Docusign Envelope ID: B8A8423E-17EF-4BE9-81D3-27B83C849605

Payment Card Industry
Data Security Standard

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

For use with PCI DSS Version 4.0.1

Revision 1

Publication Date: December 2024

Docusign Envelope ID: B8A8423E-17EF-4BE9-81D3-27B83C849605

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.

This AOC reflects the results documented in an associated Self-Assessment Questionnaire (SAQ).

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Self-Assessment Questionnaire.

Part 1. Contact Information	
Part 1a. Assessed Entity	
Company name:	Congruit Inc.
DBA (doing business as):	Congruit Credit
Company mailing address:	1703 N McMullen Booth Road, #207, Safety Harbor FL 34695
Company main website:	congruitcredit.com
Company contact name:	Jim James
Company contact title:	CTO
Contact phone number:	+1.727.735.2983
Contact e-mail address:	jim.james@congruitcredit.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):	Not Applicable
Qualified Security Assessor	
Company name:	Johanson Group LLP
Company mailing address:	6547 North Academy Blvd #105 Colorado Springs, CO 80918
Company website:	https://johansongroupllp.com
Lead Assessor Name:	Anthony Fulda
Assessor phone number:	+1.719.434.0750
Assessor e-mail address:	pci@johansonllp.com
Assessor certificate number:	106-062

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: B8A8423E-17EF-4BE9-81D3-27B83C849605

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:	Credit bureau API platform	
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.*

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: B8A8423E-17EF-4BE9-81D3-27B83C849605

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:	Not Applicable

Type of service(s) not assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POI / card present
☐ Hardware	☐ IT support	☐ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web-hosting services		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service Provider		
☐ Other Hosting (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:	Not Applicable

Part 2b. Description of Role with Payment Cards

Describe how the business stores, processes, and/or transmits account data.	Congruit does not accept credit card details. We do accept and store consumer name, address, and other personal details. We wish to achieve the same level of security as if we accepted credit cards. As a credit bureau, Congruit accepts consumer PII and stores it for use in underwriting. The storage of key consumer items (address, bank account, SSN) is encrypted and tokenized. Such PII is not provided to any external parties, it is only for use within our platform. The terms CHD and CDE in this document are used for the critical portions of our infrastructure and data that relate to consumer PII. Again, no credit card details are accepted.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Appropriate security controls such as TLS encryption, strict access control, and secure application development practices are implemented to protect the

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: B8A8423E-17EF-4BE9-81D3-27B83C849605

	integrity and confidentiality of the data during its handling and storage.
Describe system components that could impact the security of account data.	System components that may impact the security of account data are Congruit's API services and backend infrastructure responsible for retrieving tokenized consumer data. The logic responsible for resolving tokens and initiating secure requests to the client's or third-party vault is critical, as it governs access to consumer PII. Transport layer security infrastructure is used to protect data in transit, ensuring all communications are encrypted and authenticated. Identity and access management systems enforce strict role-based controls, limiting access to only authorized service components. Congruit operates centralized logging, monitoring, and alerting systems to detect unauthorized activity or abnormal usage patterns, even though no cardholder data is logged or stored. These components together play a central role in maintaining the confidentiality and integrity of consumer data during processing.

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: B8A8423E-17EF-4BE9-81D3-27B83C849605

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.*	Connections into the CDE are limited to authenticated API calls over TLS. System components that could impact the security of consumer data include the database backend, token resolution logic, and TLS-enforced data transport paths.
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)
AWS Datacenter	1	US-East-2

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: B8A8423E-17EF-4BE9-81D3-27B83C849605

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)
Not Applicable	Not Applicable	Not Applicable	Not Applicable	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)—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.

