Payment Card Industry
Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0.1

Revision 2

Publication Date: August 2024

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

Entity Name: Optomany Ltd

Assessment End Date: 2025-26-08

Date of Report as noted in the Report on Compliance: 2025-01-09

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:	Optomany Ltd
DBA (doing business as):	Optomany
Company mailing address:	10, Lower Grosvenor Place London Westminster SW1W 0EN
Company main website:	www.optomany.com
Company contact name:	Abiodun Ajibola
Company contact title:	Information Security Manager, DNA Payments
Contact phone number:	+44 208 102 8000
Contact e-mail address:	Abiodun.Ajibola@dnapaymentsgroup.com
Part 1b. Assessor (ROC Section 1.1)	
Provide the following information for all assessors involved in the Assessment. If there was no assessor for a given assessor type, enter Not Applicable	
PCI SSC Internal Security Assessor(s)	
ISA name(s):	Not Applicable
Qualified Security Assessor	
Company name:	Foregenix Ltd
Company mailing address:	1 Watts Barn Badbury Swindon Wiltshire SN4 0EU

	United Kingdom
Company website:	https://www.foregenix.com
Lead Assessor name:	Sabina Sovane
Assessor phone number:	+44 845 309 6232
Assessor e-mail address:	ssovane@foregenix.com
Assessor certificate number:	QSA (201-065)

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:	Optomany Axept platform and payment gateway services including: EFT Authorization, Tokenization, PayerAuth, Settlement, Gateway. Optomany Reporting and Management Services: Optomany Control Centre (OCC)	
Type of service(s) assessed:		
Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☒ POS / 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): 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:	Not Applicable

Type of service(s) not assessed:

Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POS / 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		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Shared Hosting 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 Section 2.1)	
Describe how the business stores, processes, and/or transmits account data.	Optomany Ltd (hereafter referred to as Optomany) has applications that underpin the transaction processing on behalf of merchants. The applications hosted are defined below. EFT Authorization: Optomany supports P2PE validated services and as part of this service, POI terminals (mainly different models of PAX) pass the encrypted transaction data over TLS v1.2 to the EFT authorization application. This encrypted data is passed to the authentication application to validate the data source and data format. If validated, the encrypted data is passed to the internal authorization application to perform the business logic, decrypt and send to acquirers for authorization. This application only handles encrypted cardholder data.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Gateway: Optomany provides fully integrated payment processing services. The gateway application is used to support the transaction processing. It receives the encrypted data over TLS v1.2. This encrypted CHD is sent to the authentication application to validate the data source and data format. If validated, the encrypted data is passed to a lookup service to validate the card details. If validated, it will encrypt the data and send it for further processing via an authorization service. Settlement: Settlement files are generated with encrypted dataand sent to the acquirer for processing. Tokenization: Optomany generates tokens for each transaction PAN that is received. Transmission: Optomany transmits cardholder data over TLS v1.2 to acquirers for the purpose of transaction authorization. Storage: Optomany stores cardholder data encrypted for settlement and tokenization purposes.
Describe system components that could impact the security of account data.	Network Components included: Domain Controllers - Authentication sources used by system in the AOC. NTP- Domain Time tool for Time Distribution Log Aggregation- To collect and analyze log data System components include: Anti-virus Services – To protect the systems from Malware File Integrity Monitoring Servers – To identify any changes in the state of the system. Access Control – User management. Multi-Factor Authentication – To provide additional security mechanism for user authentication. Monitoring - Monitoring of all systems for performance and threat analysis.

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.*	This assessment included the review of critical systems and network devices within the CDE. Verification of scope included reviewing the firewalls at the perimeter and webs servers hosted within the DMZ. Web servers receive payment transaction data. Network traffic is managed by both the firewall and load balancers. Internal zones within the CDE include applications, tokenization services and databases that enable the payment transaction services between merchants and acquirers. Services reviewed included authorizations, settlements, tokenization, and transaction reporting. Connections into the CDE are over secure protocol and files are transferred outside to acquirers via secure file transfer mechanism. User connectivity to the CDE requires a VPN connection with two-factor authentication. Review of the management network included: • Domain controllers – Authentication sources used by systems in the CDE. • Log Aggregators – To collect and analyze log data. • Anti-Virus Servers – To protect the systems from Malware. • File Integrity Monitoring Servers – To identify any changes in the state of the system. • NTP - Domain Time II tool for time distribution. • Access Control – User access management. • Multi-Factor Authentication - To provide additional security mechanism for user authentication. Monitoring – Monitoring of all systems for performance and threat analysis
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)
Example: Data centers	*3*	*Boston, MA, USA*
Pulsant Data Centre	1	UK, Edinburg
Custodian Data Centre	1	UK, Maidstone
Corporate offices	1	UK, London

