



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

---

**Payment Application Connected to Internet,  
No Electronic Cardholder Data Storage**

**Version 1.1**

February 2008

## Table of Contents

---

<b>PCI Data Security Standard: Related Documents .....</b>	<b>ii</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 C.....</b>	<b>2</b>
<b>Self-Assessment Questionnaire C.....</b>	<b>6</b>
<b>Build and Maintain a Secure Network.....</b>	<b>6</b>
<i>Requirement 1: Install and maintain a firewall configuration to protect data .....</i>	<i>6</i>
<i>Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters .....</i>	<i>6</i>
<b>Protect Cardholder Data .....</b>	<b>7</b>
<i>Requirement 3: Protect stored cardholder data.....</i>	<i>7</i>
<i>Requirement 4: Encrypt transmission of cardholder data across open, public networks .....</i>	<i>7</i>
<b>Maintain a Vulnerability Management Program.....</b>	<b>8</b>
<i>Requirement 5: Use and regularly update anti-virus software or programs .....</i>	<i>8</i>
<i>Requirement 6: Develop and maintain secure systems and applications .....</i>	<i>8</i>
<b>Implement Strong Access Control Measures .....</b>	<b>8</b>
<i>Requirement 7: Restrict access to cardholder data by business need-to-know.....</i>	<i>8</i>
<i>Requirement 8: Assign a unique ID to each person with computer access .....</i>	<i>8</i>
<i>Requirement 9: Restrict physical access to cardholder data.....</i>	<i>9</i>
<b>Regularly Monitor and Test Networks .....</b>	<b>10</b>
<i>Requirement 10: Track and monitor all access to network resources and cardholder data. ....</i>	<i>10</i>
<i>Requirement 11: Regularly test security systems and processes .....</i>	<i>10</i>
<b>Maintain an Information Security Policy .....</b>	<b>11</b>
<i>Requirement 12: Maintain a policy that addresses information security for employees and contractors .....</i>	<i>11</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 C has been developed to address requirements applicable to merchants who process cardholder data via payment applications (for example, POS systems) connected to the Internet (via high-speed connection, DSL, cable modem, etc.), but who do not store cardholder data on any computer system. These payment applications are connected to the Internet either because:

1. The payment application is on a personal computer connected to the Internet, or
2. The payment application is connected to the Internet to transmit cardholder data.

These merchants are defined as SAQ Validation Type 4, as defined here and in the *PCI DSS Self-Assessment Questionnaire Instructions and Guidelines*. Validation Type 4 merchants process cardholder data via POS machines connected to the Internet, do not store cardholder data on any computer system, and may be either brick-and-mortar (card-present) or e-commerce or mail/telephone-order (card-not-present) merchants. Such merchants must validate compliance by completing SAQ C and the associated Attestation of Compliance, confirming that:

- Your company has a payment application system and an Internet connection on the same device;
- The payment application/Internet device is not connected to any other systems within your environment;
- Your company retains only paper reports or paper copies of receipts;
- Your company does not store cardholder data in electronic format; and
- Your company's payment application vendor uses secure techniques to provide remote support to your payment system.

Each section of this 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 C) according to the instructions in the *Self-Assessment Questionnaire Instructions and Guidelines*.
2. Complete a clean vulnerability scan with a PCI SSC Approved Scanning Vendor (ASV), and obtain evidence of a passing scan from the ASV.
3. Complete the Attestation of Compliance in its entirety.
4. Submit the SAQ, evidence of a passing scan, and the Attestation of Compliance, along with any other requested documentation, to your acquirer.

# Attestation of Compliance, SAQ C

## 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 C

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

<input type="checkbox"/>	Merchant has a payment application system and an Internet or public network connection on the same device;
<input type="checkbox"/>	The payment application system/Internet device is not connected to any other system within the merchant environment;
<input type="checkbox"/>	Merchant retains only paper reports or paper copies of receipts;
<input type="checkbox"/>	Merchant does not store cardholder data in electronic format; <b>and</b>
<input type="checkbox"/>	Merchant's payment application software vendor uses secure techniques to provide remote support to merchant's payment application system.

## Part 3. PCI DSS Validation

Based on the results noted in the SAQ C dated (*completion date*), (*Merchant Company Name*) asserts the following compliance status (check one):

- |                          |  |
|--------------------------|--|
| <input type="checkbox"/> | <b>Compliant:</b> All sections of the PCI SAQ are complete, and all questions answered "yes," resulting in an overall <b>COMPLIANT</b> rating, <b>and</b> a passing scan has been completed by a PCI SSC Approved Scan Vendor, thereby ( <i>Merchant Company Name</i> ) has demonstrated full compliance with the PCI DSS.   |
| <input type="checkbox"/> | <b>Non-Compliant:</b> Not all sections of the PCI SAQ are complete, or some questions are answered "no," resulting in an overall <b>NON-COMPLIANT</b> rating, <b>or</b> a passing scan has not been completed by a PCI SSC Approved Scan Vendor, thereby ( <i>Merchant Company Name</i> ) has not demonstrated full compliance with the PCI DSS. <ul style="list-style-type: none"><li>▪ <b>Target Date</b> for Compliance:</li><li>▪ 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. <i>Check with your acquirer or the payment brand(s) before completing Part 4, since not all payment brands require this section.</i></li></ul> |

