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, LLC

**Assessment End Date:** 2025-02-14

**Date of Report as noted in the Report on Compliance:** 2025-02-14


*© 2006 - 20224 PCI Security Standards Council, LLC. All rights reserved.*

# 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, LLC |
| DBA (doing business as): | OMNI |
| Company mailing address: | 1450 American Lane, Suite 1200<br>Schaumburg<br>IL<br>60173 |
| Company main website: | https://nmi.com |
| Company contact name: | Jules Meyer |
| Company contact title: | Director of Platform Architecture |
| Contact phone number: | +44 7900 495 399 |
| Contact e-mail address: | jules.meyer@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<br>Badbury<br>Swindon<br>Wiltshire<br>SN4 0EU |


*© 2006 - 20224 PCI Security Standards Council, LLC. All rights reserved.*

| | |
|---|---|
| | United Kingdom |
| Company website: | https://www.foregenix.com |
| Lead Assessor name: | Greg Marler |
| Assessor phone number: | +44 845 309 6232 |
| Assessor e-mail address: | gmarler@foregenix.com |
| Assessor certificate number: | QSA(206-172) |

## 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: | Network Merchants, LLC. OMNI |

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): | | |


*© 2006 - 20224 PCI Security Standards Council, LLC. All rights reserved.*

***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 |


*© 2006 - 20224 PCI Security Standards Council, LLC. All rights reserved.*

| Part 2b. Description of Role with Payment Cards (ROC Section 2.1) | |
|---|---|
| Describe how the business stores, processes, and/or transmits account data. | Cardholder data (PAN, cardholder name, expiration date, card verification code, full track data) is received from merchants over public Internet via TLS v1.2 for processing. Transactions are then subsequently transmitted to the upstream processors over IPSEC VPN or TLS v1.2 connections. Communication to upstream processors is dependent solely on the direction of the processors and is out of scope of this assessment. Card-present transactions capture CHD (PAN, cardholder name, expiration date, card verification code, full track data) via dip/swipe at brick-and-mortar merchant locations and are transmitted to NMI's public internet-facing web application suite via TLS v1.2. Card not-present channels transactions capture CHD (PAN, cardholder name, card verification code, and expiration date). Encrypted (AES 256-bit) CHD (PAN, cardholder name, expiration date) and truncated PAN (first six (6) / last four (4) digits) are stored in [redacted] databases with a retention period of thirty-six (36) months. |
| Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data. | Transmission:<br>NMI transmits CHD via public Internet encapsulate using TLS v1.2 to upstream processors for transaction processing.<br><br>Processes:<br>NMI processes CHD (PAN, cardholder name, expiration date, card verification code, full track data) as they function as a payment gateway.<br><br>Storage:<br>Encrypted (AES 256-bit) CHD (PAN, cardholder name, expiration date) and truncated (first six (6) / last four (4) digits) PAN are stored for reporting and recurring transaction processing with a retention period of thirty-six (36) months. |
| Describe system components that could impact the security of account data. | Based on the dataflow reviewed by Foregenix, these are the only system components that could affect account data security:<br>Payment applications, data repositories (such as file system and database), servers hosted in a data center. Account data is handled in all forms on these system components, such as transmitted, processed, and stored, including in the clear-text and encrypted format. |


*© 2006 - 20224 PCI Security Standards Council, LLC. All rights reserved.*

## Part 2. Executive Summary *(continued)*

### Part 2c. Description of Payment Card Environment

| | |
|---|---|
| Provide a high-level description of the environment covered by this Assessment.<br>*For example:*<br>• *Connections into and out of the cardholder data environment (CDE).*<br>• *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.*<br>• *System components that could impact the security of account data.* | Network Merchants, Inc. (NMI) provides an electronic payment gateway for transaction processing and is considered a Level 1 Service Provider.<br>NMI provides merchant services including an online portal, API integration and batch processing. NMI also offers affiliates the ability to market NMI's merchant services to other businesses.<br>CDE Segmentation:<br>Segmentation is managed by [redacted] stateful inspection firewalls. NMI has implemented its network segmentation by separating its system components into dedicated layer 3 VLANs based on designated device function. Logical access between differing network security zones is controlled by [redacted] firewalls and [redacted] switches.<br>Transmission:<br>NMI transmits CHD via public Internet encapsulate using TLS v1.2 to upstream processors for transaction processing.<br>Processes:<br>NMI processes CHD (PAN, cardholder name, expiration date, card verification code, full track data) as they function as a payment gateway.<br>Storage:<br>Encrypted (AES 256-bit) CHD (PAN, cardholder name, expiration date) and truncated first six (6) / last four (4) digits) PAN are stored for reporting and recurring transaction processing with a retention period of thirty-six (36) months. |
| Indicate whether the environment includes segmentation to reduce the scope of the Assessment.<br>(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* |


