



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: Network Merchants Ltd

Assessment End Date: 2026-03-23

Date of Report as noted in the Report on Compliance: 2026-04-15

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:	Network Merchants Ltd
DBA (doing business as):	Not Applicable
Company mailing address:	Programme, All Saints Street Bristol United Kingdom BS1 2LZ
Company main website:	https://nmi.com
Company contact name:	David Sage
Company contact title:	VP, SITE RELIABILITY ENGINEERING
Contact phone number:	+44 (0) 117 930 4455
Contact e-mail address:	david.sage@nmi.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

Company website:	https://www.foregenix.com
Lead Assessor name:	Sterling Thomas
Assessor phone number:	+44 845 309 6232
Assessor e-mail address:	stthomas@foregenix.com
Assessor certificate number:	QSA(202-396) and PFI Core (1200-084)

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:	NMI Cardease	
Type of service(s) 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 <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Shared Hosting Provider <input type="checkbox"/> Other Hosting (specify):	Managed Services (specify): <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 checked="" type="checkbox"/> POS / card present <input checked="" type="checkbox"/> Internet / e-commerce <input checked="" 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 checked="" 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 checked="" 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):		

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:

- 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):

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.

Card data is currently processed within the NMI environment using the following applications:

CardeaseIP:

CardeaseIP enables customers to connect to Network Merchants using XML Encrypted data over TLS v1.2 (RSA 2048 bit). The product supports both card present and card not present transactions.

CardeaseXML/ChipDNA Direct:

CardeaseXML/ChipDNA Direct is the next generation of Network Merchant’s payment protocol based on the Cardease V2 platform architecture. Requests and responses are structured using XML and encrypted with TLS v1.2 (RSA 2048 bit).

eKashu:

This is the e-commerce payment processing service which operates over TLS v1.2 and authorizes card-not-present transactions.

A70:

The A70 application provides authorization and settlement services for Cardease. Depending upon the payment channel (card present or card not present), transactions are received by the respective application via the Load Balancer (as described above) for validation. If the transaction source is legitimate and validated, transactions are forwarded to the XML server which runs the business logic. Account data from transactions is encrypted using AES256 Data Encryption Key that is rotated daily. All sensitive authentication data received is processed in VRAM only and Network Merchants does not store sensitive authentication data after authorization.

P2PE:

Network Merchants also offers a validated Point to Point Encryption (P2PE) solution called ‘Network Merchants P2PE Solution’ (solution number 2024-01028.005) to the merchants. Data is encrypted in POI devices using DUKPT 3DES and AES128. Encrypted data from POI devices is received at [REDACTED] which sanitizes and validates the data. If the transaction is legitimate, encrypted data is sent to XML server. For decryption of cardholder data, encrypted data is received at the Crypto Server and it makes an API call to FutureX EXcrypt HSMs. Clear text account data is sent back to the Crypto server from the HSMs. The Crypto server sends this data back to the XML server which sends it to the A70 server. From A70 servers, data is sent to acquirers/processors for authorization. Network Merchants uses an IPsec VPN

	<p>or TLS v1.2 to transmit cardholder data depending upon the acquirer's supported channels. The environment assessed in this report includes the P2PE decryption environment.</p> <p>WebMIS: Network Merchants provides its customers with a reporting portal called WebMIS where business customers can login and check their account. Terminal Management System (TMS) and a virtual terminal are also part of this portal but only for authorized customers. Customers can use Network Merchants reporting system called WebMIS which allows customers to report on transactions, settle transactions and perform refunds.</p> <p>NMI stores cardholder data (PAN and expiry date) in [REDACTED] using AES256. Data Encryption Keys are stored encrypted with an RSA 16384-bit Key Encrypting Keys. Production data is backed up digitally to a secure cloud service. Historical data is stored in an offsite facility on tape, encrypted using an additional layer of RSA 2048-bit encryption. NMI stores historical Salted SHA256 Hashes of PANs in a database which is being transitioned to HMAC SHA512 Hashes. NMI also stores truncated PAN (first 6 and last 4 digits) in the databases.</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>Not Applicable</p> <p>All cardholder data functions are performed during narrated payment channels as described above.</p>
<p>Describe system components that could impact the security of account data.</p>	<ul style="list-style-type: none"> • Firewalls • Load balancers. • Encryption • Authentication • Databases • Management tools • FIM • IDS/IPS • Virtualization • Switches • Antimalware • Bespoke Applications.

