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 OMNI

Assessment End Date: 2026-01-05

Date of Report as noted in the Report on Compliance: 2026-02-13

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 Schaumburg, IL 60173
Company main website:	https://nmi.com
Company contact name:	David Sage
Company contact title:	VP, SRE & Information Security
Contact phone number:	+44 7900 495 399
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:	Network Merchants, LLC. OMNI
Type of service(s) assessed:	

Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☒ POS / card present ☒ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (specify):
☐ Account Management	☐ Fraud and Chargeback	☒ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☐ Others (specify):		

***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.	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: NMI transmits CHD via public Internet encapsulate using TLS v1.2 to upstream processors for transaction processing. Processes: NMI processes CHD (PAN, cardholder name, expiration date, card verification code, full track data) as they function as a payment gateway. Storage: 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: Payment applications, data repositories (such as file system and database), servers hosted in a data centre. 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.

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.*	Network Merchants, Inc. (NMI) provides an electronic payment gateway for transaction processing and is considered a Level 1 Service Provider. 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. CDE Segmentation: 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. Transmission: NMI transmits CHD via public Internet encapsulate using TLS v1.2 to upstream processors for transaction processing. Processes: NMI processes CHD (PAN, cardholder name, expiration date, card verification code, full track data) as they function as a payment gateway. Storage: 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. (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 Centers	2	[REDACTED], US [REDACTED], US

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:**
[REDACTED]	Datacentre
[REDACTED]	Datacentre
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

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
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: Network Merchants, LLC. OMNI

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 – Only approved protocols are used. 2.2.5 - Not Applicable – No insecure protocols are used. 2.3.1 - Not Applicable – No wireless in the CDE. 2.3.2 - Not Applicable - No wireless in the CDE. 3.3.2 - Not Applicable – SAD only in volatile memory. 3.3.3 - Not Applicable – OMNI is not an issuer. 3.4.2 - Not Applicable - No PAN is available for view regardless of location. 3.5.1.2 - Not Applicable – FDE is not used. 3.5.1.3 - Not Applicable – FDE is not used. 3.7.9 - Not Applicable – No shared encryption keys. 4.2.1.2 – Not Applicable – No CHD is transmitted over wireless. 4.2.2 – Not Applicable – No CHD is transmitted via end-user messaging. 5.2.3.X – Not Applicable – All in-scope systems are protected by anti-malware. 5.3.3 – Not Applicable – CHD on removable media is prohibited. 6.4.1 – Not Applicable – Superseded requirement. 6.5.2 – Not Applicable – No significant changes. 8.2.3 – Not Applicable – No access to customer premises. 8.2.7 – Not Applicable – No 3rd-party CDE access. 8.3.10 – Not Applicable – No in-scope non-consumer IDs. 8.6.1 – Not Applicable – No system accounts are configured to support interactive logins. 8.6.2 – Not Applicable – No system accounts are configured to support interactive logins. 8.6.3 – Not Applicable – No system accounts are configured to support interactive logins. 9.4.1.2 – Not Applicable – No CHD within hard-copy materials. 9.4.[2-7] – Not Applicable – No CHD within hard-copy materials. 9.5.1 – Not Applicable – No in-scope POIs. 9.5.1.1 – Not Applicable – No in-scope POIs. 9.5.1.2 – Not Applicable – No in-scope POIs. 9.5.1.2.1 – Not Applicable – No in-scope POIs. 9.5.1.3 – Not Applicable – No in-scope POIs. 10.7.1 – Not Applicable – Superseded requirement. 11.3.1.3 – Not Applicable – No significant changes. 11.3.2.1 – Not Applicable – No significant changes. 11.4.4 – Not Applicable – No re-testing required. 11.4.7 – Not Applicable – Not a multi-tenant service provider. 12.3.2 – Not Applicable – No customized approach. A1.1.X – Not Applicable – Not a multi-tenant service provider. A1.2.X – Not Applicable – Not a multi-tenant service provider. A2.1.X – Not Applicable – No early SSL / 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.*	2025-11-17
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	2026-01-05
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* 2026-02-13*)*.

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, LLC OMNI 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
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	
David Sage	
Signature of Service Provider Executive Officer ↑	Date: 02/23/2026
Service Provider Executive Officer Name: David Sage	Title: VP, SRE & Information Security

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:
Signature of Lead QSA ↑	Date: 02/23/2026
Lead QSA Name: Shawn Shifflett	
Ricardo dos Santos	
Signature of Duly Authorized Officer of QSA Company ↑	Date: 02/23/2026
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	□	□	
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/