Docusign Envelope ID: 7F5170B0-53E8-447D-BCA6-3185FB81655E



Payment Card Industry
Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0.1

Publication Date: August 2024

Docusign Envelope ID: 7F5170B0-53E8-447D-BCA6-3185FB81655E

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

Entity Name: Limio

Date of Report as noted in the Report on Compliance: 26th February 2026

Date Assessment Ended: 13th February 2026

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 7F5170B0-53E8-447D-BCA6-3185FB81655E

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:	Innovate42 Ltd
DBA (doing business as):	Limio
Company mailing address:	Unit 13.2.1 The Leather Market, Weston Street, London, England, SE1 3ER
Company main website:	https://www.limio.com/
Company contact name:	Daniel Morton
Company contact title:	CTO
Contact phone number:	+44 (0) 20 3827 0250
Contact e-mail address:	daniel@limio.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:	Dionach Ltd
Company mailing address:	Unipart House, Garsington Road, Oxford, United Kingdom OX4 2PG
Company website:	https://www.dionach.com/
Lead Assessor name:	Hakim Fubara
Assessor phone number:	+441865877830
Assessor e-mail address:	hakim.fubara@dionach.com
Assessor certificate number:	206-585

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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:	Limio Integration 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): Integration Services	**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 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.	Limio provides subscription shop and self-service portal solutions that allows pricing, checkout, payment, and account experiences using standardised templates and integrations. This allows their customers to build custom solutions that significantly reduce the time to launch, without having to write any code. This includes options for Salesforce or direct website integration with Limio's Amazon AWS environment.

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 7F5170B0-53E8-447D-BCA6-3185FB81655E

	Limio only operates as a managed service provider for the integration of the payment service providers as a fully outsourced PCI DSS compliant payment service provider on behalf of their customers. Limio do not hold the merchant contract or have access to the payment service provider portals. Limio only integrates the payment solution as an iframe or fully hosted payment page for their customers.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Limio does not store, process, or transmit payment card data on behalf of their merchant customers and only provide the integration layer.
Describe system components that could impact the security of account data.	Limio does not store, process, or transmit payment card data on behalf of their merchant customers and only provide the integration layer. Limio can control or impact the security of cardholder data through the integration of the PSP (iframe or hosted payment page only) for the customer in the code that they generate, and host on the platforms that they provide.

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 7F5170B0-53E8-447D-BCA6-3185FB81655E

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.*	Limio provides a SaaS platform that allows Limio's customers to build commerce solutions that integrate with PSP to allow end users to purchase subscriptions. The commercial relationship with the PSP is with Limio's customers and it is the responsibility of Limio's customers to ensure the PSP is PCI DSS compliant. Limio delivers the solution though two mechanisms • Limio E-Commerce infrastructure • Salesforce Managed package The Limio E-Commerce infrastructure is the production system that interfaces directly with the end customer's browser. The only interface to the customer's browser is via AWS CloudFront. The Limio E-Commerce infrastructure does not directly interface with a CDE. The scope includes the systems that generate the code that will deliver the redirect or iframe URL to the end user's browser, including: • The build environment (AWS) • The software development lifecycle (SDLC) • GitHub where the source code is managed. All of these environments are physically separate from the Limio E-Commerce infrastructure.
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 centres, call centres and mail rooms) in scope for this Assessment.

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 7F5170B0-53E8-447D-BCA6-3185FB81655E

Facility Type	Total Number of Locations (How many locations of this type are in scope)	Location(s) of Facility (city, country)
Example: Data centers	*3*	*Boston, MA, USA*
Not Applicable	Not Applicable	Not Applicable

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 7F5170B0-53E8-447D-BCA6-3185FB81655E

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))	☐ Yes ☒ 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)	☒ Yes ☐ No
• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	☐ Yes ☒ No

If Yes:

Name of Service Provider:	**Description of Services Provided:**
Amazon Web Services	Hosting platform for the Limio services
GitHub	Source Code Repository

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

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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: Limio Integration Services

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:	☐	☒	☐	☐	☐
Requirement 2:	☒	☐	☐	☐	☐
Requirement 3:	☐	☒	☐	☐	☐
Requirement 4:	☐	☒	☐	☐	☐
Requirement 5:	☐	☒	☐	☐	☐
Requirement 6:	☒	☒	☐	☐	☐
Requirement 7:	☒	☒	☐	☐	☐
Requirement 8:	☒	☒	☐	☐	☐
Requirement 9:	☐	☒	☐	☐	☐
Requirement 10:	☒	☒	☐	☐	☐
Requirement 11:	☒	☒	☐	☐	☐
Requirement 12:	☒	☐	☐	☐	☐
Appendix A1:	☐	☒	☐	☐	☐
Appendix A2:	☐	☒	☐	☐	☐

