



**Payment Card Industry (PCI)  
Data Security Standard  
Self-Assessment Questionnaire A  
and Attestation of Compliance**

---

**No Electronic Storage, Processing, or  
Transmission of Cardholder Data**

**Version 1.1**

February 2008

## Table of Contents

---

<b>PCI Data Security Standard: Related Documents .....</b>	<b>ii</b>
<b>Before you Begin.....</b>	<b>iii</b>
<b>Completing the Self-Assessment Questionnaire .....</b>	<b>iii</b>
<b>PCI DSS Compliance – Completion Steps .....</b>	<b>iii</b>
<b>Attestation of Compliance, SAQ A.....</b>	<b>1</b>
<b>Self-Assessment Questionnaire A.....</b>	<b>4</b>
<b>Implement Strong Access Control Measures .....</b>	<b>4</b>
<i>Requirement 9: Restrict physical access to cardholder data .....</i>	<i>4</i>
<b>Maintain an Information Security Policy .....</b>	<b>4</b>
<i>Requirement 12: Maintain a policy that addresses information security for employees and contractors.....</i>	<i>4</i>

## PCI Data Security Standard: Related Documents

The following documents were created to assist merchants and service providers in understanding the PCI Data Security Standard and the PCI DSS SAQ.

Document	Audience
<i>PCI Data Security Standard</i>	All merchants and service providers
<i>Navigating PCI DSS: Understanding the Intent of the Requirements</i>	All merchants and service providers
<i>PCI Data Security Standard: Self-Assessment Guidelines and Instructions</i>	All merchants and service providers
<i>PCI Data Security Standard: Self-Assessment Questionnaire A and Attestation</i>	Merchants <sup>1</sup>
<i>PCI Data Security Standard: Self-Assessment Questionnaire B and Attestation</i>	Merchants <sup>1</sup>
<i>PCI Data Security Standard: Self-Assessment Questionnaire C and Attestation</i>	Merchants <sup>1</sup>
<i>PCI Data Security Standard: Self-Assessment Questionnaire D and Attestation</i>	Service providers and all other merchants <sup>1</sup>
<i>PCI DSS Glossary, Abbreviations, and Acronyms</i>	All merchants and service providers

<sup>1</sup> To determine the appropriate Self-Assessment Questionnaire, see *PCI Data Security Standard: Self-Assessment Guidelines and Instructions*, “Selecting the SAQ and Attestation That Best Apply to Your Organization.”

## Before you Begin

---

### Completing the Self-Assessment Questionnaire

SAQ A has been developed to address requirements applicable to merchants who retain only paper reports or receipts with cardholder data, do not store cardholder data in electronic format and do not process or transmit any cardholder data on their premises.

These merchants, defined as SAQ Validation Type 1 here and in the *PCI DSS Self-Assessment Questionnaire Instructions and Guidelines*, do not store cardholder data in electronic format and do not process or transmit any cardholder data on their premises. Such merchants must validate compliance by completing SAQ A and the associated Attestation of Compliance, confirming that:

- Your company handles only card-not-present (e-commerce or mail/telephone-order) transactions;
- Your company does not store, process, or transmit any cardholder data on your premises, but relies entirely on third party service provider(s) to handle these functions;
- Your company has confirmed that the third party service provider(s) handling storage, processing, and/or transmission of cardholder data is PCI DSS compliant;
- Your company retains only paper reports or receipts with cardholder data, and these documents are not received electronically; **and**
- Your company does not store any cardholder data in electronic format.

**This option would never apply to merchants with a face-to-face POS environment.**

### PCI DSS Compliance – Completion Steps

1. Complete the Self-Assessment Questionnaire (SAQ A) according to the instructions in the *Self-Assessment Questionnaire Instructions and Guidelines*.
2. Complete the Attestation of Compliance in its entirety.
3. Submit the SAQ and the Attestation of Compliance, along with any other requested documentation, to your acquirer.

## Attestation of Compliance, SAQ A

### 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). 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:					
State/Province:		Country:		ZIP:	
URL:					

#### Part 2. Merchant Organization Information

Company Name:		DBA(S):			
Contact Name:		Title:			
Telephone:		E-mail:			
Business Address:					
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 (e.g. 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. Eligibility to Complete SAQ A

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

- |                          |  |
|--------------------------|--|
| <input type="checkbox"/> | Merchant does not store, process, or transmit any cardholder data on merchant premises but relies entirely on third party service provider(s) to handle these functions; |
| <input type="checkbox"/> | The third party service provider(s) handling storage, processing, and/or transmission of cardholder data is confirmed to be PCI DSS compliant;                           |
| <input type="checkbox"/> | Merchant retains only paper reports or receipts with cardholder data, and such documents are not received electronically; <b>and</b>                                     |
| <input type="checkbox"/> | Merchant does not store any cardholder data in electronic format.  |

### Part 3. PCI DSS Validation

Based on the results noted in the SAQ A 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, 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, 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 A, 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.          |
| <input type="checkbox"/> | I have read the PCI DSS and I recognize that I must maintain full PCI DSS compliance at all times.                               |

### Part 3b. Merchant Acknowledgement

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

*Merchant Company Represented* ↑

#### 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	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security	<input type="checkbox"/>	<input type="checkbox"/>	

## Self-Assessment Questionnaire A

Date of Completion:

### Implement Strong Access Control Measures

#### Requirement 9: Restrict physical access to cardholder data

9.6	Are all paper and electronic media that contain cardholder data physically secure? <i>(Such media includes computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes.)</i>	<input type="checkbox"/>	<input type="checkbox"/>
9.7	(a) Is strict control maintained over the internal or external distribution of any kind of media that contains cardholder data?	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Do controls include the following:		
9.7.1	Is the media classified so it can be identified as confidential?	<input type="checkbox"/>	<input type="checkbox"/>
9.7.2	Is the media sent by secured courier or other delivery method that can be accurately tracked?	<input type="checkbox"/>	<input type="checkbox"/>
9.8	Are processes and procedures in place to ensure management approval is obtained prior to moving any and all media from a secured area (especially when media is distributed to individuals)?	<input type="checkbox"/>	<input type="checkbox"/>
9.9	Is strict control maintained over the storage and accessibility of media that contains cardholder data?	<input type="checkbox"/>	<input type="checkbox"/>
9.10	Is media containing cardholder data destroyed when it is no longer needed for business or legal reasons? Destruction should be as follows:	<input type="checkbox"/>	<input type="checkbox"/>
9.10.1	Are hardcopy materials cross-cut shredded, incinerated, or pulped?	<input type="checkbox"/>	<input type="checkbox"/>

### Maintain an Information Security Policy

#### Requirement 12: Maintain a policy that addresses information security for employees and contractors

Question	Response:	Yes	No
12.8	Contractually, are the following required if cardholder data is shared with service providers?	<input type="checkbox"/>	<input type="checkbox"/>
12.8.1	That service providers must adhere to the PCI DSS requirements?	<input type="checkbox"/>	<input type="checkbox"/>
12.8.2	An agreement that includes an acknowledgement that the service provider is responsible for the security of cardholder data the provider possesses?	<input type="checkbox"/>	<input type="checkbox"/>