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 NMI environment is segmented between the corporate and cardholder data processing environments. NMI uses dedicated and third-party managed data center facilities to host its CDE. The data center environments are firewalled and contain multiple dedicated network zones used to host application and management servers.

Third-Party Relationships:
Yes. Reference AOC Part 2f.

CDE Segmentation:
Segmentation is managed by stateful inspection firewalls. NMI has implemented its network segmentation by separating its system components into dedicated VLANs based on designated function.

Transmission:
NMI receives, processes, and transmits cardholder data to provide gateway services for their customers for purposes of transaction authorization functions.

Processes:
NMI receives, processes, and transmits cardholder data to provide gateway services for their customers for purposes of authorization functions.

Storage:
NMI receives, processes, and transmits cardholder data to provide gateway services for their customers for purposes of authorization functions. Cardholder data is stored for facilitating recurring transactions, reconciling payment disputes and generating reports.

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	Bristol, United Kindgom
Data center	1	[REDACTED]
Data center	1	[REDACTED]
Data center	1	[REDACTED]
Data center	1	[REDACTED]

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.

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 type="checkbox"/> Yes <input checked="" type="checkbox"/> No |

If Yes:

Name of Service Provider:	Description of Services Provided:
The Logic Group t/a Barclaycard	Transaction processing/upstream service provider
Paymentech, LLC. (Chase)	Transaction processing/upstream service provider
CredoRax Bank Limited	Transaction processing/upstream service provider
Elavon, Inc.	Transaction processing/upstream service provider
US Bank/Elavon Merchant Processing System	Transaction processing/upstream service provider
EVERY Card Services AB	Transaction processing/upstream service provider
Evy Card Services AS	Transaction processing/upstream service provider
First Data GmbH	Transaction processing/upstream service provider
First Data Resources Ltd	Transaction processing/upstream service provider
Global Payments Europe s.r.o.	Transaction processing/upstream service provider
Heartland Payment Systems LLC, a division of Global Payments Direct Inc.	Transaction processing/upstream service provider
MONERIS SOLUTIONS	Transaction processing/upstream service provider
Moneris Solutions Corporation	Transaction processing/upstream service provider
ACI Worldwide Corp and Affiliates (ACI ReD1 Gateway (Ecommerce, iFrame, Tokenization, Web Services, XML and Assist), ACI ReDi Business Intelligence, ACI ReDShield, ACI ReDShield RTR) (Retail Decisions)	Transaction processing/upstream service provider
TSYS - GA	Transaction processing/upstream service provider
TSYS Acquiring Solutions	Transaction processing/upstream service provider

TSYS International Core	Transaction processing/upstream service provider
TSYS International Prime	Transaction processing/upstream service provider
TSYS Issuing Processing	Transaction processing/upstream service provider
TSYS Managed Services - Issuing	Transaction processing/upstream service provider
TSYS Managed Services EMEA Limited	Transaction processing/upstream service provider
TSYS Merchant Solutions	Transaction processing/upstream service provider
TSYS Output Services	Transaction processing/upstream service provider
Vantiv Acquiring Systems	Transaction processing/upstream service provider
Vantiv Issuing and Switch-Providing Systems	Transaction processing/upstream service provider
Vantiv Prepaid Systems	Transaction processing/upstream service provider
WorldPay (UK) Limited	Transaction processing/upstream service provider
Worldpay from FIS eCommerce	Transaction processing/upstream service provider
Worldpay from FIS Mercury Integrated Payments	Transaction processing/upstream service provider
Worldpay, Inc.	Transaction processing/upstream service provider
Worldpay, LLC	Transaction processing/upstream service provider
[REDACTED]	Colocation datacenter for the UK
[REDACTED]	Colocation datacenter for the US
[REDACTED]	Colocation datacenter for the EU
Logz.io	Cloud-based log housing

