



Payment Card Industry Data Security Standard



Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0.1

Publication Date: August 2024



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 2026

Date Assessment Ended: 5 Jun 2026



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, CP: 12006 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 Tecnologías Informática, Sociedad Ltd.
Company mailing address:	Avda. Francesc Cambó 21, 10. Barcelona.
Company website:	www.a2secure.com
Lead Assessor name:	Miquel Casasayas
Assessor phone number:	(+34) 933 945 603
Assessor e-mail address:	miquel.casasayas@a2secure.com
Assessor certificate number:	QSA (Certificate Number: 206-455)



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:

- 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): 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.



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: <input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web-hosting services <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Multi-Tenant Service Provider <input type="checkbox"/> Other Hosting (specify):	Managed Services: <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	Payment Processing: <input type="checkbox"/> POI / card present <input type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Network Provider		
<input type="checkbox"/> Others (specify):		
Provide a brief explanation why any checked services were not included in the Assessment:		All PaynoPain services not specifically listed above have been excluded as they are not within the present PCI DSS scope.

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 SOLUTIONS S.L. is a Spanish company, classified as a Level 1 Payment Service Provider, that provides a payment gateway to multiple clients in different countries. The company provides services for merchants to allow automated payment solutions, mainly for card-not-present transactions, such as e-commerce payments.
---	--



	<p>During card-not-present transactions, the company processes payment data coming from customers' e-commerce website services and transmits it to other payment gateways, acquirers or issuers for payment authorization.</p> <p>As a payment gateway, PAYNOPAIN SOLUTIONS S.L. uses and stores cardholder data to tokenize payment details internally, supporting recurring transactions or repeat transactions for one or multiple acquirers. Cardholder data is stored securely using strong cryptography. In addition, the information is stored only for as long as required, and retention periods are continuously monitored.</p> <p>PAYNOPAIN SOLUTIONS S.L. exclusively transmits cardholder data to secure acquirers for mandatory payment operations.</p> <p>In addition to the card-not-present e-commerce channel, PAYNOPAIN SOLUTIONS S.L. also supports a card-present payment flow related to POS/TPV transactions. This card-present channel is commercially contracted and managed through PAYNOPAIN FINANCIAL SERVICE S.L.; however, PAYNOPAIN SOLUTIONS S.L. is responsible for the technical processing, transmission and storage of the transaction data associated with these in-person payments.</p> <p>For card-present transactions, the payment data is captured through POS/TPV terminals provided and operated through PAYNOPAIN FINANCIAL SERVICE S.L. PAYNOPAIN SOLUTIONS S.L. processes and transmits the transaction information required for authorization and settlement purposes, however, it does not operate or manage the POS/TPV terminals, does not have access to the terminals' cryptographic keys, and is not responsible for the operational management, maintenance or cryptographic configuration of the terminals.</p> <p>PAYNOPAIN SOLUTIONS S.L. does not store cardholder data from these card-present transactions.</p> <p>Finally, the payment platform consists of different services developed and maintained by PAYNOPAIN SOLUTIONS S.L.</p>
<p>Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.</p>	<p>PAYNOPAIN is classified as a payment gateway that provides multiple payment solutions, as well as cardholder data processing, to their online business customers.</p>



	<p>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.</p> <p>It is important to mention that sensitive authentication data (SAD) elements (CVC2, CVV, CVV2) are never retained after authorization.</p>
<p>Describe system components that could impact the security of account data.</p>	<p>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).</p>



Part 2. Executive Summary (continued)

Part 2c. Description of Payment Card Environment

Provide a high-level description of the environment covered by this Assessment.

For example:

- *Connections into and out of the cardholder data environment (CDE).*
- *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.*
- *System components that could impact the security of account data.*

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



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

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

Facility Type	Total Number of Locations (How many locations of this type are in scope)	Location(s) of Facility (city, country)
<i>Example: Data centers</i>	3	<i>Boston, MA, USA</i>
Corporate Office	1	Castellón de la Plana, Spain
AWS Data Centers	multiple	-



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.