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: B8A8423E-17EF-4BE9-81D3-27B83C849605

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:

• 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 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.	☒ 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 service(s) provided:**
AWS	Colocation and platform hosting

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

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: B8A8423E-17EF-4BE9-81D3-27B83C849605

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment

(SAQ Section 2 and related appendices)

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: Credit bureau API platform

PCI DSS Requirement	Requirement Responses *More than one response may be selected for a given requirement. Indicate all responses that apply.*				
	In Place	In Place with CCW	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: B8A8423E-17EF-4BE9-81D3-27B83C849605

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	1.2.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and associated NSCs subject to this requirement.
	1.2.2	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and associated NSCs subject to this requirement.
	1.2.5	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and associated technical configurations subject to this requirement.
	1.2.6	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and associated technical configurations subject to this requirement.
	1.2.7	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and associated NSCs subject to this requirement.
	1.2.8	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and associated NSCs subject to this requirement.
	1.3.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and associated technical configurations subject to this requirement.
	1.3.2	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and associated technical configurations subject to this requirement.
	1.3.3	There are no wireless components used to transmit cardholder data that are subject to this requirement.
	1.4.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and associated technical configurations subject to this requirement.
	1.4.2	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: B8A8423E-17EF-4BE9-81D3-27B83C849605

		CDE and associated technical configurations subject to this requirement.
	1.4.3	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and associated technical configurations subject to this requirement.
	1.4.4	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and associated technical configurations subject to this requirement.
	1.4.5	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and associated technical configurations subject to this requirement.
	1.5.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	2.2.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	2.2.3	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	2.2.4	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	2.2.5	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	2.2.6	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	2.2.7	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: B8A8423E-17EF-4BE9-81D3-27B83C849605

2.3.1	There are no wireless components used to transmit cardholder data that are subject to this requirement.
2.3.2	There are no wireless components used to transmit cardholder data that are subject to this requirement.
3.3.1	Congruit Credit does not store, process, or transmit cardholder data. There is no stored account data (CHD / SAD) that is subject to this requirement.
3.3.1.1	Congruit Credit does not store, process, or transmit cardholder data. There is no stored account data (CHD / SAD) that is subject to this requirement.
3.3.1.2	Congruit Credit does not store, process, or transmit cardholder data. There is no stored account data (CHD / SAD) that is subject to this requirement.
3.3.1.3	Congruit Credit does not store, process, or transmit cardholder data. There is no stored account data (CHD / SAD) that is subject to this requirement.
3.3.2	Congruit Credit does not store, process, or transmit cardholder data. There is no stored account data (CHD / SAD) that is subject to this requirement.
3.3.3	Congruit Credit is not classified as an issuer and does not provide issuing services.
3.4.1	Congruit Credit does not store, process, or transmit cardholder data. There is no stored account data (CHD / SAD) that is subject to this requirement.
3.4.2	Congruit Credit does not store, process, or transmit cardholder data. There is no stored account data (CHD / SAD) that is subject to this requirement.
3.5.1	Congruit Credit does not store, process, or transmit cardholder data. There is no stored account data (CHD / SAD) that is subject to this requirement.
3.5.1.1	Congruit Credit does not store, process, or transmit cardholder data. There is no stored account data (CHD / SAD) that is subject to this requirement.
3.5.1.2	Congruit Credit does not store, process, or transmit cardholder data. There is no stored account data (CHD / SAD) that is subject to this requirement.
3.5.1.3	Congruit Credit does not store, process, or transmit cardholder data. There is no stored

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: B8A8423E-17EF-4BE9-81D3-27B83C849605