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: NMI Cardease

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:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input 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"/>	<input type="checkbox"/>
Requirement 3:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input 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"/>	<input type="checkbox"/>
Requirement 5:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 6:	<input checked="" type="checkbox"/>	<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"/>	<input type="checkbox"/>
Requirement 8:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input 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"/>	<input type="checkbox"/>
Requirement 10:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input 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 type="checkbox"/>	<input type="checkbox"/>
Requirement 12:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A1:	<input type="checkbox"/>	<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"/>	<input type="checkbox"/>

Justification for Approach

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

- 1.2.6 - Not Applicable - Foregenix confirmed that only approved protocols were identified in the configured network rules.
- 2.2.5 - Not Applicable - Foregenix confirmed that no insecure services or protocols are approved in the CDE.
- 2.3.1 - Not Applicable - No wireless AP are used within the CDE. This was verified through review of the network diagrams and asset listings.
- 2.3.2 - Not Applicable - No wireless AP are used within the CDE. This was verified through review of the network diagrams and asset listings.
- 3.3.2 - Not Applicable - Foregenix observed that there was no evidence of SAD stored prior to or after authorization.
- 3.3.3 - Not Applicable - NMI is not an issuer nor supports issuing services.
- 3.4.2 - Not Applicable - Full PAN is never stored within the NMI environment.
- 3.5.1.2 - Not Applicable - No disk-level or partition-level encryption is used to protect CHD stored at-rest.
- 3.5.1.3 - Not Applicable - No disk-level or partition-level encryption is used to protect CHD stored at-rest.
- 3.7.9 - Not Applicable - Foregenix confirmed that NMI do not share encryption keys with clients.
- 4.2.1.2 - Not Applicable - Foregenix confirmed via interview of personnel and review of network diagrams that CHD is never transmitted over wireless networks.
- 4.2.2 - Not Applicable - Foregenix confirmed that PAN is never distributed over end-user messaging.
- 5.2.3 - Not Applicable - Foregenix confirmed that all in-scope systems are currently monitored by antimalware software.
- 5.2.3.1 - Not Applicable - Foregenix confirmed that all in-scope systems are currently monitored by antimalware software.
- 5.3.3 - Not Applicable - Foregenix verified that OMNI does not use removable media for storage of CHD.
- 6.4.1 - Not Applicable - This requirement is superseded by requirement 6.4.2.
- 8.2.3 - Not Applicable - Foregenix verified through reviewing documentation and interviewing key personnel that NMI does not have access to customers' premises.
- 8.2.7 - Not Applicable - While interviewing security personnel, it was identified that there are no third parties with access to the CDE.
- 8.3.10 - Not Applicable - This requirement is superseded by requirement 8.3.10.1.
- 8.6.1 - Not Applicable - Foregenix confirmed that, by design, application and system accounts are specifically and deliberately never enabled for interactive logins.
- 8.6.2 - Not Applicable - Foregenix confirmed that, by design, application and system accounts are specifically and deliberately never enabled for interactive logins.
- 9.4.1 - Not Applicable - NMI does not have hard-copy materials containing cardholder data.
- 9.4.1.1 - Not Applicable - NMI does not have hard-copy materials containing cardholder data.

9.4.1.2 - Not Applicable - NMI does not have hard-copy materials containing cardholder data.

9.4.2 - Not Applicable - NMI does not have hard-copy materials containing cardholder data.

9.4.3 - Not Applicable - NMI does not have hard-copy materials containing cardholder data.

9.4.4 - Not Applicable - NMI does not have hard-copy materials containing cardholder data.

9.4.5 - Not Applicable - NMI does not have hard-copy materials containing cardholder data.

9.4.5.1 - Not Applicable - NMI does not have hard-copy materials containing cardholder data.

9.4.6 - Not Applicable - NMI does not have hard-copy materials containing cardholder data.

9.4.7 - Not Applicable - NMI does not have hard-copy materials containing cardholder data.

9.5.1 - Not Applicable - Foregenix confirmed that no terminals are in scope for this assessment.