*© 2006 - 20224 PCI Security Standards Council, LLC. All rights reserved.*

| | | |
|---|---|---|
| Datacenter | 2 | [redacted] |
| Corporate Office | 1 | Bristol, UK |


*© 2006 - 20224 PCI Security Standards Council, LLC. All rights reserved.*

## 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.


*© 2006 - 20224 PCI Security Standards Council, LLC. All rights reserved.*

## 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: |
|---|---|
| [redacted] | Datacenter |
| [redacted] | Datacenter |
| Bambora Inc. | Transaction Processing |
| BlueSnap, Inc. | Transaction Processing |
| Cardworks Servicing, LLC. | Transaction Processing |
| Checkout Ltd | Transaction Processing |
| Chronopay LLC | Transaction Processing |
| Cielo S.A. | Transaction Processing |
| Credomatic | Transaction Processing |
| Credorax Bank Ltd | Transaction Processing |
| Elavon, Inc. | Transaction Processing |
| Electronic Payment Exchange | Transaction Processing |
| Evertec Group, LLC | Transaction Processing |
| EVO Payments, Inc. | Transaction Processing |
| First Data Buypass | Transaction Processing |
| First Data Corporation | Transaction Processing |
| Global Payments Direct, Inc. | Transaction Processing |
| Heartland Payment Systems, LLC. | Transaction Processing |
| Ingenico, Inc. | Transaction Processing |
| Integrapay Pty Ltd | Transaction Processing |


*© 2006 - 20224 PCI Security Standards Council, LLC. All rights reserved.*

| | |
|---|---|
| Intuit Inc. | Transaction Processing |
| IPpay LLC | Transaction Processing |
| Mercadotecnia Ideas Y Tecnologia | Transaction Processing |
| Merchant Partners | Transaction Processing |
| Moneris Solutions | Transaction Processing |
| National Merchants Association | Transaction Processing |
| NCR Payment Solutions, LLC | Transaction Processing |
| NMI | Transaction Processing |
| Nuvei Technologies | Transaction Processing |
| Pay360 by Capita | Transaction Processing |
| Payment World | Transaction Processing |
| Paymentech, LLC. (Subsidiary of Chase) | Transaction Processing |
| Paynamics Technologies, Inc. | Transaction Processing |
| PayPal, Inc. | Transaction Processing |
| Paysafe | Transaction Processing |
| Payvision B.V. | Transaction Processing |
| Plug & Pay Technologies, Inc. | Transaction Processing |
| Processing.com LLC. | Transaction Processing |
| Propay Inc. | Transaction Processing |
| RS2 Smart Processing | Transaction Processing |
| SIA Transact Pro | Transaction Processing |
| Skrill Limited | Transaction Processing |
| TSYS International | Transaction Processing |
| US Alliance Group, Inc. | Transaction Processing |
| Valitor UK ltd | Transaction Processing |
| Vantiv | Transaction Processing |
| Vesta Corporation | Transaction Processing |
| Wirecard Processing LLC | Transaction Processing |
| Worldpay, Inc. | Transaction Processing |


*© 2006 - 20224 PCI Security Standards Council, LLC. All rights reserved.*

## Part 2. Executive Summary *(continued)*

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

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

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

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

*Name of Service Assessed:* Network Merchants, LLC. OMNI

| PCI DSS Requirement | Requirement Finding<br>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**


