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 / NMI (UK)

Assessment End Date: 2025-02-03

Date of Report as noted in the Report on Compliance: 2025-03-04

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 / NMI (UK)
DBA (doing business as):	USAePay
Company mailing address:	1450 American Ln Ste 1200 Schaumburg, IL 60173 United States
Company main website:	https://nmi.com
Company contact name:	Jules Meyer
Company contact title:	Director of Platform Architecture
Contact phone number:	+1 847 352 4850
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 Badbury Swindon Wiltshire

	SN4 0EU United Kingdom
Company website:	https://www.foregenix.com
Lead Assessor name:	Kiska Satterfield
Assessor phone number:	+44 845 309 6232
Assessor e-mail address:	ksatterfield@foregenix.com
Assessor certificate number:	QSA (205-542)

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:	USAePay Payment Gateway

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.	Network Merchants Ltd / NMI (UK) (doing business as USAePay) is a Level 1 service provider and serves as an electronic payment gateway. Additionally, USAePay provides check verification services. USAePay transactions originate from merchants and consumers using the USAePay payments website or are passed to USAePay via an API integrated into the merchant e-commerce web sites (shopping cart, etc.), and merchant payment processors, including Bluefin P2PE, and FutureX VirtuCrypt. USAePay processes payments for Visa, Mastercard, American Express, Discover, Diners Club, Union Pay, and JCB via USAePay's website or an API integrated into merchant web sites. Cardholder data (CHD), including full track, card security codes, PAN, PIN block, cardholder name, and expiration date, as determined by USAePay's merchant customers' acceptance channels, enters via USAePay's FrontEnd application over a TLS v1.2 RSA 4096-bit connection. The FrontEnd forwards CHD to the BackEnd application, as follows: If transaction data contains full track the BackEnd extracts PAN, cardholder name, and expiration date, and stores it in its database. The database instance is contained within RAM and encrypted with RSA 2048-bit encryption. BackEnd simultaneously assembles an authorization message (PAN, name, expiry), which is transmitted to processors for authorization via TLS v1.2, (RSA 4096-bit) and direct connections over private point to- point or IPSEC (AES 256-bit) circuits. When the authorization message has been received PAN, cardholder name and expiration date are stored and/or updated in the database, which is protected with RSA 4096-bit encryption. Full track is then deleted by overwriting memory registers, while PAN, cardholder name and expiration date are overwritten and deleted from the BackEnd application. While the authorization message is compiled, BackEnd hashes and salts PAN (SHA-256), which is stored in Lockbox. While the authorization message is compiled, BackEnd hashes and salts PAN (SHA-256), which is stored in Lockbox and used in the internal transaction table to reference the card for recurring transactions. If the transaction data does not include full track the BackEnd assembles an authorization message containing PAN, cardholder name, expiration date and card security code and transmits the authorization message to its processors via TLS v1.2, RSA 4096-bit encrypted connections. Once the authorization message is created, BackEnd stores the PAN, cardholder name and expiration date in its database. The database instance is contained within RAM and encrypted with RSA 4096-bit encryption.

	When the authorization message has been received, hashed, and salted PAN, the first 6 and last 4 digits of PAN, cardholder name and expiration date are stored and/or updated in the database, which is protected with RSA 4096-bit encryption. Sensitive authentication data (card security codes) is then overwritten and deleted from BackEnd memory registers. While the authorization message is compiled, BackEnd hashes and salts PAN (SHA-256), which is stored in Lockbox and used in the internal transaction table to reference the card. If the transaction data contains PIN block the BackEnd extracts PAN, cardholder name, and expiration date from full track data, and stores it in the database. The database instance is contained within RAM and encrypted with RSA 4096-bit encryption. BackEnd simultaneously assembles an authorization message (PAN, name, expiry, PIN block), which is transmitted to processors via TLS v1.2, RSA 4096-bit encrypted connections for authorization. USAePay does not manage PIN/debit keys, but only transports (relays) PIN data to upstream payment processors. When the authorization message has been received full track and PIN block are deleted by overwriting BackEnd memory registers, hashed and salted PAN, first 6 and last 4 digits of PAN, cardholder name and expiration date are stored and/or updated in the database, which is protected with RSA 4096-bit encryption. While the authorization message is compiled, BackEnd hashes and salts PAN (SHA-256), which is stored in Lockbox. and used in the internal transaction table to reference the card.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Transmission: USAePay receives, processes, and transmits cardholder data to provide gateway services for their customers for purposes of authorization. Processes: USAePay receives, processes, and transmits cardholder data to provide gateway services for their customers for purposes of authorization. Storage: USAePay receives, processes, and transmits cardholder data to provide gateway services for their customers for purposes of authorization. Cardholder data is stored for facilitating recurring transactions, reconciling payment disputes, and generating reports.
Describe system components that could impact the security of account data.	☐ Firewalls ☐ Load balancers. ☐ Encryption ☐ Authentication ☐ Databases ☐ Management tools

	☐ FIM ☐ IDS/IPS ☐ Virtualization ☐ Switches ☐ Anti-virus ☐ 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 USAePay environment is segmented between the corporate and cardholder data processing environments. The corporate environment is located at USAePay's office is Lindon, Utah. USAePay 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. This allows USAePay to apply granular role-based access to its environment and only users with a need to know are granted permission to access the facility both physically and virtually. Technologies included within the assessment include: • Firewalls • Load balancers. • Encryption • Authentication • Databases • Management tools • FIM • IDS/IPS • Virtualization • Switches • Anti-virus • Bespoke Applications.

