

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) 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. 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 does not store any cardholder data in electronic format; and
<input type="checkbox"/>	If Merchant does store cardholder data, such data is only in paper reports or copies of receipts and is not received electronically.

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> ↑
<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	
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

Question		Response:	<u>Yes</u>	<u>No</u>	<u>Special*</u>
9.6	Are all paper and electronic media that contain cardholder data physically secure?		<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 containing cardholder data 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 so that cardholder data cannot be reconstructed?		<input type="checkbox"/>	<input type="checkbox"/>	

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

Maintain an Information Security Policy

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

Question		Response:	<u>Yes</u>	<u>No</u>	<u>Special*</u>
12.8	If cardholder data is shared with service providers, are policies and procedures maintained and implemented to manage service providers, and do the policies and procedures include the following?		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.1	A list of service providers is maintained.		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.2	A written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.3	There is an established process for engaging service providers, including proper due diligence prior to engagement.		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.4	A program is maintained to monitor service providers' PCI DSS compliance status.		<input type="checkbox"/>	<input type="checkbox"/>	

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.