

Payment Card Industry (PCI) Data Security Standard

Attestation of Compliance for Self Assessments - Merchants

Version 3.2.1
January 2021

Attestation of Compliance, SAQ A 3.2.1

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the merchant's 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 your acquirer (merchant bank) or the payment brands for reporting and submission procedures.

Part 1. and Qualified Security Assessor Information

Part 1a. Organization Information

Company Name:	Smile Train Inc.	DBA (doing business as):	
Contact Name:	Beatriz Day	Title:	Computer User
Telephone:	8775437645	E-mail:	bgday@smiletrain.org
Business Address:	633 Third Ave, 9th Floor	City:	New York
State/Province:	NY	Country:	United States
		Zip:	10017
URL:			

Part 1b. Qualified Security Assessor Company Information (Not applicable: self-attested)

Company Name:			
Lead QSA Contact Name:		Title:	
Telephone:		E-mail:	
Business Address:		City:	
State/Province:		Country:	
		Zip:	
URL:			

Part 2. Executive Summary

Part 2a. Type of Merchant Business (check all that apply)

- | | | |
|---|--|--|
| <input type="checkbox"/> Retailer | <input type="checkbox"/> Telecommunication | <input type="checkbox"/> Grocery and Supermarkets |
| <input type="checkbox"/> Petroleum | <input type="checkbox"/> E-Commerce | <input type="checkbox"/> Mail order/telephone order (MOTO) |
| <input type="checkbox"/> Others (please specify): | | |

What types of payment channels does your business serve?

- ☐ Mail order/telephone order (MOTO)
- ☐ E-Commerce
- ☐ Card-present (face-to-face)

Which payment channels are covered by this assessment?

- ☐ Mail order/telephone order (MOTO)
- ☐ E-Commerce
- ☐ Card-present (face-to-face)

Note: If your organization has a payment channel or process that is not covered by this assessment, consult your acquirer or payment brand about validation for other channels.

Part 2b. Description of Payment Card Business

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

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility	Number of facilities of this type	Location(s) of facility (city, country)
------------------	-----------------------------------	---

Part 2d. Payment Application

Does the organization use one or more Payment Applications? ☐ Yes ☒ No

Part 2e. Description of 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 POS devices, databases, web servers, etc., and any other necessary payment components, as applicable

Does your business use network segmentation to affect the scope of your PCI DSS environment?
(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)

☐ Yes ☐ No

Part 2f. Third-Party Service Providers

Does your company use a Qualified Integrator & Reseller (QIR)?		<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Does your company share cardholder data with any third-party service providers (for example, Qualified Integrator & Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.)?		<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Name of service provider:	Description of services provided:	
None	Co-Location	
Rackspace Managed Hosting (www.rackspace.com)	Web Host	

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

Part 2g. Eligibility to Complete SAQ A

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

<input checked="" type="checkbox"/>	Merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions;
<input checked="" type="checkbox"/>	All payment acceptance and processing are entirely outsourced to PCI DSS validated third-party service providers
<input checked="" type="checkbox"/>	Merchant has no direct control of the manner in which cardholder data is captured, processed, transmitted, or stored;
<input checked="" type="checkbox"/>	Merchant does not electronically store, process, or transmit any cardholder data on merchant systems or premises, but relies entirely on a third party(s) to handle all these functions;
<input checked="" type="checkbox"/>	Merchant has confirmed that all third party(s) handling acceptance, storage, processing, and/or transmission of cardholder data are PCI DSS compliant; and
<input checked="" type="checkbox"/>	Merchant retains only paper reports or receipts with cardholder data, and these documents are not received electronically.
	<i>Additionally, for e-commerce channels</i>
<input checked="" type="checkbox"/>	The entirety of all payment pages delivered to the consumer's browser originates directly from a third-party PCI DSS validated service provider(s).

Section 2: Self-Assessment Questionnaire A

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

The assessment documented in this attestation and in the SAQ was completed on:	2020-05-26
Have compensating controls been used to meet any requirement in the SAQ?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Were any requirements in the SAQ identified as being not applicable (N/A)?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Were any requirements in the SAQ unable to be met due to legal constraint?	<input type="checkbox"/> Yes <input type="checkbox"/> No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the SAQ A dated (2020-05-26).

Based on results documented in the SAQ 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>Smile Train Inc.</i> has demonstrated full compliance with PCI DSS.
<input type="checkbox"/>	Non-Compliant: Not all sections of the PCI DSS SAQ are complete, or not all questions answered affirmatively, resulting in an overall NON-COMPLIANT rating; thereby <i>Smile Train Inc.</i> has not demonstrated full compliance with 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 "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.

Part 3a. Acknowledgement of Status

Signatory(s) confirms:
(Check all that apply)

<input checked="" type="checkbox"/>	PCI DSS Self-Assessment Questionnaire A, Version 3.2.1, 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 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.
<input checked="" type="checkbox"/>	No evidence of full track data, CAV2, CVC2, CID, or CVV2 data, or PIN data storage after transaction authorization was found on ANY system reviewed during this assessment.

Part 3b. Attestation

ELECTRONICALLY ATTESTED

Signature of Executive Officer ^	Date: 2020-05-26
Executive Officer Name: Beatriz Day	Title: Computer User

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

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

N/A: Self-Attested only

Signature of Duly Authorized Officer of QSA Company ^

Date:

Duly Authorized Officer Name:

QSA Company:

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

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