



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

**Imprint Machines or Stand-alone Dial-out
Terminals Only, no Electronic Cardholder Data
Storage**

Version 1.1

February 2008

Table of Contents

PCI Data Security Standard: Related Documents	iii
Before you Begin.....	iv
Completing the Self-Assessment Questionnaire	iv
PCI DSS Compliance – Completion Steps	iv
Attestation of Compliance, SAQ B.....	1
Self-Assessment Questionnaire B.....	4
Protect Cardholder Data	4
<i>Requirement 3: Protect stored cardholder data.....</i>	<i>4</i>
<i>Requirement 4: Encrypt transmission of cardholder data across open, public networks</i>	<i>4</i>
Implement Strong Access Control Measures	5
<i>Requirement 7: Restrict access to cardholder data by business need-to-know.....</i>	<i>5</i>
<i>Requirement 9: Restrict physical access to cardholder data.....</i>	<i>5</i>
Maintain an Information Security Policy	6
<i>Requirement 12: Maintain a policy that addresses information security for employees and contractors</i>	<i>6</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 ¹
<i>PCI Data Security Standard: Self-Assessment Questionnaire B and Attestation</i>	Merchants ¹
<i>PCI Data Security Standard: Self-Assessment Questionnaire C and Attestation</i>	Merchants ¹
<i>PCI Data Security Standard: Self-Assessment Questionnaire D and Attestation</i>	Service providers and all other merchants ¹
<i>PCI DSS Glossary, Abbreviations, and Acronyms</i>	All merchants and service providers

¹ 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 B has been developed to address requirements applicable to merchants who process cardholder data only via imprint machines or stand-alone dial-up terminals.

These merchants are defined as SAQ Validation Types 2 and 3, here and in the *PCI DSS Self-Assessment Questionnaire Instructions and Guidelines*. SAQ Validation Type 2 merchants process cardholder data only via imprint machines. SAQ Validation Type 3 merchants process cardholder data only via stand-alone, dial-out terminals. Both of these merchant types may be either brick-and-mortar (card-present) or e-commerce or mail/telephone order (card-not-present) merchants. These merchants must validate compliance by completing SAQ B and the associated Attestation of Compliance, confirming that:

For Validation Type 2:

- Your company uses only imprint machines;
- Your company does not transmit cardholder data over either a phone line or the Internet;
- Your company retains only paper reports or paper copies of receipts; and
- Your company does not store cardholder data in electronic format

For Validation Type 3:

- Your company uses only standalone, dial-out terminals (connected via a phone line to your processor);
- Your stand-alone dial-out terminals are not connected to any other systems or to the Internet;
- Your company retains only paper reports or paper copies of receipts; and
- Your company does not store cardholder data in electronic format.

Each section of the questionnaire focuses on a specific area of security, based on the requirements in the PCI Data Security Standard.

PCI DSS Compliance – Completion Steps

1. Complete the Self-Assessment Questionnaire (SAQ B) 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 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). 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. 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. <input type="checkbox"/>	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;
	or	
<input type="checkbox"/>	B. <input type="checkbox"/>	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 retains only paper reports or paper copies of receipts; and	
<input type="checkbox"/>	Merchant does not store cardholder data in electronic format.	

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:

- PCI DSS Self-Assessment Questionnaire B, Version (*version of SAQ*), was completed according to the instructions therein.
- All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment.
- I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
- I have read the PCI DSS and I recognize that I must maintain full PCI DSS compliance at all times.
- No evidence of magnetic stripe (i.e., track) data², CAV2, CVC2, CID, or CVV2 data³, or PIN data⁴ storage subsequent to transaction authorization was found on ANY systems reviewed during this assessment.

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> ↑	

² Data encoded in the magnetic stripe used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data subsequent to 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 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:	
		Yes	No
3.2	Do all systems adhere to the following requirements regarding storage of sensitive authentication data?	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	Do not store the full contents of any track from the magnetic stripe (that is on the back of a card, in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data. <i>In the normal course of business, the following data elements from the magnetic stripe may need to be retained: the accountholder's name, primary account number (PAN), expiration date, and service code. To minimize risk, store only those data elements needed for business. NEVER store the card verification code or value or PIN verification value data elements.</i>	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	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.	<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	Is the PAN masked when displayed? The first six and last four digits are the maximum number of digits to be displayed.) <i>Note: This requirement does not apply to employees and other parties with a specific need to see the full PAN; nor does the requirement 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"/>

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

4.2	Are policies, procedures, and practices in place to preclude the sending of unencrypted PANs by e-mail?	<input type="checkbox"/>	<input type="checkbox"/>
-----	---	--------------------------	--------------------------

Implement Strong Access Control Measures

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

	Question	Response:	Yes	No
			<input type="checkbox"/>	<input type="checkbox"/>
7.1	Is access to computing resources and cardholder information limited to only those individuals whose jobs require such access?		<input type="checkbox"/>	<input type="checkbox"/>

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:	<u>Yes</u>	<u>No</u>
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 (such as modems and wireless) 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	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"/>