Docusign Envelope ID: 17D28E44-14A7-8913-810A-F4C5C263F6FB



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: 17D28E44-14A7-8913-810A-F4C5C263F6FB

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

Entity Name: Inovio Payments, LLC

Date of Report as noted in the Report on Compliance: 2026-09-23

Date Assessment Ended: 2026-09-22

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

Docusign Envelope ID: 17D28E44-14A7-8913-810A-F4C5C263F6FB

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:	Inovio Payments, LLC
DBA (doing business as):	Not Applicable
Company mailing address:	250 Stephenson Highway, Troy, MI 48084
Company main website:	https://inoviopay.com
Company contact name:	Scott Richardson
Company contact title:	Head of Information Compliance and Assurance
Contact phone number:	(720) 673-2679
Contact e-mail address:	srichardson@north.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):	**David Armah** **Joshua Wingate**
Qualified Security Assessor	
Company name:	Wipfli Advisory LLC
Company mailing address:	10000 W Innovation Drive Suite 250, Milwaukee, WI 53226
Company website:	https://wipfli.com
Lead Assessor name:	Matt Goodman
Assessor phone number:	(414) 431-9300
Assessor e-mail address:	matt.goodman@wipfli.com
Assessor certificate number:	206-079

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

Docusign Envelope ID: 17D28E44-14A7-8913-810A-F4C5C263F6FB

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:	InovioPay Payment Processing	
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.

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:	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 (ROC Sections 2.1 and 3.1)

Describe how the business stores, processes, and/or transmits account data.	As a payment gateway, Inovio Payments accepts Visa, MasterCard, American Express, Discover, and Diners Club from merchants and transmits them to processors for payment processing.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Inovio operates and administers an e-commerce payment gateway and the supporting application, database, server, and network infrastructure used to facilitate payment authorization, capture, and settlement. Functions that could impact the security of account data include administration of gateway and

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

Docusign Envelope ID: 17D28E44-14A7-8913-810A-F4C5C263F6FB

	payment-processing applications, management of connections to payment processors and third-party services, network segmentation and network security controls, system and database administration, access management, encryption and key-management activities, security monitoring, vulnerability management, software and payment-page change management, backup and recovery, incident response, and vendor management.
Describe system components that could impact the security of account data.	System components that could impact the security of account data include the payment gateway and its supporting application servers, proxy servers, web application firewall and load-balancing systems, database servers, Oracle database, domain controllers, firewalls, network infrastructure, network security controls, and virtualization infrastructure. These components provide transaction-processing, database, authentication, traffic-management, connectivity, segmentation, or administrative functions for the CDE.

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

Docusign Envelope ID: 17D28E44-14A7-8913-810A-F4C5C263F6FB

Part 2. Executive Summary *(continued)*

Part 2c. Description of Payment Card Environment

Provide a high-level description of the environment covered by this Assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.* • *System components that could impact the security of account data.*	The assessed environment consists of the CDE located in North Shared Service data center locations. The following categories and system types are included in the assessment scope: **Network Infrastructure** • Firewalls • Network Security Controls • Internal and External Network Connections • Processor Connections • Connections to Third-party Services • Internal/External Network Boundaries • Demarcation Between CDE and Other Networks • Network Segmentation Technologies **Servers and Hosting** • Windows Servers • Linux Servers • Web Servers • Database Servers **Payment and Data Management** • In-Scope Payment Gateway • Encryption and Key Management Systems • Cardholder Data Flows and Storage • Security and Monitoring • Web Application Firewall (WAF) and Monitoring • Intrusion Detection Systems (IDS) • File Integrity Monitoring (FIM) • Logging and Monitoring Solutions • Vulnerability Management **Access and Authentication** • Remote Access • Multifactor Authentication (MFA) • Identity and Access Management (IAM) **Processes and Governance** • Development Processes • Change Management Processes • Policies and Procedures • Education and Training Programs

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

Docusign Envelope ID: 17D28E44-14A7-8913-810A-F4C5C263F6FB

	• Hiring Practices • Vendor Management • Incident Response Procedures This assessment covers all people, processes, and technologies that store, process, or transmit cardholder data, as well as those that could impact the security of the CDE.
Indicate whether the environment includes segmentation to reduce the scope of the Assessment. (Refer to the "Segmentation" section of PCI DSS for guidance on segmentation)	☒ Yes ☐ No

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

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

Facility Type	Total Number of Locations (How many locations of this type are in scope)	Location(s) of Facility (city, country)
Data Center	2	Grand Rapids, MI, USA Las Vegas, NV, USA

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

Docusign Envelope ID: 17D28E44-14A7-8913-810A-F4C5C263F6FB

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
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, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions), and Mobile Payments on COTS (MPoC) products.

