



# **Payment Card Industry Data Security Standard**

---

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

**Version 4.0**

Revision 2

Publication Date: August 2023

# **PCI DSS v4.0 Attestation of Compliance for Report on Compliance – Service Providers**

**Entity Name: AlumnIQ**

**Assessment End Date: 2024-06-30**

**Date of Report as noted in the Report on Compliance: 2024-07-01**

## 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:	AlumniQ
DBA (doing business as):	
Company mailing address:	10 Verbena Ct., Cheshire, CT 06410
Company main website:	<a href="https://www.alumniq.com/">https://www.alumniq.com/</a>
Company contact name:	Steve Rittler
Company contact title:	Founder/CEO
Contact phone number:	6108101550x1
Contact e-mail address:	steve@alumniq.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):	
Qualified Security Assessor	
Company name:	
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 Assessment (select all that apply):

Name of service(s) assessed: AlumniQ Signature Events Service

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:

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:

### Part 2b. Description of Role with Payment Cards (ROC Section 2.1)

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

Depending on the client, payment information is captured by Spreedly, Braintree, or Blackbaud, vaulted in their PCI compliant vault, and then routed for payment processing to the appropriate gateway. The limit of our surface area for compliance is the secure injection of the Spreedly/Braintree/Blackbaud scripts to initiate the card information capture - the software and underlying services that paint this page is the complete extent of our CDE. At no time does AlumniQ have the capacity to see cardholder data, and you'll see many requirements marked Not Applicable as a result.

	<p>It is our understanding that if we were not a service provider, the SAQ-A would entirely cover the scope of our application's services.</p>
<p>Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.</p>	<p>Proper customer education about the role of their staff in proper payment handling, including strong recommendations to send links to their constituents to enter payment information when and as needed so they are never exposed to any CHD even inadvertently.</p>
<p>Describe system components that could impact the security of account data.</p>	<p>The web/application server is the resource that demands the most careful protection as the code in that environment is what drives the insertion of the payment modal (contents and target entirely attached to Spreedly/Braintree/Blackbaud). The backing database server cluster is secondary. All of this sits behind a load balancer and web application firewall, providing the only public traffic channel to the web server. The database is not publicly exposed at all.</p>

## 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.*

ALB > WAF > Web Server > Application Server > Database.

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)
<i>Example: Data centers</i>	3	<i>Boston, MA, USA</i>
AWS Data Center (US-EAST-1)	1	Virginia, 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\*?

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

\* 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 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:

<ul style="list-style-type: none"> <li>• 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))</li> </ul>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
<ul style="list-style-type: none"> <li>• 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)</li> </ul>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
<ul style="list-style-type: none"> <li>• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).</li> </ul>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

**If Yes:**

<b>Name of Service Provider:</b>	<b>Description of Services Provided:</b>
AWS	Hosting, perimeter network security, internal network security, systems management, logging <a href="https://aws.amazon.com/compliance/pci-dss-level-1-faqs/">https://aws.amazon.com/compliance/pci-dss-level-1-faqs/</a>
Spreadly	Payment information capture, vaulting, routing <a href="https://www.spreadly.com/pci">https://www.spreadly.com/pci</a>
Blackbaud	Payment information capture, vaulting, routing <a href="https://www.blackbaud.com/security/pci-compliance">https://www.blackbaud.com/security/pci-compliance</a>
Braintree	Payment information capture, vaulting, routing <a href="https://www.braintreepayments.com/features/data-security">https://www.braintreepayments.com/features/data-security</a>
Tailscale	VPN services
Google	SSO for administrative access, IAM
Github	Code repository

**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: AlumnIQ Signature Events Service

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If Below Method(s) Was Used	
	In Place	Not Applicable	Not Tested	Not in Place	Customized Approach	Compensating Controls
Requirement 1:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 2:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Requirement 6:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Requirement 7:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 10:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11:	<input checked="" 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 checked="" type="checkbox"/>
Appendix A1:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Justification for Approach**

<p>For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.</p>	<p>           1.3 - we do not have a CDE            1.4.4 - we do not have any components that store cardholder data            1.5.1 - we do not have any components that transmit or store cardholder data            2.3.1 - no wireless network            2.3.2 - no wireless network            3.2.1 - we do not have cardholder data to store            3 - we do not have cardholder data            4.2.1.2 - no wireless networks            4.2.2 - no messaging services            5.3.3 - no removable media in scope            7.2.6 - we do not have cardholder data            8.2.3 - we have no such accounts            8.2.7 - we have no such accounts            8.3.10 - we do not have cardholder data            8.3.11 - we do not use this            9 - we do not have access to cardholder data, so this entire section is moot            10.2.1 - no access to cardholder data because we do not have cardholder data            11.2.1 - we do not have a wireless network (nor a physical location where one could be maliciously activated)            11.2.2 - we do not have a wireless network (nor a physical location where one could be maliciously activated)         </p>
<p>For any Not Tested responses, identify which sub-requirements were not tested and the reason.</p>	

## Section 2 Report on Compliance

(ROC Sections 1.2 and 1.3.2)

Date Assessment began: <i>Note: This is the first date that evidence was gathered, or observations were made.</i>		2024-06-09
Date Assessment ended: <i>Note: This is the last date that evidence was gathered, or observations were made.</i>		2024-06-30
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? If yes, for each testing activity below, indicate whether remote assessment activities were performed:		<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
• Examine documentation	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
• Interview personnel	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
• Examine/observe live data	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
• Observe process being performed	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
• Observe physical environment	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
• Interactive testing	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
• Other:	<input 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 2024-07-01)*.

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 AlumnIQ 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>(Service Provider Company Name)</i> has not demonstrated compliance with PCI DSS requirements.</p> <p><b>Target Date</b> for Compliance: YYYY-MM-DD</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>(Service Provider Company Name)</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" data-bbox="289 1497 1395 1724"> <thead> <tr> <th data-bbox="289 1497 631 1575">Affected Requirement</th> <th data-bbox="631 1497 1395 1575">Details of how legal constraint prevents requirement from being met</th> </tr> </thead> <tbody> <tr> <td data-bbox="289 1575 631 1623"></td> <td data-bbox="631 1575 1395 1623"></td> </tr> <tr> <td data-bbox="289 1623 631 1671"></td> <td data-bbox="631 1623 1395 1671"></td> </tr> <tr> <td data-bbox="289 1671 631 1724"></td> <td data-bbox="631 1671 1395 1724"></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 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

<i>Signature of Service Provider Executive Officer</i> ↑	Date: 2024-07-01
Service Provider Executive Officer Name: Stephen C. Rittler	Title: Founder/CEO

#### Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:	<input type="checkbox"/> QSA performed testing procedures.
	<input type="checkbox"/> QSA provided other assistance. If selected, describe all role(s) performed:

<i>Signature of Lead QSA</i> ↑	Date: YYYY-MM-DD
Lead QSA Name:	

<i>Signature of Duly Authorized Officer of QSA Company</i> ↑	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:	<input type="checkbox"/> ISA(s) performed testing procedures.
	<input type="checkbox"/> 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 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"/>	

