Docusign Envelope ID: 37918DD6-8936-4724-BB8B-BBABEA98E5CF

Payment Card Industry
Data Security Standard

PaynoPain

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0.1

Publication Date: August 2024

Docusign Envelope ID: 37918DD6-8936-4724-BB8B-BBABEA98E5CF

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

Entity Name: PAYNOPAIN SOLUTIONS, S.L.

Date of Report as noted in the Report on Compliance: 5 Jun 2025

Date Assessment Ended: 5 Jun 2025

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

Docusign Envelope ID: 37918DD6-8936-4724-BB8B-BBABEA98E5CF

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:	PAYNOPAIN SOLUTIONS S.L.
DBA (doing business as):	PAYNOPAIN
Company mailing address:	Paseo de la universidad 23, Pta. 5 bajo, Castellón de la Plana
Company main website:	https://paynopain.com
Company contact name:	Jordi Nebot Carda
Company contact title:	CEO
Contact phone number:	+34 622 63 62 07
Contact e-mail address:	jordi@paynopain.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):	N/A
Qualified Security Assessor	
Company name:	A2Secure Technologias Informatica, Sociedad Ltd.
Company mailing address:	Avda. Francesc Cambó 21, 10. Barcelona.
Company website:	www.a2secure.com
Lead Assessor name:	Guillem Cuesta
Assessor phone number:	+34 933 945 600
Assessor e-mail address:	guillem.cuesta@a2secure.com
Assessor certificate number:	205-308

© 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:	• **Paylands**: Payment method or solutions. • **PCI Proxy:** To replace the PAN with tokens for the hospitality industry

Type of service(s) 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): Card Tokenization		

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:	All PaynoPain services not specifically listed above

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:	

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.	PAYNOPAIN is a Spanish company (Level 1 Payment Service Provider) that provides a payment gateway to multiple clients in different countries. The company offers services to merchants, allowing automated solutions in payment methods as described in Part 2a. Scope Verification. During card-not-present transactions, the company processes payment data from customers on e-commerce websites and forwards it to other payment

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

Docusign Envelope ID: 37918DD6-8936-4724-BB8B-BBABEA98E5CF

	gateways, acquirers, or issuers for payment authorization. As a payment gateway, PAYNOPAIN uses strong cryptography to securely store and tokenize cardholder data internally, supporting recurring or repeat transactions for one or multiple acquirers. The company ensures that cardholder data is stored only for as long as necessary and retention periods are constantly monitored. PAYNOPAIN exclusively transmits cardholder data to secure acquirers for mandatory operations. Finally, the payment platform consists of different services developed and maintained by the company.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	PAYNOPAIN is classified as a payment gateway that provides multiple payment solutions, as well as cardholder data processing, to their online business customers. As a result of the above activities, PAYNOPAIN collects and processes the cardholder data (CHD) to internally tokenize the details, supporting recurring transactions or repeat transactions for multiple acquirers. It is important to mention that sensitive authentication data (SAD) elements (CVC2, CVV, CVV2) are never retained after authorization.
Describe system components that could impact the security of account data.	PAYNOPAIN's PCI environment consists of web and application servers, databases, applications, and security systems that provide security services (e.g., SIEM, FIM, etc.). These components are located within a Cloud Platform (AWS).

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

Docusign Envelope ID: 37918DD6-8936-4724-BB8B-BBABEA98E5CF

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.*	PAYNOPAIN's PCI environment consists of web and application servers, databases, applications, and security systems that provide security services (e.g., SIEM, FIM, etc.). These components are located within a Cloud Platform (AWS). On the Cloud Platform, the company utilizes Virtual Private Cloud (VPC) to create different networks, subnets, ACLs, and network security groups. This infrastructure enables the implementation of segmentation techniques to isolate the cardholder data environment (CDE) from non-business-related systems and functions. Both incoming and outgoing connections within PAYNOPAIN's environment are always set up as HTTPS, secured with TLS 1.2. The Primary Account Number (PAN) is encrypted using strong cryptography (AES-256) with the associated key-management AWS service (KMS). All services listed in the scope of this assessment, including Internet/eCommerce and Payment Gateway/Switch, were evaluated for the storage, processing, or transmission of cardholder data (CHD) and sensitive authentication data (SAD). The locations and flow of data were identified through: • Reviewing the services' architecture and implementation • Conducting interviews with service owners, developers, and administrators • Examining policies, procedures, and services documentation • Validating data locations and cardholder data flows with the key stakeholders at PAYNOPAIN.
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

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

Docusign Envelope ID: 37918DD6-8936-4724-BB8B-BBABEA98E5CF

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)
Example: Data centers	*3*	*Boston, MA, USA*
Corporate Office	1	Castellón de la Plana, Spain
AWS Data Centers	multiple	-

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

Docusign Envelope ID: 37918DD6-8936-4724-BB8B-BBABEA98E5CF

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
N/A	N/A	N/A	N/A	N/A

* 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.