Justification for Approach

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 7F5170B0-53E8-447D-BCA6-3185FB81655E

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	**Requirement 1** Limio does not store, process, or transmit CHD on any network. Payment processing is outsourced to a PCI DSS compliant TPSP. **Requirement 2.2.5** No insecure services, protocols, or daemons are present in Limio environment. **Requirement 2.3** No wireless present in Limio environment. **Requirement 3** Limio does not store, process or transmit CHD. **Requirement 4** Limio does not transmit CHD. All payment processing is outsourced to a PCI Compliant Payment Service Provider. **Requirement 5** There are no networks or Systems in scope for this assessment. **Requirement 6.4.3** Limio clients are responsible for all payment page scripts that are loaded and executed in their consumer's browser. **Requirement 6.5.5** Limio does not store, process or transmit CHD and there is no mechanism for CHD to be entered into the Limio environment. **Requirements 7.2.6, 8.4.1, 8.4.2, 8.4.3** Limio does not store Cardholder Data. **Requirement 8.2.3** Limio does not have remote access to customer premises. **Requirement 8.2.7** Third-party access is not enabled. **Requirements 8.3.9, 8.3.10.1** Passwords are not the only authentication factor to log onto the in-scope systems. MFA is in place. **Requirement 8.3.10** Limio does not support customer user access to the environment. **Requirement 8.3.11** There are no physical or logical security tokens, smart cards, or certificates in use for authentication. **Requirement 8.6.1** Interactive logins are expressly prohibited. **Requirement 9** Limio does not have any physical access to Cardholder Data. **Requirements 10.2.1, 10.2.1.1** There is no cardholder data in the Limio environment.

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 7F5170B0-53E8-447D-BCA6-3185FB81655E

	Requirements 11.2.1, 11.2.2 No wireless access points in-scope for Limio. **Requirements 11.4.5, 11.4.6** There is no CDE in scope for this assessment, so no segmentation has been used. **Requirement 11.4.7** Limio is not a multi-tenant provider. **Requirement 11.6.1** Limio clients are responsible for managing changes to payment pages in their environment. **Appendix A1** Limio is not a multi-tenant service provider. **Appendix A2** Limio does not use SSL/early TLS as a security control, nor does it provide connections into POS POI terminals that use SSL/early TLS.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	Not applicable

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 7F5170B0-53E8-447D-BCA6-3185FB81655E

Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*	2026-02-09
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	2026-02-13
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No
Were any testing activities performed remotely?	☒ Yes ☐ No

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 7F5170B0-53E8-447D-BCA6-3185FB81655E

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 2026-02-26)*.

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)*:

☒	**Compliant:** 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 **COMPLIANT** rating; thereby *Limio* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.
☐	**Non-Compliant:** 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 **NON-COMPLIANT** rating; thereby *(Service Provider Company Name)* has not demonstrated compliance with PCI DSS requirements. **Target Date** for Compliance: *YYYY-MM-DD* 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.
☐	**Compliant but with Legal exception:** 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 **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Service Provider Company Name)* 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. This option requires additional review from the entity to which this AOC will be submitted. *If selected, complete the following:*

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

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 7F5170B0-53E8-447D-BCA6-3185FB81655E

Part 3. PCI DSS Validation *(continued)*

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:
(Select all that apply)

☒	The ROC was completed according to *PCI DSS*, Version 4.0.1 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
☒	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

DocuSigned by:
Daniel Morton
DBB3DBAEB26F469...

Signature of Service Provider Executive Officer ↑	Date: 2026-02-26
Service Provider Executive Officer Name: Daniel Morton	Title: CTO

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:

Signed by:
Hakim Fubara
16B93A8139EB472...

Signature of Lead QSA ↑	Date: 2026-02-26
Lead QSA Name: Hakim Fubara	

DocuSigned by:
Bil Bragg
B02FE02F6A7A49E...

Signature of Duly Authorized Officer of QSA Company ↑	Date: 2026-02-26
Duly Authorized Officer Name: Bil Bragg	QSA Company: Dionach Ltd

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:

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 7F5170B0-53E8-447D-BCA6-3185FB81655E

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	☐	☐	
2	Apply secure configurations to all system components	☐	☐	
3	Protect stored account data	☐	☐	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	☐	☐	
5	Protect all systems and networks from malicious software	☐	☐	
6	Develop and maintain secure systems and software	☐	☐	
7	Restrict access to system components and cardholder data by business need to know	☐	☐	
8	Identify users and authenticate access to system components	☐	☐	
9	Restrict physical access to cardholder data	☐	☐	
10	Log and monitor all access to system components and cardholder data	☐	☐	
11	Test security systems and networks regularly	☐	☐	
12	Support information security with organizational policies and programs	☐	☐	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	☐	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☐	☐	

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/

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.