



Payment Card Industry (PCI) **Data Security Standard**

Attestation of Compliance for Self-Assessment Questionnaire B

For use with PCI DSS Version 4.0

December 2022

Section 1: Assessment Information

Instruction for Submission

This document must be completed as a declaration of the results of the merchant's self-assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact acquirer (merchant bank) or the payment brands to determine reporting and submission procedures.

Part 1. Contact Information

Part 1a. Assessed Merchant

Company name:	Theodore Seeber
DBA (doing business as):	Informationr.us
Company mailing address:	5470 SW Erickson Ave
Company main website:	
Company contact name:	Theodore Seeber
Company contact title:	
Company phone number:	(503) 318-1508
Company e-mail address:	seebert42@gmail.com

Part 1b. Assessor

Provide the following information for all assessors involved in the assessment. If there was no assessor for a given assessor type, enter Not Applicable.

PCI SSC Internal Security Assessor(s)	
ISA name(s):	
Qualified Security Assessor	
Company name:	
Company mailing address:	
Company website:	
Lead Assessor Name:	
Assessor phone number:	
Assessor e-mail address:	
Assessor certificate number:	

Part 2. Executive Summary

Part 2a. Merchant Business Payment Channels (select all that apply):

Indicate all payment channels used by the business that are included in this assessment.

<input checked="" type="checkbox"/> Mail order/telephone order (MOTO)	
<input checked="" type="checkbox"/> E-Commerce	
<input checked="" type="checkbox"/> Card-present	
Are any payment channels not included in this	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

assessment?

If yes, indicate which channel(s) is not included in the assessment and provide a brief explanation about why the channel was excluded.

Note: If the organization has a payment channel that is not covered by this SAQ, consult with the entity(ies) to which this AOC will be submitted about validation for the other channels.

Part 2b. Description of Role with Payment Cards

For each payment channel included in this assessment as selected in Part 2a above, describe how the business stores, processes, and/or transmits account data.

Mail order/telephone order (MOTO)	We do not electronically store or transmit consumer account data.
E-Commerce	We do not electronically store or transmit consumer account data.
Card-present	We do not electronically store or transmit consumer account data.

Part 2c. Description of Payment Card Environment

Provide a **high-level** description of the environment covered by this assessment.

For example:

- Connections into and out of the cardholder data environment (CDE).
- Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.
- System components that could impact the security of account data.

- We process payment cards using a stand-alone terminal that is only connected to our processor via a cellular connection.

Indicate whether the environment includes segmentation to reduce the scope of the assessment.
(Refer to "Segmentation" section of PCI DSS for guidance on segmentation.)

☐ Yes ☒ No

Part 2d. In-Scope Locations/Facilities

List all types of physical locations/facilities (for example, retail locations, corporate offices, data centers, call centers, and mail rooms) in scope for the PCI DSS assessment.

Facility Type	Total number of locations (How many locations of this type are in scope)	Location(s) of facility (city, country)
E-Commerce, Mail/Telephone-Order	1	4228997700829331, Beaverton, OR, US

Part 2f. Third-Party Service Providers

Does the merchant have relationships with one or more third-party service providers that:

- | | |
|---|---|
| • Store, process, or transmit account data on the merchant's behalf (for example, payment gateways, payment processors, payment service providers (PSPs), and off-site storage) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| • Manage system components included in the scope of the merchant's PCI DSS assessment—for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting services, and IaaS, PaaS, SaaS, and FaaS cloud providers. | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| • Could impact the security of the merchant's CDE (for example, vendors providing support via remote access, and/or bespoke software developers) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |

If Yes:

Name of service provider:	Description of service(s) provided:
Paysafe	Clover Go card reader

Note: Requirement 12.8 applies to all entities in this list.

Part 2g. Eligibility to Complete SAQ B

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

- | | |
|-------------------------------------|---|
| <input checked="" 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; and/or
Merchant uses only standalone, dial-out terminals (connected via a phone line to your processor); and the standalone, dial-out terminals are not connected to the Internet or any other systems within the merchant environment; |
| <input checked="" type="checkbox"/> | Merchant does not transmit cardholder data over a network (either an internal network or the Internet); |
| <input checked="" type="checkbox"/> | Merchant does not store cardholder data in electronic format; and |
| <input checked="" type="checkbox"/> | If Merchant does store cardholder data, such data is only paper reports or copies of paper receipts and is not received electronically. |

Section 2: Self-Assessment Questionnaire B

This Attestation of Compliance reflects the results of a self-assessment, which is documented in an accompanying SAQ.

The assessment documented in this attestation and in the SAQ was completed on:	3/22/2024	
Have compensating controls been used to meet any requirement in the SAQ?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the SAQ identified as being not applicable (N/A)?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the SAQ unable to be met due to a legal constraint?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ B (Section 2), dated (3/22/2024).

Based on the results documented in the SAQ B noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (**check one**):

<input checked="" type="checkbox"/>	Compliant: All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby (<i>Informationr.us</i>) has demonstrated full compliance with the PCI DSS.						
<input type="checkbox"/>	Non-Compliant: Not all sections of the PCI DSS SAQ are complete, or not all questions are answered affirmatively, resulting in an overall NON-COMPLIANT rating, thereby (<i>Informationr.us</i>) 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. <i>Check with your acquirer or the payment brand(s) before completing Part 4.</i>						
<input type="checkbox"/>	Compliant but with Legal exception: One or more requirements are marked "No" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand. <i>If checked, complete the following:</i> <table border="1" data-bbox="245 963 1455 1108"> <thead> <tr> <th>Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met				
Affected Requirement	Details of how legal constraint prevents requirement being met						

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

<input checked="" type="checkbox"/>	PCI DSS Self-Assessment Questionnaire B, Version (4.0), was completed according to the instructions therein.
<input checked="" 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 checked="" type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

Part 3a. Acknowledgement of Status (continued)

<input checked="" type="checkbox"/>	No evidence of full track data ¹ , CAV2, CVC2, CID, or CVV2 data ² , or PIN data ³ 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>Aperia</i>)

Part 3b. Merchant Attestation

Theodore M. Seeber

Signature of Merchant Executive Officer [↑]	Date: 3/22/2024
Merchant Executive Officer Name: Theodore M. Seeber	Title: Sole Proprietor

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:

Signature of Duly Authorized Officer of QSA Company [↑]	Date:
Duly Authorized Officer Name:	QSA Company:

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:

¹ 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 track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

² The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

³ 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 Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to 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.

PCI DSS Requirement*	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
3	Protect stored cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

* PCI DSS Requirements indicated here refer to the questions in Section 2 of the SAQ.

