



Payment Card Industry Data Security Standard

Self-Assessment Questionnaire D for Service Providers and Attestation of Compliance

For use with PCI DSS Version 4.0

Publication Date: April 2022

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the entity's self-assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures*. Complete all sections: The entity is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which the Attestation of Compliance (AOC) will be submitted for reporting and submission procedures.

Part 1. Contact Information

Part 1a. Assessed Entity

Company name:	Clarity Ventures
DBA (doing business as):	
Company mailing address:	16238 Ranch Road 620 N, Suite E-395 Austin, TX 78717
Company main website:	https://www.clarity-ventures.com/
Company contact name:	Clint Thompson
Company contact title:	Integration Program Manager
Contact phone number:	800.928.8160
Contact e-mail address:	clint.thompson@claritymis.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):	N/A
--------------	-----

Qualified Security Assessor

Company name:	N/A
---------------	-----

Company mailing address:	
--------------------------	--

Company website:	
------------------	--

Lead Assessor Name:	
---------------------	--

Assessor phone number:	
------------------------	--

Assessor e-mail address:	
--------------------------	--

Assessor certificate number:	
------------------------------	--

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the PCI DSS Assessment (select all that apply):

Name of service(s) assessed: Clarity Ventures Payment Hub

Type of service(s) assessed:

Hosting Provider:

- Applications / software
- Hardware
- Infrastructure / Network
- Physical space (co-location)
- Storage
- Web-hosting services
- Security services
- 3-D Secure Hosting Provider
- Multi-Tenant Service Provider
- Other Hosting (specify):

Managed Services (specify):

- Systems security services
- IT support
- Physical security
- Terminal Management System
- Other services (specify):

Payment Processing:

- POI / card present
- Internet / e-commerce
- MOTO / Call Center
- ATM
- Other processing (specify):

Account Management

Fraud and Chargeback

Payment Gateway/Switch

Back-Office Services

Issuer Processing

Prepaid Services

Billing Management

Loyalty Programs

Records Management

Clearing and Settlement

Merchant Services

Tax/Government Payments

Network Provider

Others (specify): Software payment portal (customer portal + virtual terminal) connected to customer's payment gateway (no sensitive PII data retained or stored whatsoever). The portal is either hosted with Clarity Ventures or in the merchant's own servers.

Note: These categories are provided for assistance only and are not intended to limit or predetermine an entity's service description. If these categories do not apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.

Part 2. Executive Summary *(continued)*

Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (select all that apply):

Name of service(s) not assessed:	Customer managed web services and platform integrations	
Type of service(s) not assessed:		
Hosting Provider: <input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web-hosting services <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Multi-Tenant Service Provider <input type="checkbox"/> Other Hosting (specify):	Managed Services (specify): <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input checked="" type="checkbox"/> Other services (specify): Web development, e-commerce site development, enterprise resource planning software, etc.	Payment Processing: <input type="checkbox"/> POI / card present <input type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Network Provider		
<input type="checkbox"/> Others (specify):		
Provide a brief explanation why any checked services were not included in the assessment:	Standard services did not include providing payment connections.	

Part 2b. Description of Role with Payment Cards

Describe how the business stores, processes, and/or transmits account data.	We do not store, process, or transmit cardholder data. We send all data to payment gateways and/or other tokenization agents. We then store tokens; never cardholder data. The payment gateway always transmits and processes payment.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	There are both client and server side authentications required to access the payment pages of our product. Cardholder data is typed into form fields but immediately sent to the payment gateway for tokenization.
Describe system components that could impact the security of account data.	None. We do not store, process, or transmit cardholder data. We send all data to payment gateways and/or other tokenization agents. We then store tokens; never cardholder data. The payment gateway always transmits and processes payment.

Part 2. Executive Summary *(continued)*

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.*

Cardholder is entered into client side browser application that is authenticated by a username/password combination. Cardholder data is submitted to an authenticated web server, either hosted by Clarity Ventures or the merchant. The cardholder data is immediately transmitted to the merchant's payment gateway and/or a tokenization agent. The token is then passed back to Clarity Ventures or the merchant's web server to be stored in the Payment Hub payment application.