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:

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

If Yes:

Name of Service Provider:	Description of Services Provided:
Amazon Web Services (AWS)	Cloud Virtual Private hosting provider
Redsys Servicios de Procesamiento S.L	Payment Gateway Switch - Transaction processing
Pay By Call	Receives merchant’s phone communication reference to process card payments
Shift4 Limited (Credorax Bank)	Authorized and regulated credit institution for authorization, settlement, and compensation services
Clearhaus A/S	Acquirer bank - maintains communication with service and banking entity for transaction processing
PAYTPV (Paycomet)	Authorized Payment Institution providing payment services
EcoPaynet	Provider of the TPV/POI
MONET+, a.s.	Used to support the Card-Present channel

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



Part 2. Executive Summary (continued)

Part 2g. Summary of Assessment (ROC Section 1.8.1)

Indicate below all responses provided within each principal PCI DSS requirement.

For all requirements identified as either “Not Applicable” or “Not Tested,” complete the “Justification for Approach” table below.

Note: One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.

Name of Service Assessed: Paylands and PCI Proxy

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:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 2:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 3:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 6:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 9:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 10:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Requirement 12:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A1:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Justification for Approach



For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.

1.2.6, 2.2.5: No insecure services, protocols, or ports were identified in the environment, which means there were no elements requiring security features to mitigate risk. Therefore, this specific requirement does not apply to the assessed environment.

1.3.3: Paynospain does not process or transmit cardholder data through wireless networks. Therefore, the requirement for implementing Network Security Controls (NSCs) between all wireless networks and the Cardholder Data Environment (CDE) does not apply to the assessed environment.

2.3.1, 2.3.2: There are no wireless networks present in the PCI-DSS environment, thus the requirement for changing or confirming the security of wireless vendor defaults does not apply. No wireless devices or configurations were found that would necessitate the implementation of these security measures.

3.3.3: Paynospain does not support issuing services.

3.5.1.2, 3.5.1.3: Disk encryption is not used in the assessed environment, thus the requirement does not apply. No configurations or processes related to disk-level or partition-level encryption were found or reviewed.

3.7.6: There are no manual cleartext cryptographic key-management operations in use, meaning that the requirement for implementing split knowledge and dual control does not apply to the assessed environment. No relevant policies, logs, or configurations were reviewed as there were no such operations to evaluate.

3.7.9: Paynospain does not share cryptographic keys with its customers, thus the requirement does not apply to its environment. No documentation or procedures were reviewed as there was no shared key arrangement to assess.

4.2.1.2: The organization does not process or transmit any cardholder data over wireless networks, thus this specific requirement does not apply to their environment. No wireless networks transmitting PAN or connected to the Cardholder Data Environment (CDE) exist within the organization's infrastructure.

4.2.2: End-user technologies are not used to transmit cardholder data, thus there is no requirement to secure PAN with strong cryptography when it is sent via such technologies. No relevant policies, configurations, or logs were reviewed since there was no use case involving end-user messaging for cardholder data transmission.

5.2.2, 5.3.1, 5.3.2, 5.3.2.1, 5.3.4, 5.3.5: PaynoPain has not deployed systems commonly affected by

malware, meaning that the requirement for an anti-malware solution does not apply to their environment.

8.2.3: PaynoPain does not have remote access to any customer's cardholder data environment (CDE).

8.3.9: The environment utilizes multiple authentication methods, including Multi-Factor Authentication (MFA) via RSA, password, and Google Authenticator, which eliminates the need for passwords/passphrases as the only authentication factor. No single-factor authentication relying solely on passwords/passphrases exists in the setup.

8.3.10: The environment utilizes multiple authentication methods for EC2 access, including RSA, password for RSA, and Google Authenticator time-based one-time password (TOTP), which eliminates the need for the additional requirement focused solely on password/passphrase management. No single-factor authentication relying exclusively on passwords/passphrases is in place.

8.3.11: The organization's systems are entirely hosted on AWS, which does not involve the use of physical authentication factors such as security tokens, smart cards, or certificates. Therefore, the requirement does not apply to their environment as there are no physical authentication factors in use.

8.6.1, 8.6.2, 8.6.3: PaynoPain does not permit the use of system or application accounts for interactive login within the PCI environment. The only interactions with production fronts are performed by the "Orch" orchestration machine, which automatically connects and runs a series of local scripts without initiating any IAM user account, nor can it log in or start a session anywhere. Additionally, CrowdStrike Falcon with Real Time Response is used to execute predetermined commands on managed hosts, and no other services requiring interactive sessions have been added to the PCI environment.

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 PCI DSS environment of PayNoPain, meaning that the requirement for securing offline media backups with cardholder data does not apply to this environment.

10.4.2.1: There are no other system components outside of those covered by Requirement 10.4.1 that require periodic log reviews in the PaynoPain deployed environment. All logs are reviewed following the specified control, and no additional components exist that would necessitate a different review frequency.