*© 2006 - 20224 PCI Security Standards Council, LLC. All rights reserved.*

| | |
|---|---|
| For any Not Applicable responses, identify which sub-requirements were not applicable and the reason. | 1.2.6 - Not Applicable<br>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.<br>2.2.5 - Not Applicable.<br>No insecure service or protocols are approved in the CDE. This was verified by reviewing the OMNI PPS.<br>2.3.1 - Not Applicable.<br>No wireless AP are used within the CDE. This was verified through review of the network diagrams and asset listings.<br>2.3.2 - Not Applicable.<br>No wireless AP are used within the CDE. This was verified through review of the network diagrams and asset listings.<br>3.3.2 - Not Applicable<br>Foregenix conducted a thorough examination of a sample of audit and transaction logs and the repositories where cardholder data is stored. Foregenix reported that no evidence of SAD stored prior or after the authorization. Per INT-1's statement, SAD is only handled by application volatile memory.<br>3.3.3 - Not Applicable<br>OMNI is not an issuer.<br>3.4.2 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI Pay is actively working towards achieving compliance by this deadline.<br>3.5.1.1 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI Pay is actively working towards achieving compliance by this deadline.<br>3.5.1.2 - Not Applicable<br>Foregenix reviewed cardholder data flows and software inventory and found no disk-level or partition-level encryption to render PAN unreadable.<br>3.5.1.3 - Not Applicable<br>Foregenix reviewed cardholder data flows and software inventory and found no disk-level or partition-level encryption to render PAN unreadable.<br>3.7.9 - Not Applicable<br>OMNI do not share any encryption keys with clients.<br>4.2.1.1 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI is actively working towards achieving compliance by this deadline.<br>4.2.1.2 - Not applicable.<br>Foregenix confirmed via interview of personnel and review of network diagrams that CHD is never transmitted over wireless networks.<br>4.2.2 - Not Applicable<br>Foregenix verified that CHD is never sent via end-user messaging.<br>5.2.3 - Not Applicable |


*© 2006 - 20224 PCI Security Standards Council, LLC. All rights reserved.*

| | |
|---|---|
| | All in-scope systems are currently monitored by antimalware software.<br>5.2.3.1 - Not Applicable<br>All in-scope systems are currently monitored by antimalware software.<br>5.3.2.1 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI Pay is actively working towards achieving compliance by this deadline.<br>5.3.3 - Not Applicable<br>Foregenix verified that OMNI does use removable media for storage of CHD.<br>5.4.1 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI Pay is actively working towards achieving compliance by this deadline.<br>6.3.2 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI Pay is actively working towards achieving compliance by this deadline.<br>6.4.2 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI is actively working towards achieving compliance by this deadline.<br>6.4.3 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI is actively working towards achieving compliance by this deadline.<br>6.5.2 - Not Applicable<br>Foregenix conducted comparisons between last year's system components inventory and the current one and noted no significant changes in the software versions.<br>7.2.4 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI is actively working towards achieving compliance by this deadline.<br>7.2.5 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI is actively working towards achieving compliance by this deadline.<br>7.2.5.1 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI is actively working towards achieving compliance by this deadline.<br>8.2.3 - Not Applicable<br>Foregenix verified through interview with the Security Manager and through review of (DOC-1), it was verified that OMNI does not have any access to customers' premises.<br>8.2.7 - Not Applicable<br>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 |


