



PCI Compliance
673-401 Woodland Square Loop SE, Lacey, WA 98503 • Phone: 800.687.8505
Fax: 1.866.371.1521 • Email: PCI@FrontStreamPayments.com

Attention: PCI Compliance

Please return this Cover Letter with your Self Assessment Questionnaire (SAQ) to FrontStream Payments via fax, mail or email. To ensure accuracy of the information we have on file, please fill in the following information as well.

If you have any questions please contact our PCI Compliance Department at 800.687.8505 or PCI@FrontStreamPayments.com

Business Legal Name:	Business DBA:
Merchant ID:	PCI Contact Person:
Phone:	Email:
Fax:	Best time/method to contact:

Please note that email or fax may be utilized for SAQ and/or scan renewal notices.

Please provide the following details if you have received your compliance certificate through a source other than FrontStream Payments. If applicable please provide PCI Approved Scanning Vendor (ASV) information.

SAQ Assessment Source And date of Compliance	
PCI Approved Scanning Vendor (ASV), Scan Date and Result:	

Notes: (any questions or comments you might have)

--

Please return your signed SAQ and/or compliance certificate to:

Fax: (866) 371-1521
Email: PCI@FrontStreamPayments.com
Mail: FrontStream Payments
Attn: PCI Compliance
673-401 Woodland Square Loop SE
Lacey, WA 98503

FrontStream Payments | 673 Woodland Square Loop SE, Suite 401 | Lacey, WA 98503
800.687.8505 (Toll Free) / 360.357.1400



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

**Imprint Machines or Standalone Dial-out
Terminals Only, No Electronic Cardholder Data
Storage**

Version 2.0

October 2010

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 standalone, dial-out terminals.

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

- Your company uses only imprint machines and/or uses only standalone, dial-out terminals (connected via a phone line to your processor) to take your customers' payment card information;
- The standalone, dial-out terminals are not connected to any other systems within your environment;
- The standalone, dial-out terminals are not connected to the Internet;
- Your company does not transmit cardholder data over a network (either an internal network or the Internet);
- Your company retains only paper reports or paper copies of receipts with cardholder data, and these documents are not received electronically; **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 DSS Requirements and Security Assessment Procedures*. This shortened version of the SAQ includes questions which apply to a specific type of small merchant environment, as defined in the above eligibility criteria. If there are PCI DSS requirements applicable to your environment which are not covered in this SAQ, it may be an indication that this SAQ is not suitable for your environment. Additionally, you must still comply with all applicable PCI DSS requirements in order to be PCI DSS compliant.

PCI DSS Compliance – Completion Steps

1. Assess your environment for compliance with the PCI DSS.
2. Complete the Self-Assessment Questionnaire (SAQ B) according to the instructions in the *Self-Assessment Questionnaire Instructions and Guidelines*.
3. Complete the Attestation of Compliance in its entirety.
4. Submit the SAQ and the Attestation of Compliance, along with any other requested documentation, to your acquirer.

Guidance for Non-Applicability of Certain, Specific Requirements

Non-Applicability: Requirements deemed not applicable to your environment must be indicated with "N/A" in the "Special" column of the SAQ. Accordingly, complete the "Explanation of Non-Applicability" worksheet in Appendix D for each "N/A" entry.

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. Merchant and Qualified Security Assessor Information

Part 1a. Merchant Organization Information

Company Name:		DBA(S):			
Contact Name:		Title:			
Telephone:		E-mail:			
Business Address		City:			
State/Province:		Country:		ZIP:	
URL/Website:					

Part 1b. 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. 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 2a. Relationships

- Does your company have a relationship with one or more third-party agents (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 2b. Transaction Processing

How and in what capacity does your business store, process and/or transmit cardholder data?

Please provide the following information regarding the Payment Applications your organization uses:

<u>Payment Application in Use</u>	<u>Version Number</u>	<u>Last Validated according to PABP/PA-DSS</u>

Part 2c. Eligibility to Complete SAQ B

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

- 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
- Merchant uses only standalone, dial-out terminals; and the standalone, dial-out terminals are not connected to the Internet or any other systems within the merchant environment;
- Merchant does not store cardholder data in electronic format; **and**
- 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.