	<p>11.3.1.3, 11.3.2.1: No significant changes have occurred in the environment, which means that internal vulnerability scans following such changes were not necessary. Therefore, the requirement to perform internal vulnerability scans after any significant change does not apply to this environment.</p> <p>12.3.2: The entity does not utilize the customized approach to meet any PCI DSS requirements, meaning that the targeted risk analysis documentation and senior management approval processes specified in this requirement are not relevant to their compliance approach. No specific tools, logs, or configurations were reviewed as they are not applicable to the entity's current compliance strategy.</p>
<p>For any Not Tested responses, identify which sub-requirements were not tested and the reason.</p>	<p>-</p>



Section 2 Report on Compliance

(ROC Sections 1.2 and 1.3)

Date Assessment began: Note: <i>This is the first date that evidence was gathered, or observations were made.</i>	7 Apr 2026
Date Assessment ended: Note: <i>This is the last date that evidence was gathered, or observations were made.</i>	5 Jun 2026
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any testing activities performed remotely?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No



Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated (*Date of Report as noted in the ROC 5 Jun 2026*)

Indicate below whether a full or partial PCI DSS assessment was completed:

- Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.
- Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

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

<input checked="" type="checkbox"/>	<p>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.</p>								
<input type="checkbox"/>	<p>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 (<i>Service Provider Company Name</i>) has not demonstrated compliance with PCI DSS requirements.</p> <p>Target Date for Compliance: YYYY-MM-DD</p> <p>An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.</p>								
<input type="checkbox"/>	<p>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 (<i>Service Provider Company Name</i>) has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction.</p> <p>This option requires additional review from the entity to which this AOC will be submitted.</p> <p><i>If selected, complete the following:</i></p> <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <thead> <tr style="background-color: #f2f2f2;"> <th style="width: 35%;">Affected Requirement</th> <th>Details of how legal constraint prevents requirement from being met</th> </tr> </thead> <tbody> <tr><td style="height: 20px;"> </td><td> </td></tr> <tr><td style="height: 20px;"> </td><td> </td></tr> <tr><td style="height: 20px;"> </td><td> </td></tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement from being met						
Affected Requirement	Details of how legal constraint prevents requirement from being met								



Part 3. PCI DSS Validation (continued)

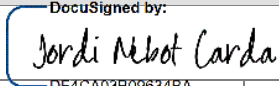
Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:







(Select all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to <i>PCI DSS</i> , Version 4.0.1 and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
<input checked="" type="checkbox"/>	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

DocuSigned by: <i>Jordi Nebot Carda</i>	
Signature of Service Provider Executive Officer 	Date: 5 Jun 2026
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:	<input checked="" type="checkbox"/> QSA performed testing procedures.
	<input type="checkbox"/> QSA provided other assistance. If selected, describe all role(s) performed:
	 Avda. Francisco Cambó 21, 10 ^a 08003 Barcelona T: 93 294 56 00 F: 93 294 56 01
Signature of Lead QSA 	Date: 5 Jun 2026
Lead QSA Name: Miquel Casayas (QSA Certificate Number: 206-455)	
	 Avda. Francisco Cambó 21, 10 ^a 08003 Barcelona T: 93 294 56 00 F: 93 294 56 01
Signature of Duly Authorized Officer of QSA Company 	Date: 5 Jun 2026
Duly Authorized Officer Name: Albert Morell (QSA Certificate Number: 203-790)	QSA Company: A2Secure Tecnologias Informática, Sociedad Ltd.

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

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



Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has Non-Compliant results noted in Section 3.

If asked to complete this section, select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement below. For any “No” responses, include the date the entity expects to be compliant with the requirement and provide a brief description of the actions being taken to meet the requirement.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If “NO” selected for any Requirement)
		YES	NO	
1	Install and maintain network security controls	<input type="checkbox"/>	<input type="checkbox"/>	
2	Apply secure configurations to all system components	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored account data	<input type="checkbox"/>	<input type="checkbox"/>	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems and networks from malicious software	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and software	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to system components and cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identify users and authenticate access to system components	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
10	Log and monitor all access to system components and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Test security systems and networks regularly	<input type="checkbox"/>	<input type="checkbox"/>	
12	Support information security with organizational policies and programs	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	<input type="checkbox"/>	<input type="checkbox"/>	

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/