	Third-Party Relationships: Yes. Reference AOC Part 2f CDE Segmentation: Segmentation is managed by stateful inspection firewalls. USAePay has implemented its network segmentation by separating its system components into dedicated VLANs based on designated device function. Logical access between differing network security zones is controlled by firewalls, and switches. . Transmission: USAePay receives, processes, and transmits cardholder data to provide gateway services for their customers for purposes of authorization. Processes: USAePay receives, processes, and transmits cardholder data to provide gateway services for their customers for purposes of authorization. Storage: USAePay receives, processes, and transmits cardholder data to provide gateway services for their customers for purposes of authorization. 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	Lindon, UT, USA
Data Center	2	-

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
Bluefin P2PE	Bluefin P2PE	P2PE v3.1	2023-00897.035	2026-12-13
Bluefin TECS Engine P2PE	Bluefin TECS Engine P2PE	P2PE v3.1	2023-00897.034	2026-12-24

* 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:
Paymentech, LLC. (Chase)	Third party payment processing and authorization
Elavon, Inc.	Third party payment processing and authorization
Electronic Payment Exchange	Third party payment processing and authorization
Fiserv, Inc. - Electronic Payments	Third party payment processing and authorization
Global Payments Direct, Inc.	Third party payment processing and authorization
Heartland Payment Systems, LLC	Third party payment processing and authorization
Merchant eSolutions	Third party payment processing and authorization
Planet Payment	Third party payment processing and authorization
TSYS International	Third party payment processing and authorization
Worldpay, Inc.	Third party payment processing and authorization
VirtuCrypt LLC	PIN Services
F5 Networks	Managed Network and Application DDoS protection

Bluefin Payment Systems	P2PE Services
-	Colocation Data Center
-	Colocation Data Center
Logz.io	Elasticsearch API and Gateway API log management
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: USAePay Payment Gateway

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.	1.2.3 - Not applicable - Foregenix reviewed policies and procedures, examined network diagrams and observed business practices and found no wireless technologies in use within the environment. 1.2.6 - Not applicable - Foregenix reviewed the approved network protocols and found now insecure configurations listed. 1.3.3 - Not applicable - Foregenix reviewed policies and procedures, examined network diagrams and observed business practices and found no wireless technologies in use within the environment. 2.2.5 - Not applicable - Foregenix reviewed script outputs and configurations and found that no insecure services, protocols, or daemons are used within the environment. 2.3.1 - Not applicable - Foregenix reviewed policies and procedures, examined network diagrams and observed business practices and found no wireless technologies in use within the environment. 2.3.2 - Not applicable - Foregenix reviewed policies and procedures, examined network diagrams and observed business practices and found no wireless technologies in use within the environment. 3.3.2 - Not applicable - This requirement is a best practice until 31 Mar 2025. 3.3.3 - Not applicable - USAePay is not an issuer, nor do they support issuing services. 3.4.2 - Not applicable - This requirement is a best practice until 31 Mar 2025. 3.5.1.1 - Not applicable - This requirement is a best practice until 31 Mar 2025. 3.5.1.2 - Not applicable - This requirement is a best practice until 31 Mar 2025. 3.5.1.3 - Not applicable - Foregenix reviewed the cardholder dataflows and software inventory and found no disk-level or partition-level encryption used to render PAN unreadable. 3.7.9 - Not applicable - Foregenix reviewed policies and procedures, examined business practices and verified that USAePay does not share keys with their customers at any time. 4.2.1.1 - Not applicable - This requirement is a best practice until 31 Mar 2025. 4.2.1.2 - Not applicable - Foregenix reviewed policies and procedures, examined network diagrams and observed business practices and found no wireless technologies in use within the environment. 4.2.2 - Not applicable - USAePay does not send any CHD via end user messaging technologies such as email or instant messaging. 5.2.3.1 - Not applicable - This requirement is a best practice until 31 Mar 2025. 5.3.2.1 - Not applicable - This requirement is a best practice until 31 Mar 2025. 5.3.3 - Not applicable - This requirement is a best practice until 31 Mar 2025.