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
axept	3.1	P2PE	2022-01044.014	2025-23-05

* 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:	
• 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:
Custodian Data Centres	Co-location service provider
Microsoft Azure	Cloud hosting provider
Pulsant Data Centres	Co-location service provider
TNS	Network provider

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: Optomany Axept platform and payment gateway services including: EFT Authorization, Tokenization, PayerAuth, Settlement, Gateway. Optomany Reporting and Management Services: Optomany Control Centre (OCC)

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If Below Method(s) Was Used	
	In Place	Not Applicable	Not Tested	Not in Place	Customized Approach	Compensating Controls
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

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	2.3.1 -2.3.2 Not Applicable. There are no wireless networks connected to Optomany's CDE. 3.3.3 - Not Applicable. Optomany is not an issuer. 3.5.1.1 - Not Applicable. Not using hashes to render PAN unreadable.. 3.7.9 - Not Applicable. Cryptographic keys are never shared. 4.2.1.2 - 4.2.2 Not Applicable. PAN is never sent over wireless networks. 5.3.3 - Not Applicable. No removable electronic media is in scope. 6.4.1 - Not Applicable. This requirement has been superseded by requirement 6.4.2 - 6.4.3 Not Applicable. No public-facing web applications are in scope. 6.5.2 - Not Applicable. No significant change reported. 8.2.3 - Not Applicable. Optomany does not have remote access to customer premises. 8.2.7 - Not Applicable. Optomany does not permit any third parties to have remote access to their environment. 8.3.10 - Not Applicable. This requirement has been superseded by requirement 8.3.10.1 - Not Applicable. There are no non-consumer customer users accounts in the scope for this assessment. 8.6.1 - 8.6.2 - Not Applicable. No accounts used by systems or applications can be used for interactive logins. 9.4.1 -9.4.1.2, 9.4.2 -9.4.5, 9.4.5.1 - Not Applicable. Optomany does not use removable media or send media outside of the CDE. 9.5.1.1 - 9.5.1.3 - Not Applicable. Optomany does not have POI devices within the scope of this assessment. 10.7.1 - Not Applicable. This requirement has been superseded by requirement 10.7.2. 11.2.2 - Not Applicable. The Optomany team does not have any wireless network in-scope. 11.3.1.3 - Not Applicable. No significant changes have occurred since the last vulnerability scan. 11.3.2.1 - Not Applicable. No significant changes have occurred since the last vulnerability scan.

	11.4.7 - Not Applicable. Optomany is not a multi-tenant service provider. 11.6.1 - Not Applicable. There are no public-facing web applications in scope in the Optomany environment. 12.3.2 - Not Applicable. Thefounder are no requirements using the customized approach to achieve compliance. 12.5.3 - Not Applicable. No significant changehas occurred in the last year. A1.1.1 - A1.1.4 - Not Applicable. Optomany is not a multi-tenant service provider. A1.2.1 - A1.2.3 - Not Applicable. Optomany is not a multi-tenant service provider. A2.1.1 - A2.1.3 - Not Applicable. No SSL/Early TLS is in use by Optomany.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	Not Applicable

Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3.2**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*	2025-19-02
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	2025-26-08
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

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* 2025-01-09*)*.

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 1) In Place, 2) In Place with Remediation, or 3) Not Applicable, resulting in an overall **COMPLIANT** rating; thereby Optomany Ltd 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 Optomany Ltd has not demonstrated compliance with PCI DSS requirements. **Target Date** for Compliance: 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 1) In Place, 2) In Place with Remediation, or 3) Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby Optomany Ltd 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

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

Abiodun Ajibola

Signature of Service Provider Executive Officer ↗	Date: 01/09/2025
Service Provider Executive Officer Name: Abiodun Ajibola	Title: Information Security Manager, DNA Payments

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:

Sabina Sovane

Signature of Lead QSA ↗	Date: 01/09/2025
Lead QSA Name: Sabina Sovane	

Ricardo dos Santos

Signature of Duly Authorized Officer of QSA Company ↗	Date: 01/09/2025
Duly Authorized Officer Name: Ricardo Dos Santos	QSA Company: Foregenix Ltd

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

If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:	☐ ISA(s) performed testing procedures.
	☐ ISA(s) provided other assistance. If selected, describe all role(s) performed:

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/