



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

---

## **Attestation of Compliance for Self-Assessment Questionnaire C**

Version 1.2

October 2008



## Attestation of Compliance, SAQ C

### Instructions for Submission

The merchant must complete this Attestation of Compliance as a declaration of the merchant's compliance status with the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Security Assessment Procedures*. Complete all applicable sections and refer to the submission instructions at "PCI DSS Compliance – Completion Steps" in this document.

### Part 1. Qualified Security Assessor Company Information (if applicable)

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

### Part 2. Merchant Organization Information

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

### Part 2a. Type of merchant business (check all that apply):

- Retailer     Telecommunication     Grocery and Supermarkets  
 Petroleum     E-Commerce     Mail/Telephone-Order     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 service providers (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

Payment Application in use:	Payment Application Version:
-----------------------------	------------------------------

## Part 2d. Eligibility to Complete SAQ C

Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because:

<input checked="" type="checkbox"/>	Merchant has a payment application system and an Internet or public network connection on the same device;
<input type="checkbox"/>	The payment application system/Internet device is not connected to any other system within the merchant environment;
<input checked="" type="checkbox"/>	Merchant does not store cardholder data in electronic format;
<input type="checkbox"/>	If Merchant does store cardholder data, such data is only in paper reports or copies of paper receipts and is not received electronically; <b>and</b>
<input checked="" type="checkbox"/>	Merchant's payment application software vendor uses secure techniques to provide remote support to merchant's payment application system.

## Part 3. PCI DSS Validation

Based on the results noted in the SAQ C dated (*completion date*), (*Merchant Company Name*) asserts the following compliance status (check one):

- Compliant:** All sections of the PCI SAQ are complete, and all questions answered "yes," resulting in an overall **COMPLIANT** rating, **and** a passing scan has been completed by a PCI SSC Approved Scan Vendor, thereby (*Merchant Company Name*) has demonstrated full compliance with the PCI DSS.
- Non-Compliant:** Not all sections of the PCI SAQ are complete, or some questions are answered "no," resulting in an overall **NON-COMPLIANT** rating, **or** a passing scan has not been completed by a PCI SSC Approved Scan 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

Merchant confirms:

<input type="checkbox"/>	PCI DSS Self-Assessment Questionnaire C, Version ( <i>version of SAQ</i> ), was completed according to the instructions therein.
<input type="checkbox"/>	All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
<input checked="" type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain full PCI DSS compliance at all times.
<input checked="" type="checkbox"/>	No evidence of magnetic stripe (i.e., track) data <sup>1</sup> , CAV2, CVC2, CID, or CVV2 data <sup>2</sup> , or PIN data <sup>3</sup> storage after transaction authorization was found on ANY systems reviewed during this assessment.

<sup>1</sup> Data encoded in the magnetic stripe 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.

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

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

### Part 3b. Merchant Acknowledgement

<i>Signature of Merchant Executive Officer</i> ↑		<i>Date</i> ↑
<i>Merchant Executive Officer Name</i> ↑		<i>Title</i> ↑
<i>Merchant Company Represented</i> ↑		

### 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 DSS Requirement	Description of Requirement	Compliance Status (Select One)		Remediation Date and Actions (if Compliance Status is “NO”)
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	
5	Use and regularly update anti-virus software	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Assign a unique ID to each person with computer access	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security	<input type="checkbox"/>	<input type="checkbox"/>	