	account data (CHD / SAD) that is subject to this requirement.
3.6.1	Congruit Credit does not store, process, or transmit cardholder data. There are no keys or key management operations used to protect stored account data that are subject to this requirement.
3.6.1.1	Congruit Credit does not store, process, or transmit cardholder data. There are no keys or key management operations used to protect stored account data that are subject to this requirement.
3.6.1.2	Congruit Credit does not store, process, or transmit cardholder data. There are no keys or key management operations used to protect stored account data that are subject to this requirement.
3.6.1.3	Congruit Credit does not store, process, or transmit cardholder data. There are no keys or key management operations used to protect stored account data that are subject to this requirement.
3.6.1.4	Congruit Credit does not store, process, or transmit cardholder data. There are no keys or key management operations used to protect stored account data that are subject to this requirement.
3.7.1	Congruit Credit does not store, process, or transmit cardholder data. There are no keys or key management operations used to protect stored account data that are subject to this requirement.
3.7.2	Congruit Credit does not store, process, or transmit cardholder data. There are no keys or key management operations used to protect stored account data that are subject to this requirement.
3.7.3	Congruit Credit does not store, process, or transmit cardholder data. There are no keys or key management operations used to protect stored account data that are subject to this requirement.
3.7.4	Congruit Credit does not store, process, or transmit cardholder data. There are no keys or key management operations used to protect stored account data that are subject to this requirement.
3.7.5	Congruit Credit does not store, process, or transmit cardholder data. There are no keys or key management operations used to protect stored account data that are subject to this requirement.

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: B8A8423E-17EF-4BE9-81D3-27B83C849605

	3.7.6	Congruit Credit does not store, process, or transmit cardholder data. There are no keys or key management operations used to protect stored account data that are subject to this requirement.
	3.7.7	Congruit Credit does not store, process, or transmit cardholder data. There are no keys or key management operations used to protect stored account data that are subject to this requirement.
	3.7.8	Congruit Credit does not store, process, or transmit cardholder data. There are no keys or key management operations used to protect stored account data that are subject to this requirement.
	3.7.9	Congruit Credit does not store, process, or transmit cardholder data. There are no keys or key management operations used to protect stored account data that are subject to this requirement.
	4.2.1	Congruit Credit does not transmit cardholder data and does not manage any keys or certificates subject to this requirement.
	4.2.1.1	Congruit Credit does not transmit cardholder data and does not manage any certificates subject to this requirement.
	4.2.1.2	There are no wireless components used to transmit cardholder data that are subject to this requirement.
	4.2.2	Congruit Credit does not transmit cardholder data using end-user messaging technologies.
	5.2.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	5.2.2	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	5.2.3	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	5.2.3.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: B8A8423E-17EF-4BE9-81D3-27B83C849605

	CDE and system components subject to this requirement.
5.3.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
5.3.2	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
5.3.2.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
5.3.3	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
5.3.4	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
5.3.5	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
5.4.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
6.2.1	Congruit Credit does not develop custom payment software that provides authorization, settlement, or chargeback functions subject to this requirement.
6.2.2	Congruit Credit does not develop custom payment software that provides authorization, settlement, or chargeback functions subject to this requirement.
6.2.3	Congruit Credit does not develop custom payment software that provides authorization, settlement, or chargeback functions subject to this requirement.
6.2.3.1	Congruit Credit does not develop custom payment software that provides

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: B8A8423E-17EF-4BE9-81D3-27B83C849605

	authorization, settlement, or chargeback functions subject to this requirement.
6.2.4	Congruit Credit does not develop custom payment software that provides authorization, settlement, or chargeback functions subject to this requirement.
6.3.2	Congruit Credit does not develop payment software subject to this requirement.
6.4.1	This testing procedure was superseded by Requirement 6.4.2 after 31 March 2025 when Requirement 6.4.2 became effective.
6.5.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
6.5.2	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
6.5.3	Congruit Credit does not develop payment software subject to this requirement.
6.5.4	Congruit Credit does not develop payment software subject to this requirement.
6.5.5	Congruit Credit does not develop payment software subject to this requirement.
6.5.6	Congruit Credit does not develop payment software subject to this requirement.
7.2.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
7.2.2	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
7.2.3	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
7.2.4	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: B8A8423E-17EF-4BE9-81D3-27B83C849605

	7.2.5	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	7.2.5.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	7.2.6	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	7.3.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	7.3.2	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	7.3.3	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	8.2.3	Congruit Credit does not connect to external customer environments.
	8.2.4	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	8.2.6	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	8.2.7	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	8.2.8	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: B8A8423E-17EF-4BE9-81D3-27B83C849605

