



# **Payment Card Industry Data Security Standard**

---

## **Attestation of Compliance for Report on Compliance – Service Providers**

**Version 4.0.1**

Publication Date: August 2024

# **PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers**

**Entity Name: Liquid Web, LLC**

**Date of Report as noted in the Report on Compliance: March 18, 2025**

**Date Assessment Ended: March 6, 2025**

## Section 1: Assessment Information

### Instructions for Submission

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

This AOC reflects the results documented in an associated Report on Compliance (ROC). Associated ROC sections are noted in each AOC Part/Section below.

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Report on Compliance Template.

#### Part 1. Contact Information

##### Part 1a. Assessed Entity (ROC Section 1.1)

Company name:	Liquid Web, LLC
DBA (doing business as):	Liquid Web
Company mailing address:	2703 Ena Dr. Lansing, MI 48917
Company main website:	www.liquidweb.com
Company contact name:	Nathan Mollenkopf
Company contact title:	Change and Compliance Manager
Contact phone number:	(800) 580-4985
Contact e-mail address:	nmollenkopf@liquidweb.com

##### 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):	Not Applicable
--------------	----------------

##### Qualified Security Assessor

Company name:	UHY Consulting, Inc.
Company mailing address:	980 Hammond Dr #100, Atlanta, GA 30328
Company website:	www.uhy-us.com
Lead Assessor name:	Jamison See
Assessor phone number:	248-204-9477
Assessor e-mail address:	jsee@uhy-us.com
Assessor certificate number:	QSA – 204-445

## Part 2. Executive Summary

### Part 2a. Scope Verification

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

Name of service(s) assessed: Data Center Services (Collocation)

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:

- ☐ 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):

**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 Assessment (select all that apply):**

Name of service(s) not assessed: Virtual Private Hosting, Dedicated Hosted, and Cloud Sites

Type of service(s) not 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:

- ☒ 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):

Provide a brief explanation why any checked services were not included in the Assessment:

The scope of this ROC includes only the physical security services the company provides to customers as part of the Data Center Services service offering.

### Part 2b. Description of Role with Payment Cards (ROC Sections 2.1 and 3.1)

Describe how the business stores, processes, and/or transmits account data.

The company does not store, process, or transmit cardholder data on behalf of customers as part of their service offerings.

Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.

The company does not store, process, or transmit cardholder data on behalf of customers as part of their service offerings. Customers using the company's services may store, process, and/or transmit cardholder data for their own business processes. Maintaining security and compliance related to transaction

	processing is the responsibility of the company's customers. The company maintains controls and processes over the physical security of systems hosted in their data centers and management of hosting platforms as part of their service offerings.
Describe system components that could impact the security of account data.	The company does not store, process, or transmit cardholder data on behalf of customers as part of their service offerings. Customers using the company's services may store, process, and/or transmit cardholder data for their own business processes. Maintaining security and compliance related to transaction processing is the responsibility of the company's customers. The company maintains controls and processes over the physical security of systems hosted in their data centers and management of hosting platforms as part of their service offerings.

## 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.*

The company does not store, process, or transmit cardholder data on behalf of customers as part of their service offerings.

Indicate whether the environment includes segmentation to reduce the scope of the Assessment.

(Refer to the "Segmentation" section of PCI DSS for guidance on segmentation)

☐ Yes ☒ No

### Part 2d. In-Scope Locations/Facilities (ROC Section 4.6)

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this Assessment.

Facility Type	Total Number of Locations (How many locations of this type are in scope)	Location(s) of Facility (city, country)
Data Centers	2	Lansing, MI, USA

## Part 2. Executive Summary *(continued)*

### Part 2e. PCI SSC Validated Products and Solutions (ROC Section 3.3)

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions<sup>♦</sup>?

☐ 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
Not Applicable				

\* 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](http://www.pcisecuritystandards.org)) (for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions), and Mobile Payments on COTS (MPoC) products.

♦ 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](http://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 (ROC Section 4.4)

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

• 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 type="checkbox"/> Yes <input checked="" type="checkbox"/> No
• Manage system components included in the entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers)	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

**If Yes:**

Name of Service Provider:	Description of Services Provided:
Not Applicable	

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

## Part 2. Executive Summary *(continued)*

### Part 2g. Summary of Assessment (ROC Section 1.8.1)

Indicate below all responses provided within each principal PCI DSS requirement.

For all requirements identified as either “Not Applicable” or “Not Tested,” complete the “Justification for Approach” table below.

