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: 2025-03-28

Date of Report as noted in the Report on Compliance: 2025-04-15

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 BS1 2LZ United Kingdom
Company main website:	https://www.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

	United Kingdom
Company website:	https://www.foregenix.com
Lead Assessor name:	Shawn Shifflett
Assessor phone number:	+44 845 309 6232
Assessor e-mail address:	sshifflett@foregenix.com
Assessor certificate number:	QSA (203-919), QPA (1300-143), 3DS Assessor (1100-232), Secure Software (1500-070), Secure SLC (1600-156), P2PE Assessor (400-152), P2PE Application Assessor (500-078)

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:	NML Cardease

Type of service(s) 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):

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.	Card data is currently processed within the Network Merchants Ltd (hereafter referred to as NML) 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 an XML server which runs the business logic. Account data from transactions is encrypted using an 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 [REDACTED]. Encrypted data from POI devices is received at F5 Load Balancer which sanitizes and validates the data. If the transaction is legitimate, encrypted data is sent to an XML server. For decryption of cardholder data, encrypted data is received at the Crypto Server, and it makes an API call to FutureX 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 use an IPsec VPN 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. 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. NML stores cardholder data (PAN, expiry date) in [REDACTED] using AES 256-bit encryption. Data Encryption Keys are stored encrypted with an RSA 16384-bit Key Encrypting Key. NML also stores salted hashed values of PAN in [REDACTED] server using SHA-1. The hashes are salted with a secret salt value, these salts are stored on the XML servers instead of the database servers. Database administrators do not have access to the salt values. Additionally, as the hash is salted it can't be used in a brute force attack on the PAN from knowledge of the first 6 and last 4 digits of the PAN. NML also stores truncated PAN (first 6 and last 4 digits) in the [REDACTED].
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Not applicable. All cardholder data functions are performed during narrated payment channels as described above.
Describe system components that could impact the security of account data.	* 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 NML environment is segmented between the corporate and cardholder data processing environments. NML 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. NML has implemented its network segmentation by separating its system components into dedicated VLANs based on designated function. Transmission: NML receives, processes, and transmits cardholder data to provide gateway services for their customers for purposes of transaction authorization functions. Processes: NML receives, processes, and transmits cardholder data to provide gateway services for their customers for purposes of authorization functions. Storage: NML 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)
Example: Data centers	*3*	*Boston, MA, USA*
Corporate office	1	Bristol, UK
Data center	1	[REDACTED]
Data center	1	[REDACTED]
Data center	1	[REDACTED]
Data center	1	[REDACTED]
Offsite tape recovery and storage	1	Surrey, UK

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:	
• 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:
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
EVRY Card Services AB	Transaction processing / upstream service provider
Evry 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]	Payment Gateway
[REDACTED]	Colocation datacenter for UK and the US
[REDACTED]	Colocation Services for US
[REDACTED]	Colocation Services for EU
logz.io	Cloud-based log hosting