*© 2006 - 20224 PCI Security Standards Council, LLC. All rights reserved.*

| | |
|---|---|
| | security personnel, it was identified that there are no third parties with access to the CDE.<br>8.3.6 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI Pay is actively working towards achieving compliance by this deadline.<br>8.3.10 - Not Applicable<br>Foregenix reviewed the user accounts in the Active Directory Domain Controller and reviewed all local users of Windows and Linux server samples to confirm OMNI does not support any non-consumer customer user IDs as part of the in-scope environment.<br>8.5.1 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI Pay is actively working towards achieving compliance by this deadline.<br>8.6.1 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI Pay is actively working towards achieving compliance by this deadline.<br>8.6.2 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI Pay is actively working towards achieving compliance by this deadline.<br>8.6.3 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI Pay is actively working towards achieving compliance by this deadline.<br>9.4.1.2 - Not Applicable<br>Foregenix reviewed (DOC-1), reviewed the network diagrams and the asset inventory and confirmed OMNI does not have hard-copy materials containing cardholder data.<br>9.4.2 - Not Applicable<br>Foregenix reviewed (DOC-1), reviewed the network diagrams and the asset inventory and confirmed OMNI does not have hard-copy materials containing cardholder data.<br>9.4.3 - Not Applicable<br>Foregenix reviewed (DOC-1), reviewed the network diagrams and the asset inventory and confirmed OMNI does not have hard-copy materials containing cardholder data.<br>9.4.4 - Not Applicable<br>Foregenix reviewed (DOC-1), reviewed the network diagrams and the asset inventory and confirmed OMNI does not have hard-copy materials containing cardholder data.9.4.5 - Not Applicable<br>Foregenix reviewed (DOC-1), reviewed the network diagrams and the asset inventory and confirmed OMNI does not have hard-copy materials containing cardholder data.9.4.5.1 - Not Applicable<br>Foregenix reviewed (DOC-1), reviewed the network diagrams and the asset inventory and confirmed OMNI does not have hard-copy materials containing cardholder data.9.4.6 - Not Applicable<br>Foregenix reviewed (DOC-1), reviewed the network diagrams and the asset inventory and confirmed OMNI does not have |


*© 2006 - 20224 PCI Security Standards Council, LLC. All rights reserved.*

| | |
|---|---|
| | hard-copy materials containing cardholder data.9.4.7 - Not Applicable<br>Foregenix reviewed (DOC-1), reviewed the network diagrams and the asset inventory and confirmed OMNI does not have hard-copy materials containing cardholder data.9.5.1 - Not Applicable<br>Foregenix verified through review of network diagrams and asset inventory reviews along with interviewing INT-1 that POI devices in the CDE.<br>9.5.1.1 - Not Applicable<br>Foregenix verified through review of network diagrams and asset inventory reviews along with interviewing INT-1 that POI devices in the CDE.<br>9.5.1.2 - Not Applicable<br>Foregenix verified through review of network diagrams and asset inventory reviews along with interviewing INT-1 that POI devices in the CDE.<br>9.5.1.2.1 - Not Applicable<br>Foregenix verified through review of network diagrams and asset inventory reviews along with interviewing INT-1 that POI devices in the CDE.<br>9.5.1.3 - Not Applicable<br>Foregenix verified through review of network diagrams and asset inventory reviews along with interviewing INT-1 that POI devices in the CDE.<br>10.4.1.1 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI is actively working towards achieving compliance by this deadline.<br>10.4.2.1 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI is actively working towards achieving compliance by this deadline.<br>10.7.2 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI is actively working towards achieving compliance by this deadline.<br>11.3.1.1 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI is actively working towards achieving compliance by this deadline.<br>11.3.1.2 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI is actively working towards achieving compliance by this deadline.<br>11.3.1.3 - Not Applicable<br>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. |


*© 2006 - 20224 PCI Security Standards Council, LLC. All rights reserved.*

| | |
|---|---|
| | 11.3.2.1 - Not Applicable<br>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.<br>11.4.4 - Not Applicable<br>Foregenix reviewed the penetration testing reports and there were no findings that needed correction and would require a re-test to be conducted.<br>11.4.7 - Not Applicable<br>OMNI is not a multi-tenant service provider.<br>11.5.1.1 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI is actively working towards achieving compliance by this deadline.<br>11.6.1 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI is actively working towards achieving compliance by this deadline.<br>12.3.1 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI is actively working towards achieving compliance by this deadline.<br>12.3.2 - Not Applicable<br>Foregenix validated all the requirements of this report and found no requirements using customized approach to achieve compliance.<br>12.3.3 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI is actively working towards achieving compliance by this deadline.<br>12.3.4 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI is actively working towards achieving compliance by this deadline.<br>12.5.2.1 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI is actively working towards achieving compliance by this deadline.<br>12.5.3 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI is actively working towards achieving compliance by this deadline.<br>12.6.2 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI is actively working towards achieving compliance by this deadline.<br>12.6.3.1 - Not Applicable |