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

Docusign Envelope ID: 37918DD6-8936-4724-BB8B-BBABEA98E5CF

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:
Redsys Servicios de Procesamiento S.L	Payment Gateway Switch - Transaction processing
Amazon Web Services (AWS)	Cloud Virtual Private hosting provider
Pay By Call	Receives merchant's phone communication reference to process card payments
Clearhaus A/S	Acquirer bank – maintains communication with service and banking entity for transaction processing
PAYTPV (Paycomet)	Authorized Payment Institution providing payment services
Shift4 Limited (Credorax Bank)	Authorized and regulated credit institution for authorization, settlement, and compensation services

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: Refer to Part 2a. Scope Verification.

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: 37918DD6-8936-4724-BB8B-BBABEA98E5CF

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	• 1.2.6, 2.2.5: No unsafe protocols identified. • 1.3.3: Paynopain does not process or transmit cardholder data over wireless networks. • 2.3.1, 2.3.2, 11.2.1, 11.2.2, 11.3.1: There are no wireless networks in the PCI-DSS environment. • 3.3.3.b: Paynopain does not support issuing services. • 3.5.1.c: Hashed versions of the same PAN are not present in the environment. • 3.5.1.2, 3.5.1.3.a: Disk encryption is not used. • 3.7.6: There are no manual clear-text cryptographic key- management operations in use. • 3.7.9: Paynopain does not share cryptographic keys with customers. • 4.2.1.2: Paynopain does not process or transmit cardholder data over wireless networks. • 4.2.2: End-user technologies are not used to transmit cardholder data. • 5.2.1.a, 5.2.2, 5.2.3.a, 5.2.3.b, 5.3.1, 5.3.2, 5.3.2.1, 5.3.4, 5.3.5: Paynopain has no systems commonly affected by malware. • 8.2.3, 8.2.7: Paynopain does not have third parties with access to PCI environment. Although the provider of Hosting (Amazon) can have access to the information of the machines subject to PCI; In no case will a user, keys or certificates be provided to access them. • 8.2.5.b: There are no physical authentication methods present on PAYNOPAIN's CDE. • 8.3.9, 8.3.10.1: This control does not apply because the client has three combined authentication methods for EC2: RSA, Password of the RSA and Google Authenticator temporary code. On the other hand, AWS additionally has an MFA. Since these methods are used together, and no single authentication factor is used at any point in the access process, the scenario described by this control does not apply. • 8.3.11: PaynoPain does not use physical tokens to access its platform. • 8.6.1, 8.6.2, 8.6.3: Paynopain does not allow interactive login. The only system that connects in auto is Orch, which launches a series of scripts in local (it is not an IAM user and does not log in anywhere). On the other hand, the administration of Crowdstrike agents is done from a console located in a central panel that is accessed from each administrator's own account.

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

Docusign Envelope ID: 37918DD6-8936-4724-BB8B-BBABEA98E5CF

	• 9.4.1, 9.4.1.1, 9.4.1.2, 9.4.2, 9.4.3, 9.4.4, 9.4.5, 9.4.5.1, 9.4.6, 9.4.7: There are no physical media (computers, removable electronic media, paper receipts, paper reports, faxes, etc.) in the PayNoPain PCI-DSS environment. • 9.5.1, 9.5.1.1, 9.5.1.2, 9.5.1.2.1, 9.5.1.3: Paynopain does not use POI devices. • 10.4.2.1: All the logs of the PaynoPain environment are reviewed following control 10.4.1 on a regular basis, there is no other system components that are reviewed with different frequency. • 11.3.1.3: No significant change in the environment. • 11.4.7: Paynopain cannot be considered a multi-tenant providers. • 12.3.2: The entity does not use the customized approach to satisfy controls. • 12.5.3.b: No significant changes this year.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	-

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

Docusign Envelope ID: 37918DD6-8936-4724-BB8B-BBABEA98E5CF

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.*	13 Mar 2025
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	5 Jun 2025
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: 37918DD6-8936-4724-BB8B-BBABEA98E5CF

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 5 Jun 2025)*
Indicate below whether a full or partial PCI DSS assessment was completed:

☒ **Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.

☐ **Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the ROC noted above, each signatory identified in any of Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document *(select one)*:

☒	**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 ***PAYNOPAIN SOLUTIONS, S.L.*** 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: 37918DD6-8936-4724-BB8B-BBABEA98E5CF

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:
Jordi Nebot Carda
DF4CA03B09634BA...

Signature of Service Provider Executive Officer ↑	Date: 5 Jun 2025
Service Provider Executive Officer Name: Jordi Nebot Carda	Title: CEO

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:

CUESTA BASSEDA GUILLEM - 47870246R
Digitally signed by CUESTA BASSEDA GUILLEM - 47870246R
Date: 2025.06.05 10:51:22 +02'00'

Signature of Lead QSA ↑	Date: 5 Jun 2025
Lead QSA Name: **Guillem Cuesta** (QSA Certificate Number: 205-308)	

A2SECURE

Signature of Duly Authorized Officer of QSA Company ↑	Date: 5 Jun 2025
Duly Authorized Officer Name: **Albert Morell** (QSA Certificate Number: 203-790)	QSA Company: **A2Secure Technologias informatica, Sociedad Ltd.**

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

Docusign Envelope ID: 37918DD6-8936-4724-BB8B-BBABEA98E5CF

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: 37918DD6-8936-4724-BB8B-BBABEA98E5CF

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.