

Attestation of Compliance, SAQ B

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 B

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

<input type="checkbox"/>	A. or	Merchant uses only an imprint machine to imprint customers' payment card information and does not transmit cardholder data over either a phone line or the Internet;
	B.	Merchant uses only standalone, dial-up terminals; and the standalone, dial-up terminals are not connected to the Internet or any other systems within the merchant environment;
<input type="checkbox"/>	Merchant does not store cardholder data in electronic format; and	
<input type="checkbox"/>	If Merchant does store cardholder data, such data is only paper reports or copies of paper receipts and is not received electronically.	

Part 3. PCI DSS Validation

Based on the results noted in the SAQ B 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 B, 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 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 type="checkbox"/>	No evidence of magnetic stripe (i.e., 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.

² 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.

³ 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.

⁴ 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	
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"/>	
7	Restrict access to cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
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 B

Date of Completion:

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Question		Response:		Special*
		Yes	No	
3.2	Do all systems adhere to the following requirements regarding storage of sensitive authentication data after authorization (even if encrypted)?	<input type="checkbox"/>	<input type="checkbox"/>	
3.2.1	<p>Do not store the full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.</p> <p><i>In the normal course of business, the following data elements from the magnetic stripe may need to be retained:</i></p> <ul style="list-style-type: none"> ▪ <i>The cardholder's name,</i> ▪ <i>Primary account number (PAN),</i> ▪ <i>Expiration date, and</i> ▪ <i>Service code</i> <p><i>To minimize risk, store only these data elements as needed for business. NEVER store the card verification code or value or PIN verification value data elements.</i></p> <p><i>Note: See PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms for additional information.</i></p>	<input type="checkbox"/>	<input type="checkbox"/>	
3.2.2	<p>Do not store the card-validation code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.</p> <p><i>Note: See PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms for additional information.</i></p>	<input type="checkbox"/>	<input type="checkbox"/>	
3.2.3	Do not store the personal identification number (PIN) or the encrypted PIN block.	<input type="checkbox"/>	<input type="checkbox"/>	
3.3	<p>Is the PAN masked when displayed? The first six and last four digits are the maximum number of digits to be displayed.)</p> <p><i>Notes:</i></p> <ul style="list-style-type: none"> ▪ <i>This requirement does not apply to employees and other parties with a specific need to see the full PAN;</i> ▪ <i>This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts.</i> 	<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.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Question		Response:	<u>Yes</u>	<u>No</u>	<u>Special*</u>
4.2	Are policies, procedures, and practices in place to preclude the sending of unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat)?		<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.

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know

Question	Response:	Yes	No	Special*
7.1 Is access to system components and cardholder data limited to only those individuals whose jobs require such access?		<input type="checkbox"/>	<input type="checkbox"/>	

Requirement 9: Restrict physical access to cardholder data

Question	Response:	Yes	No	Special*
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:	Yes	No	Special*
12.1	Is a security policy established, published, maintained, and disseminated, and does it accomplish the following:		<input type="checkbox"/>	<input type="checkbox"/>	
12.1.3	Includes a review at least once a year and updates when the environment changes?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3	(a) Are usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants [PDAs], e-mail, and Internet usage) developed to define proper use of these technologies for all employees and contractors?		<input type="checkbox"/>	<input type="checkbox"/>	
12.4	Do the security policy and procedures clearly define information security responsibilities for all employees and contractors?		<input type="checkbox"/>	<input type="checkbox"/>	
12.5	Are the following information security management responsibilities assigned to an individual or team?				
12.5.3	Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations?		<input type="checkbox"/>	<input type="checkbox"/>	
12.6	Is a formal security awareness program in place to make all employees aware of the importance of cardholder data security?		<input type="checkbox"/>	<input type="checkbox"/>	
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.