



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

---

Card-not -present Merchants,  
All Cardholder Data Functions Fully Outsourced

For use with PCI DSS Version 3.2

Revision 1.1

January 2017

## Document Changes

Date	PCI DSS Version	SAQ Revision	Description
October 2008	1.2		To align content with new PCI DSS v1.2 and to implement minor changes noted since original v1.1.
October 2010	2.0		To align content with new PCI DSS v2.0 requirements and testing procedures.
February 2014	3.0		To align content with PCI DSS v3.0 requirements and testing procedures and incorporate additional response options.
April 2015	3.1		Updated to align with PCI DSS v3.1. For details of PCI DSS changes, see <i>PCI DSS – Summary of Changes from PCI DSS Version 3.0 to 3.1</i> .
July 2015	3.1	1.1	Updated version numbering to align with other SAQs.
April 2016	3.2	1.0	Updated to align with PCI DSS v3.2. For details of PCI DSS changes, see <i>PCI DSS – Summary of Changes from PCI DSS Version 3.1 to 3.2</i> . Requirements added from PCI DSS v3.2 Requirements 2, 8, and 12.
January 2017	3.2	1.1	Updated Document Changes to clarify requirements added in the April 2016 update. Added note to Before You Begin section to clarify intent of inclusion of PCI DSS Requirements 2 and 8.









## Section 1: Assessment Information

---

### ***Instructions for Submission***

This document must be completed as a declaration of the results of the self-assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: ~~The merchant~~ merchant is responsible for ensuring that each section is completed by ~~the~~ all sections







## Section 2: Self-Assessment Questionnaire A

---

**Note:**

## Implement Strong Access Control Measures

### Requirement 8: Identify and authenticate access to system components

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
8.1.1	Are all users assigned a unique ID before allowing them to access system components or cardholder data?	Review password procedures Interview personnel	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.1.3	Is access for any terminated users immediately deactivated or removed?	Review password procedures Examine terminated users accounts Review current access lists Observe returned physical authenticat9 183.86 71.88 5g8004 0.48 i				



**PCI DSS Question**

**Expected Testing**

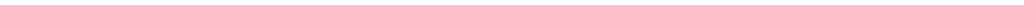
## Maintain an Information Security Policy

### Requirement 12: Maintain a policy that addresses information security for all personnel

**Note:** For the purposes of Requirement 12, “personnel” refers to full-time part-time employees, temporary employees and personnel, and contractors and consultants who are “resident” on the entity’s site or otherwise have access to the company’s site cardholder data environment.

PCI DSS Question	Expected Testing	Response (Check one response for each question)			
		Yes	Yes with CCW	No	N/A
12.8	Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:				
12.8.1	Is a list of service providers maintained, including a description of the service(s) provided?  Review policies and procedures Observe processes Review list of service providers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.2	Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent cardholder data environment?  <b>Note:</b> The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibility assigned to each party.				









## Appendix C: Explanation of Non-Applicability

If the "N/A" (Not Applicable) column was checked in the questionnaire, use this worksheet to explain why the related requirement is not applicable to your organization.

Requirement	Reason Requirement is Not Applicable
<i>Example:</i>	
3.4	Cardholder data is never stored electronically

96 re



**Part 3a. Acknowledgement of Status** (continued)

- |                          |  |
|--------------------------|--|
| <input type="checkbox"/> | No evidence of full 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 system reviewed during this assessment. |
| <input type="checkbox"/> | ASV scans are being completed by the PCI SSC Approved Scanning Vendor ( <i>ASV Name</i> )  |