**Note:** One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.

Name of Service Assessed: Data Center Services (Collocation)

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If a Compensating Control(s) Was Used
	In Place	Not Applicable	Not Tested	Not in Place	
Requirement 1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 3:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 6:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 7:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 9:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 10:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 12:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A1:	<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 checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A3:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Justification for Approach

## Part 2. Executive Summary *(continued)*

<p>For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.</p>	<p>9.2.4 - Not Applicable - There are no user accessible consoles in the data centers.</p> <p>9.4 - Not Applicable - The organization does not store or provide cardholder data storage as part of their service offering.</p> <p>9.5 - Not Applicable - The organization's cardholder environment does not include POI devices.</p> <p>12.3.2 - Not Applicable - The organization does not use a Customized Approach method to meet any requirements.</p> <p>12.3.3 - Not Applicable - Requirements related to cryptographic suites and protocols are in in-scope for this assessment.</p> <p>12.3.4 - Not Applicable - The organization has not adopted this best practice early.</p> <p>12.4.2, 12.4.2.1 - Not Applicable – The scope of this assessment was limited to Requirements 9 &amp; 12 and as a result the specified quarterly review component are for requirements that are not in scope for this assessment.</p> <p>12.5.2.1, 12.5.3 - Not Applicable - The organization has not adopted this best practice early.</p> <p>12.6.3.2 - Not Applicable - The organization has not adopted this best practice early.</p> <p>12.8 - Not applicable - The company does not have relationships with third-party service providers that affect physical security controls at their Data Centers.</p> <p>12.10.7 - Not Applicable - The organization has not adopted this best practice early.</p>
<p>For any Not Tested responses, identify which sub-requirements were not tested and the reason.</p>	<p>Requirements 1 – 8, 10, 11, and Appendix A – The scope of the ROC include only the Data Center Services physical security service offering which limited the scope of the assessment to Requirements 9 &amp; 12.</p>

## Section 2 Report on Compliance

### (ROC Sections 1.2 and 1.3)

Date Assessment began: <b>Note:</b> <i>This is the first date that evidence was gathered, or observations were made.</i>	October 25, 2024
Date Assessment ended: <b>Note:</b> <i>This is the last date that evidence was gathered, or observations were made.</i>	March 6, 2025
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any testing activities performed remotely?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

## Section 3 Validation and Attestation Details

### Part 3. PCI DSS Validation (ROC Section 1.7)

**This AOC is based on results noted in the ROC dated** *(Date of Report as noted in the ROC March 18, 2025).*

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

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

Based on the results documented in the ROC 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 checked="" type="checkbox"/>	<p><b>Compliant:</b> All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall <b>COMPLIANT</b> rating; thereby <i>(Liquid Web, LLC)</i> has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.</p>								
<input type="checkbox"/>	<p><b>Non-Compliant:</b> Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall <b>NON-COMPLIANT</b> rating; thereby <i>(Liquid Web, LLC)</i> has not demonstrated compliance with PCI DSS requirements.</p> <p><b>Target Date</b> for Compliance: Not Applicable</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 before completing Part 4.</p>								
<input type="checkbox"/>	<p><b>Compliant but with Legal exception:</b> One or more assessed requirements in the ROC 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 In Place or Not Applicable, resulting in an overall <b>COMPLIANT BUT WITH LEGAL EXCEPTION</b> rating; thereby <i>(Liquid Web, LLC)</i> has demonstrated compliance with all PCI DSS requirements 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.</p> <p><i>If selected, complete the following:</i></p> <table border="1"> <thead> <tr> <th>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 3. PCI DSS Validation *(continued)*

#### Part 3a. Service Provider Acknowledgement

**Signatory(s) confirms:**

(Select all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to <i>PCI DSS</i> , Version 4.0.1 and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of the 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



Signature of Service Provider Executive Officer ↑	Date: March 18, 2025
Service Provider Executive Officer Name: Scott Arlen	Title: Director of Network and Security Ops

#### 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: Not Applicable



Signature of Lead QSA ↑	Date: March 18, 2025
Lead QSA Name: Jamison See	

Signature of Duly Authorized Officer of QSA Company ↑

Date: March 18, 2025

Duly Authorized Officer Name: Jamison See

QSA Company: UHY Consulting, Inc.

#### 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: Not Applicable

## 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 Non-Compliant results 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 provide 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 type="checkbox"/>	<input type="checkbox"/>	
2	Apply secure configurations to all system components	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored account data	<input type="checkbox"/>	<input type="checkbox"/>	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems and networks from malicious software	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and software	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to system components and cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identify users and authenticate access to system components	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
10	Log and monitor all access to system components and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Test security systems and networks regularly	<input type="checkbox"/>	<input type="checkbox"/>	
12	Support information security with organizational policies and programs	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	<input 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 type="checkbox"/>	<input type="checkbox"/>	

*Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance accepting organization to ensure that this form is acceptable in their program. For more information about PCI SSC and our stakeholder community please visit: [https://www.pcisecuritystandards.org/about\\_us/](https://www.pcisecuritystandards.org/about_us/)*