9.5.1.1 - Not Applicable - Foregenix confirmed that no terminals are in scope for this assessment.

9.5.1.2 - Not Applicable - Foregenix confirmed that no terminals are in scope for this assessment.

9.5.1.2.1 - Not Applicable - Foregenix confirmed that no terminals are in scope for this assessment.

9.5.1.3 - Not Applicable - Foregenix confirmed that no terminals are in scope for this assessment.

10.7.1 - Not Applicable - This requirement is superseded by requirement 10.7.2.

11.3.1.3 - Not Applicable - While interviewing security personnel, it was identified that the internal and external scans are run frequently and scheduled with the reports being reviewed. The scans are unattended and therefore, based on the change management process, do not require a change to be logged for vulnerability scans

11.3.2.1 - Not Applicable - While interviewing security personnel, it was identified that the internal and external scans are run frequently and scheduled with the reports being reviewed. The scans are unattended and therefore, based on the change management process, do not require a change to be logged for vulnerability scans.

11.4.4 - Not Applicable - Foregenix reviewed the penetration testing reports and there were no findings that needed correction and would require a re-test to be conducted.

11.4.7 - Not Applicable - Foregenix confirmed that NMI is not a multi-tenant service provider.

A1.1.1 - Not Applicable - Foregenix confirmed that NMI is not a multitenant hosting provider.

A1.1.2 - Not Applicable - Foregenix confirmed that NMI is not a multitenant hosting provider.

A1.1.3 - Not Applicable - Foregenix confirmed that NMI is not a multitenant hosting provider.

A1.1.4 - Not Applicable - Foregenix confirmed that NMI is not a multitenant hosting provider.

A1.2.1 - Not Applicable - Foregenix confirmed that NMI is not a multitenant hosting provider.

	<p>A1.2.2 - Not Applicable - Foregenix confirmed that NMI is not a multitenant hosting provider.</p> <p>A1.2.3 - Not Applicable - Foregenix confirmed that NMI is not a multitenant hosting provider.</p> <p>A2.1.1 - Not Applicable - Foregenix confirmed that NMI are not utilizing SSL or early TLS.</p> <p>A2.1.2 - Not Applicable - Foregenix confirmed that NMI are not utilizing SSL or early TLS.</p> <p>A2.1.3 - Not Applicable - Foregenix confirmed that NMI are not utilizing SSL or early TLS.</p>
<p>For any Not Tested responses, identify which sub-requirements were not tested and the reason.</p>	<p>Not Applicable</p>

Section 2 Report on Compliance

(ROC Sections 1.2 and 1.3.2)

Date Assessment began: Note: <i>This is the first date that evidence was gathered, or observations were made.</i>	2026-02-02
Date Assessment ended: Note: <i>This is the last date that evidence was gathered, or observations were made.</i>	2026-03-23
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 2026-04-15).

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 1) In Place, 2) In Place with Remediation, or 3) Not Applicable, resulting in an overall COMPLIANT rating; thereby Network Merchants Ltd 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 Network Merchants Ltd has not demonstrated compliance with PCI DSS requirements.</p> <p>Target Date for Compliance:</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 1) In Place, 2) In Place with Remediation, or 3) Not Applicable, resulting in an overall COMPLIANT BUT WITH LEGAL EXCEPTION rating; thereby Network Merchants 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.</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%;"> <thead> <tr> <th style="text-align: center;">Affected Requirement</th> <th style="text-align: center;">Details of how legal constraint prevents requirement from being met</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">Not Applicable</td> <td style="text-align: center;">Not Applicable</td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement from being met	Not Applicable	Not Applicable
Affected Requirement	Details of how legal constraint prevents requirement from being met				
Not Applicable	Not Applicable				

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



Signature of Service Provider Executive Officer ↑

Date: 04/16/2026

Service Provider Executive Officer Name: David Sage

Title: VP, Site Reliability Engineering

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: Not Applicable



Signature of Lead QSA ↑

Date: 04/16/2026

Lead QSA Name: Sterling Thomas



Signature of Duly Authorized Officer of QSA Company ↑

Date: 04/16/2026

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: Not Applicable

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/