Payment Card Industry (PCI)

Data Security Standard

Attestation of Compliance for Self-Assessment Questionnaire P2PE

For use with PCI DSS Version 3.2.1

September 2020

Section 1: Assessment Information

Instructions 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 (PCI DSS) Requirements and Security Assessment Procedures*. 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 to determine reporting and submission procedures.

Part 1. Merchant and Qualified Security Assessor Information

Part 1a. Merchant Organization Information

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

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. Executive Summary

Part 2a: Type of merchant business (check all that apply):

☐ Retailer	☐ Telecommunication	☐ Grocery and Supermarkets
☐ Petroleum	☐ Mail/Telephone-Order (MOTO)	☐ Others (please specify):

What types of payment channels does your business serve?	Which payment channels are covered by this SAQ?
☐ Mail order/telephone order (MOTO)	☐ Mail order/telephone order (MOTO)
☐ E-Commerce	
☐ Card-present (face-to-face)	☐ Card-present (face-to-face)

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

Part 2. Executive Summary *(continued)*

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)
Example: Retail outlets	*3*	*Boston, MA, USA*

Part 2d. P2PE Solution

Provide the following information from the PCI SSC listing regarding the validated PCI-listed P2PE solution your organization uses:

Name of P2PE Solution Provider:	
Name of P2PE Solution:	
PCI SSC listing "Reference #"	
Listed POI Devices used by Merchant (found under "PTS POI Devices Supported):	
P2PE Solution "Reassessment Date":	

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 2. Executive Summary *(continued)*

Part 2f. Third-Party Service Providers

Does your company use a Qualified Integrator & Reseller (QIR)?	☐ Yes ☐ No

If Yes:

Name of QIR Company:	
QIR Individual Name:	
Description of services provided by QIR:	

Does your company share cardholder data with any third-party service providers (for example, Qualified Integrator & Resellers (QIR), gateways, airline booking agents, loyalty program agents, etc.)?	☐ Yes ☐ No

If Yes:

Name of service provider:	**Description of services provided:**

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

Part 2g. Eligibility to Complete SAQ P2PE

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

☐	All payment processing is via the validated PCI-listed P2PE solution (per above).
☐	The only systems in the merchant environment that store, process or transmit account data are the payment terminals that are part of the validated PCI-listed P2PE solution.
☐	Merchant does not otherwise receive or transmit cardholder data electronically.
☐	Merchant verifies there is no legacy storage of electronic cardholder data.
☐	Any such cardholder data the Merchant might retain is only on paper (for example, paper reports or copies of paper receipts) and is not received electronically, **and**
☐	Merchant has implemented all controls in the P2PE Instruction Manual (PIM) provided by the P2PE Solution Provider.

Section 2: Self-Assessment Questionnaire P2PE

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:		
Have compensating controls been used to meet any requirement in the SAQ?	☐ Yes	☐ No
Were any requirements in the SAQ identified as being not applicable (N/A)?	☐ Yes	☐ No
Were any requirements in the SAQ unable to be met due to a legal constraint?	☐ Yes	☐ No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ P2PE (Section 2), dated *(SAQ completion date).*

Based on the results documented in the SAQ P2PE 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):***

☐	**Compliant:** All sections of the PCI DSS SAQ P2PE are complete, and all questions answered affirmatively, 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 DSS SAQ P2PE are complete, or not all questions are answered affirmatively, 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.*
☐	**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. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(*Check all that apply*)

☐	PCI DSS Self-Assessment Questionnaire P2PE, 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 read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.

Part 3a. Acknowledgement of Status (continued)	
☐	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.
☐	No evidence of, full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3]) was found on ANY system reviewed during this assessment.

Part 3b. Merchant Attestation	
Signature of Merchant Executive Officer ↑	*Date:*
Merchant Executive Officer Name:	*Title:*

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 magnetic-stripe data after transaction authorization. The only elements of track data that may be retained are account number, expiration date, and name.

[2] 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.

[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 Status

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, since not all payment brands require this section.

PCI DSS Requirement*	Description of Requirement	Compliance to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
3	Protect stored cardholder data	☐	☐	
9	Restrict physical access to cardholder data	☐	☐	
12	Maintain a policy that addresses information security for all personnel	☐	☐	

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