### Part 3a. Confirmation of Compliant Status

**Merchant confirms:**

<input type="checkbox"/>	PCI DSS Self-Assessment Questionnaire C, 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 in all material respects.
<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 <sup>2</sup> , CAV2, CVC2, CID, or CVV2 data <sup>3</sup> , or PIN data <sup>4</sup> 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> ↑

*Merchant Company Represented* ↑

<sup>2</sup> 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.

<sup>3</sup> 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.

<sup>4</sup> 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	
1	Install and maintain a firewall configuration to protect cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input type="checkbox"/>	<input type="checkbox"/>	
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"/>	
5	Use and regularly update anti-virus software	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Assign a unique ID to each person with computer access	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security	<input type="checkbox"/>	<input type="checkbox"/>	

## Self-Assessment Questionnaire C

Date of Completion:

### Build and Maintain a Secure Network

#### Requirement 1: Install and maintain a firewall configuration to protect data

	Question	Response:	YES	NO
1.3	(a) Does the firewall configuration restrict connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks?		<input type="checkbox"/>	<input type="checkbox"/>
1.4	(a) Does the firewall configuration prohibit direct public access between external networks and any system component that stores cardholder data (for example, databases, logs, trace files),		<input type="checkbox"/>	<input type="checkbox"/>

#### Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

	Question	Response:	YES	NO
2.1	Are vendor-supplied defaults always changed <b>before</b> installing a system on the network? <i>Examples include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.</i>		<input type="checkbox"/>	<input type="checkbox"/>
2.1.1	Are wireless environment defaults changed before installing a wireless system? <i>Wireless environment defaults include but are not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings.</i>		<input type="checkbox"/>	<input type="checkbox"/>
	(a) Are SSID broadcasts disabled?		<input type="checkbox"/>	<input type="checkbox"/>
	(b) Is WiFi protected access (WPA and WPA2) technology enabled for encryption and authentication when WPA-capable?		<input type="checkbox"/>	<input type="checkbox"/>
2.3	Is all non-console administrative access encrypted? <i>Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.</i>		<input type="checkbox"/>	<input type="checkbox"/>

## 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

4.1	Are strong cryptography and security protocols, such as secure sockets layer (SSL) / transport layer security (TLS) and Internet protocol security (IPSEC), used to safeguard sensitive cardholder data during transmission over open, public networks?  <i>Examples of open, public networks that are in scope of the PCI DSS are the Internet, WiFi (IEEE 802.11x), global system for mobile communications (GSM), and general packet radio service (GPRS).</i>		<input type="checkbox"/>	<input type="checkbox"/>
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"/>

## Maintain a Vulnerability Management Program

### *Requirement 5: Use and regularly update anti-virus software or programs*

	Question	Response:	YES	NO
5.1	Is anti-virus software deployed on all systems commonly affected by viruses (particularly personal computers and servers)? <i>Note: Systems commonly affected by viruses typically do not include UNIX-based operating systems or mainframes.</i>		<input type="checkbox"/>	<input type="checkbox"/>
5.1.1	Are anti-virus programs capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware?		<input type="checkbox"/>	<input type="checkbox"/>
5.2	Are all anti-virus mechanisms current, actively running, and capable of generating audit logs?		<input type="checkbox"/>	<input type="checkbox"/>

### *Requirement 6: Develop and maintain secure systems and applications*

6.1	(a) Do all system components and software have the latest vendor-supplied security patches installed?		<input type="checkbox"/>	<input type="checkbox"/>
	(b) Are relevant security patches installed within one month of release?		<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
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 8: Assign a unique ID to each person with computer access*

8.5.6	Are accounts used by vendors for remote maintenance enabled only during the time period needed?		<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"/>

## Regularly Monitor and Test Networks

### *Requirement 10: Track and monitor all access to network resources and cardholder data*

Question	Response:	YES	NO
No questions applicable to SAQ C.			

### *Requirement 11: Regularly test security systems and processes*

11.1	(a) Are security controls, limitations, network connections, and restrictions tested annually to assure the ability to adequately identify and to stop any unauthorized access attempts?	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Is a wireless analyzer used at least quarterly to identify all wireless devices in use?	<input type="checkbox"/>	<input type="checkbox"/>
11.2	Are internal and external network vulnerability scans run at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades)?  <b>Note:</b> Quarterly external vulnerability scans must be performed by a scan vendor qualified by the payment card industry. Scans conducted after network changes may be performed by the company's internal staff.	<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
12.1	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"/>