♦ For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components appearing on the PCI SSC website (www.pcisecuritystandards.org)—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: 17D28E44-14A7-8913-810A-F4C5C263F6FB

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:
North Shared Services	Hosting, shared services
Banorte	Payment Processing
Cielo	Payment Processing
eMerchantPay Limited (UK)	Payment Processing
EPX	Payment Processing
Global Payments	Payment Processing
Payplug Enterprise SAS	Payment Processing
Paysafe	Payment Processing
PXP Solutions Limited	Payment Processing
Shift4 Limited	Payment Processing
Trust Payments (UK) Ltd	Payment Processing
Worldline Merchant Services UK Ltd	Payment Processing
Cybersource Corporation	Payment Processing
Fiserv Global Business Solutions	Payment Processing
Paynetics AD	Payment Processing
Planet Payment	Payment Processing
Creative Cloud AG	Payment Processing
TRANSACT PRO, SIA	Payment Processing
Cashflows	Payment Processing
Trust Pay a.s. (Finby)	Payment Processing
ACI Worldwide (Pay.On)	Payment Processing

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

Docusign Envelope ID: 17D28E44-14A7-8913-810A-F4C5C263F6FB

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

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

Docusign Envelope ID: 17D28E44-14A7-8913-810A-F4C5C263F6FB

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: InovioPay Payment Processing

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:	☐	☒	☐	☐	☐
Appendix A3:	☐	☒	☐	☐	☐

Justification for Approach

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

Docusign Envelope ID: 17D28E44-14A7-8913-810A-F4C5C263F6FB

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	1.2.6 - Inovio did not have insecure ports, protocols, or services in use. 1.5.1 - No device is connected directly to both an untrusted network and the CDE. 2.3.1, 2.3.2, 4.2.1.2 - There are no wireless environments connected to the CDE or transmitting account data. 3.3.2 - Inovio does not store SAD prior to authorization. 3.3.3 - Inovio is not an issuer and does not support issuing services. 3.4.1, 3.4.2 - No personnel exist with a legitimate business need to view full PAN. 3.5.1.2, 3.5.1.3 - Inovio does not use disk-level or partition-level encryption to render PAN unreadable. 3.7.9 - Inovio does not share cryptographic keys with its customers. 4.2.2 - PAN is not sent over end-user technologies. 5.2.3, 5.2.3.1 - All in-scope system components have Crowdstrike deployed, regardless of malware risk. 6.4.1, 8.3.10, 10.7.1 - This requirement has been superseded. 6.5.2, 11.3.1.3, 11.3.2.1 - Inovio did not undergo significant changes in the past 12 months. 8.2.3 - Inovio has no access to customer premises or systems. 8.2.7 - There are no third parties with access into Inovio's environment. 8.3.10.1 - Customer user access is not provisioned to the in-scope systems. 8.6.1, 8.6.2 - Inovio does that have system or application accounts that can be used for interactive login. 9.4.1.1, 9.4.1.2 - Inovio does not maintain any offline media with cardholder data. 9.4.3, 9.4.4 - Inovio does not move media with cardholder data outside its facilities. 9.4.6 - Inovio does not maintain any hard-copy materials with cardholder data. 9.5.1, 9.5.1.1, 9.5.1.2, 9.5.1.2.1, 9.5.1.3, A2.1.1, A2.1.2, A2.1.3 - Inovio does not use or maintain POI devices in any capacity. 11.2.2 - Inovio does not have authorized wireless access points that are in scope. 11.4.7, A1.1.1, A1.1.2, A1.1.3, A1.1.4, A1.2.1, A1.2.2, A1.2.3 - Inovio is not a multi-tenant service provider. 12.3.2 - Inovio did not use the customized approach to meet any PCI DSS 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: 17D28E44-14A7-8913-810A-F4C5C263F6FB

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.*	2026-06-16
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	2026-09-22
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: 17D28E44-14A7-8913-810A-F4C5C263F6FB

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 2026-09-23).*

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 *(Inovio Payments, LLC)* 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 *(Inovio Payments, LLC)* has not demonstrated compliance with PCI DSS requirements. **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 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 *(Inovio Payments, LLC)* 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: 17D28E44-14A7-8913-810A-F4C5C263F6FB

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

Signed by:
Scott Richardson
88A06AF5D51B4E8...

Signature of Service Provider Executive Officer ↑	Date: 9/24/2026
Service Provider Executive Officer Name: Scott Richardson	Title: Head of Information Compliance and Assurance

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:

DocuSigned by:
Matt Goodman
86E5094442BA437...

Signature of Lead QSA ↑	Date: 9/24/2026
Lead QSA Name: Matt Goodman	

DocuSigned by:
Brandon Breslin
331E3EF0F6EF46A...

Signature of Duly Authorized Officer of QSA Company ↑	Date: 9/24/2026
Duly Authorized Officer Name: Brandon Breslin	Wipfli Advisory LLC

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: David Armah and Joshua Wingate, ISAs, assisted Inovio personnel with

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

Docusign Envelope ID: 17D28E44-14A7-8913-810A-F4C5C263F6FB

	procuring and gathering appropriate evidence, and performed reviews to provide additional context for provided documentation.

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

Docusign Envelope ID: 17D28E44-14A7-8913-810A-F4C5C263F6FB

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.