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: NML 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:	☒	☒	☐	☐	☐	☐
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.	1.2.6 - Not applicable. Foregenix reviewed the approved network protocols and cross-referenced them with the configured network rules. They confirmed that only approved protocols were identified in the configured network rules. 2.2.5 - Not applicable. Foregenix confirmed that no insecure service or protocols are approved in the CDE via review of DOC-1, review of system evidence, and review of firewall rulesets. 2.3.1 - Not applicable. No wireless APs are used within the CDE. This was verified through review of the network diagrams and asset listings. 2.3.2 - Not applicable. No wireless APs are used within the CDE. This was verified through review of the network diagrams and asset listings. 3.3.2 - Not applicable. Foregenix conducted a thorough examination of a sample of audit and transaction logs and the repositories where cardholder data is stored. Foregenix reported that there was no evidence of SAD stored prior or after the authorization. Per INT-1's statement, SAD is only handled by application volatile memory. 3.3.3 - Not applicable. NML is not an issuer nor supports issuing services. 3.4.2 - Not applicable. Full PAN is never stored within the NML 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 NML 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 anti-malware software. 5.2.3.1 - Not applicable. Foregenix confirmed that all in-scope systems are currently monitored by anti-malware software. 5.3.3 - Not applicable Foregenix verified that NML does not use removable media for storage of CHD. 6.4.1 - Not applicable. This requirement is superseded by requirement 6.4.2. 6.5.2 - Not applicable. Foregenix conducted comparisons between last year's system components inventory and the current one and noted no significant changes in the software versions. 8.2.3 - Not applicable. Foregenix verified through interview with the Security Manager and through review of DOC-1, that NML do not have any access to customers' premises. 8.2.7 - Not applicable. The local credentials and all credentials on the Active Directory systems were reviewed and confirmed that there were no third-party accounts listed. While interviewing the 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. 9.4.1.2 - Not applicable. Foregenix reviewed DOC-1, reviewed network diagrams, and reviewed the asset inventory and confirmed NML does not have hard-copy materials containing cardholder data. 9.4.2 - Not applicable. Foregenix reviewed DOC-1, reviewed network diagrams, and reviewed the asset inventory and confirmed NML does not have hard-copy materials containing cardholder data. 9.4.3 - Not applicable. Foregenix reviewed DOC-1, reviewed network diagrams, and reviewed the asset inventory and confirmed NML does not have hard-copy materials containing cardholder data. 9.4.4 - Not applicable. Foregenix reviewed DOC-1, reviewed network diagrams, and reviewed the asset inventory and confirmed NML does not have hard-copy materials containing cardholder data. 9.4.5 - Not applicable. Foregenix reviewed DOC-1, reviewed network diagrams, and reviewed the asset inventory and confirmed NML does not have hard-copy materials containing cardholder data. 9.4.5.1 - Not applicable. Foregenix reviewed DOC-1, reviewed network diagrams, and reviewed the asset inventory and confirmed NML does not have hard-copy materials containing cardholder data. 9.4.6 - Not applicable. Foregenix reviewed DOC-1, reviewed network diagrams, and reviewed the asset inventory and confirmed NML does not have hard-copy materials containing cardholder data. 9.4.7 - Not applicable. Foregenix reviewed DOC-1, reviewed network diagrams, and reviewed the asset inventory and confirmed NML 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. 10.4.2.1 - Not applicable. Foregenix confirmed that specific to the NML in-scope environment all in-scope devices are exporting logs for ingestion to a SIEM solution. 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. Change controls are logged for all changes and remediation required based on the review of the vulnerability scan reports. There were no significant changes to CDE identified within the last 12 months. 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. Change controls are logged for all changes and remediation required based on the review of the vulnerability scan reports. There were no significant changes to CDE identified within the last 12 months. 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 NML is not a multi-tenant service provider. A1.1.1 - Not applicable. Foregenix confirmed that NML is not a multi-tenant hosting provider. A1.1.2 - Not applicable. Foregenix confirmed that NML is not a multi-tenant hosting provider. A1.1.3 - Not applicable. Foregenix confirmed that NML is not a multi-tenant hosting provider. A1.1.4 - Not applicable. Foregenix confirmed that NML is not a multi-tenant hosting provider. A1.2.1 - Not applicable. Foregenix confirmed that NML is not a multi-tenant hosting provider. A1.2.2 - Not applicable. Foregenix confirmed that NML is not a multi-tenant hosting provider. A1.2.3 - Not applicable. Foregenix confirmed that NML is not a multi-tenant hosting provider. A2.1.1 - Not applicable. Foregenix confirmed that NML are not utilizing SSL or early TLS. A2.1.2 - Not applicable. Foregenix confirmed that NML are not utilizing SSL or early TLS. A2.1.3 - Not applicable. Foregenix confirmed that NML are not utilizing SSL or early TLS.
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.*	2025-02-03
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	2025-03-28
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* 2025-04-15.

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):*

☒ **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.

☐ **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.

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 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.

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
Not applicable.	Not applicable.

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

Signature of Service Provider Executive Officer ↗	Date: 2025-04-15
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: Foregenix performed the PCI DSS assessment and completed the report on compliance.

Signature of Lead QSA ↗	Date: 2025-04-15
Lead QSA Name: Shawn Shifflett	

Signature of Duly Authorized Officer of QSA Company ↗	Date: 2025-04-15
Duly Authorized Officer Name: Dan Farr	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	☐	☐	
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/