		CDE and system components subject to this requirement.
	8.3.2	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	8.3.3	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	8.3.4	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	8.3.8	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	8.3.10	This requirement for service providers was superseded by Requirement 8.3.10.1 as of 31 March 2025.
	8.3.10.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	8.3.11	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	8.6.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	8.6.2	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	8.6.3	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: B8A8423E-17EF-4BE9-81D3-27B83C849605

9.4.1	Congruit Credit does not store, process, or transmit cardholder data. There is no media subject to this requirement.
9.4.1.1	Congruit Credit does not store, process, or transmit cardholder data. There is no media subject to this requirement.
9.4.1.2	Congruit Credit does not store, process, or transmit cardholder data. There is no media subject to this requirement.
9.4.2	Congruit Credit does not store, process, or transmit cardholder data. There is no media subject to this requirement.
9.4.3	Congruit Credit does not store, process, or transmit cardholder data. There is no media subject to this requirement.
9.4.4	Congruit Credit does not store, process, or transmit cardholder data. There is no media subject to this requirement.
9.4.5	Congruit Credit does not store, process, or transmit cardholder data. There is no media subject to this requirement.
9.4.5.1	Congruit Credit does not store, process, or transmit cardholder data. There is no media subject to this requirement.
9.4.6	Congruit Credit does not store, process, or transmit cardholder data. There is no media subject to this requirement.
9.4.7	Congruit Credit does not store, process, or transmit cardholder data. There is no media subject to this requirement.
9.5.1	Congruit Credit has no POI devices in scope that are subject to this requirement.
9.5.1.1	Congruit Credit has no POI devices in scope that are subject to this requirement.
9.5.1.2	Congruit Credit has no POI devices in scope that are subject to this requirement.
9.5.1.2.1	Congruit Credit has no POI devices in scope that are subject to this requirement.
9.5.1.3	Congruit Credit has no POI devices in scope that are subject to this requirement.
10.2.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
10.2.1.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: B8A8423E-17EF-4BE9-81D3-27B83C849605

	CDE and system components subject to this requirement.
10.2.1.2	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
10.2.1.3	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
10.2.1.4	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
10.2.1.5	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
10.2.1.6	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
10.2.1.7	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
10.2.2	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
10.3.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
10.3.2	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
10.3.3	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: B8A8423E-17EF-4BE9-81D3-27B83C849605

	10.3.4	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	10.4.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	10.4.1.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	10.4.2	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	10.4.2.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	10.4.3	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	10.5.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	10.6.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	10.6.2	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
	10.6.3	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: B8A8423E-17EF-4BE9-81D3-27B83C849605

10.7.1	This requirement was superseded by Requirement 10.7.2 as of 31 March 2025.
10.7.2	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
10.7.3	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
11.4.1	Congruit Credit does not maintain a payment application that directly stores, processes, or transmits cardholder data.
11.4.2	Congruit Credit does not maintain a payment application that directly stores, processes, or transmits cardholder data.
11.4.3	Congruit Credit does not maintain a payment application that directly stores, processes, or transmits cardholder data.
11.4.4	Congruit Credit does not maintain a payment application that directly stores, processes, or transmits cardholder data.
11.4.5	Congruit Credit does not maintain a payment application that directly stores, processes, or transmits cardholder data.
11.4.6	Congruit Credit does not maintain a payment application that directly stores, processes, or transmits cardholder data.
11.4.7	Congruit Credit is not classified as a multi-tenant service provider.
11.5.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
11.5.1.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
11.5.2	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
12.2.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: B8A8423E-17EF-4BE9-81D3-27B83C849605