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 ↑

² Data encoded in the magnetic stripe or equivalent data on a chip 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 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 for all personnel.	<input type="checkbox"/>	<input type="checkbox"/>	



Self-Assessment Questionnaire B

Note: The following questions are numbered according to PCI DSS requirements and testing procedures, as defined in the PCI DSS Requirements and Security Assessment Procedures document.

Date of Completion:

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

PCI DSS Question		Response:	Yes	No	Special*
3.2	(b) If sensitive authentication data is received and deleted, are processes in place to securely delete the data to verify that the data is unrecoverable?		<input type="checkbox"/>	<input type="checkbox"/>	
	(c) Do all systems adhere to the following requirements regarding non-storage of sensitive authentication data after authorization (even if encrypted)?				
3.2.1	<p>The full contents of any track from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored under any circumstance? 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"> ▪ The cardholder's name, ▪ Primary account number (PAN), ▪ Expiration date, and ▪ Service code <p><i>To minimize risk, store only these data elements as needed for business.</i></p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.2	The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored under any circumstance?		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.3	The personal identification number (PIN) or the encrypted PIN block are not stored under any circumstance?		<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"> ▪ This requirement does not apply to employees and other parties with a specific need to see the full PAN; ▪ This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts. 		<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

PCI DSS Question		Response:	<u>Yes</u>	<u>No</u>	<u>Special</u> *
4.2	(b) Are policies in place that state that unprotected PANs are not to be sent via end-user messaging technologies?		<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

PCI DSS Question		Response:	<u>Yes</u>	<u>No</u>	<u>Special*</u>
7.1	Is access to system components and cardholder data limited to only those individuals whose jobs require such access as follows:				
7.1.1	Are access rights for privileged user IDs restricted to least privileges necessary to perform job responsibilities?		<input type="checkbox"/>	<input type="checkbox"/>	
7.1.2	Are privileges assigned to individuals based on job classification and function (also called "role-based access control" or RBAC)?		<input type="checkbox"/>	<input type="checkbox"/>	

Requirement 9: Restrict physical access to cardholder data

PCI DSS Question		Response:	<u>Yes</u>	<u>No</u>	<u>Special*</u>
9.6	Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)? <i>For purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data.</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?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Do controls include the following:				
9.7.1	Is media classified so the sensitivity of the data can be determined?		<input type="checkbox"/>	<input type="checkbox"/>	
9.7.2	Is media sent by secured courier or other delivery method that can be accurately tracked?		<input type="checkbox"/>	<input type="checkbox"/>	
9.8	Are logs maintained to track all media that is moved from a secured area, and is management approval obtained prior to moving the media (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?		<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.

PCI DSS Question		Response:	<u>Yes</u>	<u>No</u>	<u>Special*</u>
9.10	Is all media destroyed when it is no longer needed for business or legal reasons?		<input type="checkbox"/>	<input type="checkbox"/>	
	Is destruction performed as follows:				
9.10.1	(a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Are containers that store information to be destroyed secured to prevent access to the contents? (For example, a "to-be-shredded" container has a lock preventing access to its contents.)		<input type="checkbox"/>	<input type="checkbox"/>	

Maintain an Information Security Policy

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

PCI DSS Question		Response:	Yes	No	Special*
12.1	Is a security policy established, published, maintained, and disseminated to all relevant personnel? <i>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.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
12.1.3	Is the information security policy reviewed at least once a year and updated as needed to reflect changes to business objectives or the risk environment?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3	Are usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants [PDAs], e-mail, and Internet usage) developed to define proper use of these technologies for all personnel, and require the following:				
12.3.1	Explicit approval by authorized parties to use the technologies?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.3	A list of all such devices and personnel with access?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.5	Acceptable uses of the technologies?		<input type="checkbox"/>	<input type="checkbox"/>	
12.4	Do the security policy and procedures clearly define information security responsibilities for all personnel?		<input type="checkbox"/>	<input type="checkbox"/>	
12.5	Are the following information security management responsibilities formally 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	(a) Is a formal security awareness program in place to make all personnel aware of the importance of cardholder data security?		<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.

PCI DSS 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, as follows?				
12.8.1	Is a list of service providers maintained?		<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?		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.3	Is there an established process for engaging service providers, including proper due diligence prior to engagement?		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.4	Is a program maintained to monitor service providers' PCI DSS compliance status?		<input type="checkbox"/>	<input type="checkbox"/>	