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, 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)
<i>Example: Data centers</i>	3	<i>Boston, MA, USA</i>

Part 2. Executive Summary *(continued)*

Part 2e. PCI SSC Validated Products and Solutions

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions*?

Yes No

Provide the following information regarding each item the entity uses from PCI SSC's Lists of Validated Products and Solutions.

Name of PCI SSC-validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which product or solution was validated	PCI SSC listing reference number	Expiry date of listing (YYYY-MM-DD)
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD

* For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components appearing on the PCI SSC website (www.pcisecuritystandards.org)—for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Payment Applications (PA-DSS), Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, and Contactless Payments on COTS (CPoC) solutions.

Part 2. Executive Summary *(continued)*

Part 2f. Third-Party Service Providers

For the services being validated, does the entity have relationships with one or more third-party service providers that:

<ul style="list-style-type: none"> Store, process, or transmit account data on the entity'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
<ul style="list-style-type: none"> Manage system components included in the scope of the entity'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
<ul style="list-style-type: none"> Could impact the security of the entity'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:
WorldPay Element payment gateway	Payment Hub transmits cardholder data to WorldPay for tokenization and processing of cardholder information.

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

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment

(SAQ Section 2 and related appendices)

Indicate below all responses that were selected for each PCI DSS requirement.

PCI DSS Requirement	Requirement Responses					
	<i>More than one response may be selected for a given requirement. Indicate all responses that apply.</i>					
	In Place	In Place with CCW	In Place with Remediation	Not Applicable	Not Tested	Not in Place
Requirement 1:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 2:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 3:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 6:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 7:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 9:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 12:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ D (Section 2), dated (Self-assessment completion date 2022-08-19).

Indicate below whether a full or partial PCI DSS assessment was completed:

- Full** – All requirements have been assessed therefore no requirements were marked as Not Tested in the SAQ.
- Partial** – One or more requirements have not been assessed and were therefore marked as Not Tested in the SAQ. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the SAQ D 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:

<input type="checkbox"/>	<p>Compliant: All sections of the PCI DSS SAQ are complete, and all assessed 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 (<i>Service Provider Company Name</i>) has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not Tested above.</p>								
<input checked="" type="checkbox"/>	<p>Non-Compliant: Not all sections of the PCI DSS SAQ are complete, or one or more requirements are marked as Not in Place, resulting in an overall NON-COMPLIANT rating, thereby (<i>Clarity Ventures</i>) has not demonstrated compliance with the PCI DSS requirements included in this SAQ.</p> <p>Target Date for Compliance: 2023-01-31</p> <p>An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted <i>before completing Part 4</i>.</p>								
<input type="checkbox"/>	<p>Compliant but with Legal exception: One or more assessed requirements in the PCI DSS SAQ are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed 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 (<i>Service Provider Company Name</i>) has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not Tested above or as Not in Place due to a legal restriction.</p> <p>This option requires additional review from the entity to which this AOC will be submitted. <i>If selected, complete the following:</i></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 40%;">Affected Requirement</th> <th>Details of how legal constraint prevents requirement from being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement from being met						
Affected Requirement	Details of how legal constraint prevents requirement from being met								

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:

(Select all that apply)

<input checked="" type="checkbox"/>	PCI DSS Self-Assessment Questionnaire D, 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 the entity's assessment in all material respects.
<input checked="" type="checkbox"/>	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

Chris Reddick

Signature of Service Provider Executive Officer ↑	Date: 2022-08-25
Service Provider Executive Officer Name: Chris Reddick	Title: CEO

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. PCI SSC 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 AOC will be submitted, and only if the Assessment has a Non-Compliant status noted in Section 3.

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

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	
1	Install and maintain network security controls	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Apply secure configurations to all system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored account data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems and networks from malicious software	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and software	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to system components and cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify users and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	Log and monitor all access to system components and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Test security systems and networks regularly	<input type="checkbox"/>	<input checked="" type="checkbox"/>	ASV scans will begin in Q1 2023. However, external vulnerability scans ARE completed annually per internal guidelines. Additionally, no CDE and no Account Data ever exist.
12	Support information security with organizational policies and programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