	CDE and system components subject to this requirement.
12.3.2	Congruit Credit not using customized approach.
12.3.3	Congruit Credit does not store, process, or transmit cardholder data. There are no keys or key management operations used to protect stored account data that are subject to this requirement.
12.3.4	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
12.5.1	Congruit Credit does not directly store, process, or transmit cardholder data. Congruit Credit and does not maintain a CDE and system components subject to this requirement.
12.5.3	
12.6.2	Congruit Credit does not store, process, or transmit cardholder data. Congruit Credit has no employees subject to this requirement.
12.6.3.2	Congruit Credit does not store, process, or transmit cardholder data. Congruit Credit has no employees subject to this requirement.
12.7.1	Congruit Credit does not store, process, or transmit cardholder data. Congruit Credit has no employees subject to this requirement.
12.10.2	Congruit Credit does not store, process, or transmit cardholder data. Congruit Credit has no employees subject to this requirement.
12.10.3	Congruit Credit does not store, process, or transmit cardholder data. Congruit Credit has no employees subject to this requirement.
12.10.4	Congruit Credit does not store, process, or transmit cardholder data. Congruit Credit has no employees subject to this requirement.
12.10.4.1	Congruit Credit does not store, process, or transmit cardholder data. Congruit Credit has no employees subject to this requirement.
12.10.5	Congruit Credit does not store, process, or transmit cardholder data. Congruit Credit

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: B8A8423E-17EF-4BE9-81D3-27B83C849605

		has no employees subject to this requirement.
	12.10.6	Congruit Credit does not store, process, or transmit cardholder data. Congruit Credit has no employees subject to this requirement.
	A1.1.1	Congruit Credit is not classified as a multi-tenant service provider.
	A1.1.2	Congruit Credit is not classified as a multi-tenant service provider.
	A1.1.3	Congruit Credit is not classified as a multi-tenant service provider.
	A1.1.4	Congruit Credit is not classified as a multi-tenant service provider.
	A1.2.1	Congruit Credit is not classified as a multi-tenant service provider.
	A1.2.2	Congruit Credit is not classified as a multi-tenant service provider.
	A1.2.3	Congruit Credit is not classified as a multi-tenant service provider.
	A2.1.1	Congruit Credit has no POI devices in scope that are subject to this requirement.
	A2.1.2	Congruit Credit has no POI devices in scope that are subject to this requirement.
	A2.1.3	Congruit Credit has no POI devices in scope that are subject to this requirement.
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: B8A8423E-17EF-4BE9-81D3-27B83C849605

Section 2: Self-Assessment Questionnaire D for Service Providers

Self-assessment completion date:	11/17/2025
Were any requirements in the SAQ unable to be met due to a legal constraint?	☐ Yes ☒ No

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: B8A8423E-17EF-4BE9-81D3-27B83C849605

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 *11/17/2025*).

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:

☒	**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 CCW, or 3) Not Applicable, resulting in an overall **COMPLIANT** rating; thereby *(Congruit Inc.)* has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not Tested above.
☐	**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 *(Congruit Inc.)* has not demonstrated compliance with the PCI DSS requirements included in this SAQ. **Target Date** for Compliance: *Not Applicable* 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 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 CCW, or 3) Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Congruit Inc.)* 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. 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: B8A8423E-17EF-4BE9-81D3-27B83C849605

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:

(Select all that apply)

☒	PCI DSS Self-Assessment Questionnaire D, Version *4.0* was completed according to the instructions therein.
☒	All information within the above-referenced SAQ and in this attestation fairly represents the results of the entity's 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

Signed by:
Jim James
0A16C0435856491...

Signature of Service Provider Executive Officer ↑	*Date:* 11/24/2025
Service Provider Executive Officer Name: Jim James	*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. The QSA provided review of Congruit's compliance evidence, including a thorough examination of information security policies and procedures within Congruit's GRC platform. QSA assisted with the validation of scope of services and generation of required compliance documentation.

Signed by:
Anthony Fulda
575C2B57C25A4BB...

Signature of Lead QSA ↑	*Date:* 11/24/2025
Lead QSA Name: Anthony Fulda	

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* 11/24/2025
Duly Authorized Officer Name: Anthony Fulda	*QSA Company:* Johanson Group LLP

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: B8A8423E-17EF-4BE9-81D3-27B83C849605

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	☐	☐	
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 its 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.