Payment Card Industry
Data Security Standard

Supplemental Attestation of Compliance for Report on Compliance

PCI DSS v4.0 Designated Entities Supplemental Validation

Publication Date: June 2022

Section 1   Assessment Information

Instructions for Submission

** Complete this Attestation of Compliance only if required by a Payment Brand or Acquirer to complete the requirements specified in the PCI DSS v4.0 Appendix A3: Designated Entities Supplemental Validation**

This Supplemental Attestation of Compliance (S-AOC) must be completed as a declaration of the results of the Designated Entity's assessment with *PCI DSS v4.0 Appendix A3: PCI DSS Designated Entities Supplemental Validation (DESV).* The S-AOC is an addendum to the *PCI DSS Attestation of Compliance (AOC)* and is not intended to stand alone. Because of this, details about the environment reviewed for the S-AOC must be included in Part 2: Executive Summary of the AOC for that entity. The Designated Entity is responsible for ensuring that all sections, in both the S-AOC and the AOC, are completed by the relevant parties, as applicable. Contact the entity(ies) to which this S-AOC will be submitted for reporting and submission procedures.

Part 1. Contact Information	
Part 1a. Assessed Entity **(ROC Section 1.1)**	
Company name:	
DBA (doing business as):	
Company mailing address:	
Company main website:	
Company contact name:	
Company contact title:	
Contact phone number:	
Contact e-mail address:	
Part 1b. Assessor **(ROC Section 1.1)**	
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:	
Note: *Section titles and numbers correspond to similar sections within the PCI DSS Attestation of Compliance (AOC). Section numbering was kept intact for clarification purposes.*	

Part 2g. Summary of Assessment

(S-ROC Summary of DESV Results)

Indicate below all responses provided within each principal DESV requirement.

DESV Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If Below Method Was Used
	In Place	**In Place with Remediation**	**Not Applicable**	**Not In Place**	**Compensating Controls**
Requirement A3.1	☐	☐	☐	☐	☐
Requirement A3.2	☐	☐	☐	☐	☐
Requirement A3.3	☐	☐	☐	☐	☐
Requirement A3.4	☐	☐	☐	☐	☐
Requirement A3.5	☐	☐	☐	☐	☐

Section 2 Supplemental Report on Compliance

This Supplemental Attestation of Compliance reflects the results of an assessment that is documented in an accompanying Supplemental Report on Compliance S-ROC for Designated Entities.

The assessment documented in this attestation and in the S-ROC for Designated Entities was completed on:	*YYYY-MM-DD*
Were any requirements in the S-ROC for Designated Entities unable to be met due to a legal constraint?	☐ Yes ☐ No
Were any testing activities performed remotely? If yes, for each testing activity below, indicate whether remote assessment activities were performed: • Examine documentation ☐ Yes ☐ No • Interview personnel ☐ Yes ☐ No • Examine/observe live data ☐ Yes ☐ No • Observe process being performed ☐ Yes ☐ No • Observe physical environment ☐ Yes ☐ No • Interactive testing ☐ Yes ☐ No • Other:	☐ Yes ☐ No

Section 3 Validation and Attestation Details

Part 3. PCI DSS Designated Entities Supplemental Validation

This S-AOC is based on results noted in the S-ROC dated *(S-ROC completion date YYYY-MM-DD).*

Based on the results documented in the S-ROC for Designated Entities noted above, each signatory identified in any of Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document *(select one):*

☐ **Compliant:** All sections of the S-ROC for Designated Entities are complete, and all requirements are marked as being either 1) In Place, 2) In Place with Remediation, or 3) Not Applicable, resulting in an overall **COMPLIANT** rating; thereby *(Designated Entity Company Name)* has demonstrated compliance with all PCI DSS Designated Entities Supplemental Validation requirements.

☐ **Non-Compliant:** Not all sections of the S-ROC for Designated Entities are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating, thereby *(Designated Entity Company Name)* has not demonstrated compliance with PCI DSS Designated Entities Supplemental Validation requirements.

Target Date for Compliance: YYYY-MM-DD

An entity submitting this form with a status of Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. *Confirm with the entity to which this S-AOC will be submitted before completing Part 4.*

☐ **Compliant but with Legal exception:** One or more requirements of the S-ROC for Designated Entities are marked "Not in Place" due to a legal restriction that prevents the requirement from being met and all other requirements are marked as being either 1) In Place, 2) In Place with Remediation, or 3) Not Applicable, resulting in an overall COMPLIANT BUT WITH LEGAL EXCEPTION rating; thereby has demonstrated compliance with all PCI DSS Designated Entities Supplemental Validation requirements except those noted as Not in Place due to a legal restriction.

This option requires additional review from the entity to which this S-AOC will be submitted. *If selected, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement from being met

Part 3a. Designated Entity Acknowledgement

Signatory(s) confirms:

(Select all that apply)

☐	The S-ROC for Designated Entities was completed according to *PCI DSS Version 4.0 Appendix A3: Designated Entities Supplemental Validation* and was completed according to the instructions therein.
☐	All information within the above-referenced S-ROC for Designated Entities and in this attestation fairly represents the results of the assessment in all material respects.
☐	*PCI DSS Appendix A3: Designated Entities Supplemental Validation* (DESV) controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Designated Entity Attestation

Signature of Designated Entity Executive Officer ↑	*Date:*
Designated Entity Executive Officer Name:	*Title:*

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:	☐ QSA performed testing procedures.
	☐ QSA provided other assistance. If selected, describe all role(s) performed:

Signature of Lead QSA ↑	Date: YYYY-MM-DD
Lead QSA Name:	

Signature of Duly Authorized Officer of QSA Company ↑	Date: YYYY-MM-DD
Duly Authorized Officer Name:	QSA Company:

Part 3d. Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:	☐ ISA(s) performed testing procedures.
	☐ ISA(s) provided other assistance. If selected, describe all role(s) performed:

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this S-AOC will be submitted, and only if the Assessment has Non-Compliant results noted in Section 3.

If asked to complete this section, select the appropriate response for "Compliant to DESV Requirements" for each requirement below. For any "No" responses, include the date the entity expects to be compliant with the requirement and provide a brief description of the actions being taken to meet the requirement.

DESV Requirement	Description of Requirement	Compliant to DESV Requirements *(Select One)*		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
A3.1	PCI DSS compliance program is implemented.	☐	☐	
A3.2	PCI DSS scope is documented and validated.	☐	☐	
A3.3	PCI DSS is incorporated into business-as-usual (BAU) activities.	☐	☐	
A3.4	Logical access to the cardholder data environment is controlled and managed.	☐	☐	
A3.5	Suspicious events are identified and responded to.	☐	☐	