*© 2006 - 20224 PCI Security Standards Council, LLC. All rights reserved.*

| | |
|---|---|
| | This requirement is considered a best practice until March 31, 2025. OMNI is actively working towards achieving compliance by this deadline.<br>12.6.3.2 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI is actively working towards achieving compliance by this deadline.<br>12.10.4.1 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI is actively working towards achieving compliance by this deadline.<br>12.10.7 - Not Applicable<br>This requirement is considered a best practice until March 31, 2025. OMNI is actively working towards achieving compliance by this deadline.<br>A1.1.1 - Not Applicable<br>OMNI is not a multi-tenant service provider.<br>A1.1.2 - Not Applicable<br>OMNI is not a multi-tenant service provider.<br>A1.1.3 - Not Applicable<br>OMNI is not a multi-tenant service provider.<br>A1.1.4 - Not Applicable<br>OMNI is not a multi-tenant service provider.<br>A1.2.1 - Not Applicable<br>OMNI is not a multi-tenant service provider.<br>A1.2.2 - Not Applicable<br>OMNI is not a multi-tenant service provider.<br>A1.2.3 - Not Applicable<br>OMNI is not a multi-tenant service provider.<br>A2.1.1 - Not Applicable<br>OMNI does not use POI devices or SSL and/or early TLS.<br>A2.1.2 - Not Applicable<br>OMNI does not use POI devices or SSL and/or early TLS.<br>A2.1.3 - Not Applicable<br>OMNI does not use POI devices or SSL and/or early TLS. |
| For any Not Tested responses, identify which sub-requirements were not tested and the reason. | Not Applicable |


*© 2006 - 20224 PCI Security Standards Council, LLC. All rights reserved.*

*© 2006 - 20224 PCI Security Standards Council, LLC. All rights reserved.*

# Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3.2**)

| | |
|---|---|
| Date Assessment began:<br>***Note:*** *This is the first date that evidence was gathered, or observations were made.* | 2024-11-04 |
| Date Assessment ended:<br>***Note:*** *This is the last date that evidence was gathered, or observations were made.* | 2025-02-14 |
| Were any requirements in the ROC unable to be met due to a legal constraint? | ☐ Yes ☒ No |
| Were any testing activities performed remotely? | ☒ Yes ☐ No |


*© 2006 - 20224 PCI Security Standards Council, LLC. All rights reserved.*

# 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* 2025-02-14*).*

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 / NMI (UK)** 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 / NMI (UK) 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 / NMI (UK) has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction.

This option requires additional review from the entity to which this AOC will be submitted.

*If selected, complete the following:*

| Affected Requirement | Details of how legal constraint prevents requirement from being met |
|---|---|
| | |


*© 2006 - 20224 PCI Security Standards Council, LLC. All rights reserved.*

| Part 3a. Service Provider Acknowledgement | |
|---|---|
| **Signatory(s) confirms:**<br>(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 | |
|---|---|
| Jules Meyer | |
| *Signature of Service Provider Executive Officer ↑* | Date: 2025-02-14 |
| Service Provider Executive Officer Name: Jules Meyer | Title: Director of Platform Architecure |

| 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.<br>If selected, describe all role(s) performed: The QSA reviewed the scope of the assessment, reviewed documentation, interviewed responsible personnel, and validated all applicable system component configurations and processes. |
| Greg Marler | |
| *Signature of Lead QSA ↑* | Date: 2025-02-14 |
| Lead QSA Name: Greg Marler | |
| Daniel Farr | |
| *Signature of Duly Authorized Officer of QSA Company ↑* | Date: 2025-02-14 |
| 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. |


*© 2006 - 20224 PCI Security Standards Council, LLC. All rights reserved.*

| | |
|---|---|
| | If selected, describe all role(s) performed: Not Applicable |


*© 2006 - 20224 PCI Security Standards Council, LLC. All rights reserved.*

## Part 4. Action Plan for Non-Compliant Requirements

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

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

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

*Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance accepting organization to ensure that this form is acceptable in their program. For more information about PCI SSC and our stakeholder community please visit: https://www.pcisecuritystandards.org/about_us/*


*© 2006 - 20224 PCI Security Standards Council, LLC. All rights reserved.*