructions therein.
☐	All information within the above-referenced ROC and in this attestation fairly represents the results of the assessment in all material respects.
☐	The merchant has confirmed with the payment application vendor that their payment application does not store sensitive authentication data after authorization.
☐	The merchant has read the PCI DSS and recognizes that they must maintain full PCI DSS compliance at all times.
☐	No evidence of magnetic stripe (that is, track) data[2], CAV2, CVC2, CID, or CVV2 data[3], or PIN data[4] storage after transaction authorization was found on ANY systems reviewed during this assessment.

Part 3b. QSA and Merchant Acknowledgments

Signature of Merchant Executive Officer ↑	***Date:***
Merchant Executive Officer Name:	***Title:***

Signature of Lead QSA ↑	***Date:***
Lead QSA Name :	***Title:***

[1] "In place" results should include compensating controls reviewed by the QSA/merchant Internal Audit. If compensating controls are determined to sufficiently mitigate the risk associated with the requirement, the QSA should mark the requirement as "in place."

[2] 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 transaction authorization. The only elements of track data that may be retained are account number, expiration date, and name.

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

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

Part 4. Action Plan for Non-Compliant Status

Please select the appropriate "Compliance Status" for each requirement. If you answer "No" to any of the requirements, you are required to provide the date Company will be compliant with the requirement and a brief description of the actions being taken to meet the requirement. *Check with your acquirer or the payment brand(s) before completing Part 4 since not all payment brands require this section.*

PCI Requirement	Description	Compliance Status (Select One)	Remediation Date and Actions (if Compliance Status is "No")
1	Install and maintain a firewall configuration to protect cardholder data.	☐ Yes ☐ No	
2	Do not use vendor-supplied defaults for system passwords and other security parameters.	☐ Yes ☐ No	
3	Protect stored cardholder data.	☐ Yes ☐ No	
4	Encrypt transmission of cardholder data across open, public networks.	☐ Yes ☐ No	
5	Use and regularly update anti-virus software.	☐ Yes ☐ No	
6	Develop and maintain secure systems and applications.	☐ Yes ☐ No	
7	Restrict access to cardholder data by business need to know.	☐ Yes ☐ No	
8	Assign a unique ID to each person with computer access.	☐ Yes ☐ No	
9	Restrict physical access to cardholder data.	☐ Yes ☐ No	
10	Track and monitor all access to network resources and cardholder data.	☐ Yes ☐ No	
11	Regularly test security systems and processes.	☐ Yes ☐ No	
12	Maintain a policy that addresses information security.	☐ Yes ☐ No