	5.4.1 - Not applicable - This requirement is a best practice until 31 Mar 2025. 6.3.2 - Not applicable - This requirement is a best practice until 31 Mar 2025. 6.4.2 - Not applicable - This requirement is a best practice until 31 Mar 2025. 6.4.3 - Not applicable - This requirement is a best practice until 31 Mar 2025. 6.5.2 - Not applicable - Foregenix confirmed that no significant changes have occurred in the past year. 7.2.4 - Not applicable - This requirement is a best practice until 31 Mar 2025. 7.2.5 - Not applicable - This requirement is a best practice until 31 Mar 2025. 7.2.5.1 - Not applicable - This requirement is a best practice until 31 Mar 2025. 8.2.3 - Not applicable - Foregenix verified through interview with responsible personnel, review of business practices that customers do not have access to the USAePay premises. 8.2.7 - Not applicable - Foregenix 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. 8.3.6 - Not applicable - This requirement is a best practice until 31 Mar 2025. 8.3.10 - Not applicable - This requirement is a best practice until 31 Mar 2025. 8.3.10.1 - Not applicable - This requirement is a best practice until 31 Mar 2025. 8.4.2 - Not applicable - This requirement is a best practice until 31 Mar 2025. 8.5.1 - Not applicable - This requirement is a best practice until 31 Mar 2025. 8.6.1 - Not applicable - This requirement is a best practice until 31 Mar 2025. 8.6.2 - Not applicable - This requirement is a best practice until 31 Mar 2025. 8.6.3 - Not applicable - This requirement is a best practice until 31 Mar 2025. 9.4.1 - Not applicable. Foregenix confirmed per interviews with responsible personnel that USAePay does not maintain offsite storage locations and does not store cardholder data on media. 9.4.1.1 - Not applicable. Foregenix confirmed per interviews with responsible personnel that USAePay does not maintain offsite storage locations and does not store cardholder data on media. 9.4.1.2 - Not applicable. Foregenix confirmed per interviews with responsible personnel that USAePay does not maintain offsite storage locations and does not store cardholder data on media. 9.4.2 - Not applicable. Foregenix confirmed per interviews with responsible personnel that USAePay does not maintain offsite storage locations and does not store cardholder data on media.

	9.4.3 - Not applicable. Foregenix confirmed per interviews with responsible personnel that USAePay does not maintain offsite storage locations and does not store cardholder data on media. 9.4.4 - Not applicable. Foregenix confirmed per interviews with responsible personnel that USAePay does not maintain offsite storage locations and does not store cardholder data on media. 9.4.5 - Not applicable. Foregenix confirmed per interviews with responsible personnel that USAePay does not maintain offsite storage locations and does not store cardholder data on media. 9.4.5.1 - Not applicable. Foregenix confirmed per interviews with responsible personnel that USAePay does not maintain offsite storage locations and does not store cardholder data on media. 9.4.6 - Not applicable. Foregenix confirmed per interviews with responsible personnel that USAePay does not maintain offsite storage locations and does not store cardholder data on media. 9.4.7 - Not applicable. Foregenix confirmed per interviews with responsible personnel that USAePay does not maintain offsite storage locations and does not store cardholder data on media. 9.5.1 - Not applicable. USAePay does not have any POI/POS terminals in scope for this assessment. 9.5.1.1 - Not applicable. USAePay does not have any POI/POS terminals in scope for this assessment. 9.5.1.2 - Not applicable. USAePay does not have any POI/POS terminals in scope for this assessment. 9.5.1.2.1 - Not applicable. USAePay does not have any POI/POS terminals in scope for this assessment. 9.5.1.3 - Not applicable. USAePay does not have any POI/POS terminals in scope for this assessment. 10.4.1.1 - Not applicable - This requirement is a best practice until 31 Mar 2025. 10.4.2.1 - Not applicable - This requirement is a best practice until 31 Mar 2025. 10.7.2 - Not applicable - This requirement is a best practice until 31 Mar 2025. 10.7.3 - Not applicable - This requirement is a best practice until 31 Mar 2025. 11.3.1.1 - Not applicable - This requirement is a best practice until 31 Mar 2025. 11.3.1.2 - Not applicable - This requirement is a best practice until 31 Mar 2025. 11.3.1.3 - Not applicable - Foregenix interviewed key personnel, reviewed change controls and examined evidence and found there were no significant changes performed during the past year. 11.3.2.1 - Not applicable - Foregenix interviewed key personnel, reviewed change controls and examined evidence and found there were no significant changes performed during the past year.

	11.4.4 - Not applicable - Foregenix review the penetration testing results and found there were no findings that needed remediation and would require a re-test. 11.4.7 - Not applicable - This requirement is a best practice until 31 Mar 2025. 11.5.1.1 - Not applicable - This requirement is a best practice until 31 Mar 2025. 11.6.1 - Not applicable - This requirement is a best practice until 31 Mar 2025. 12.3.1 - Not applicable - This requirement is a best practice until 31 Mar 2025. 12.3.3 - Not applicable - This requirement is a best practice until 31 Mar 2025. 12.3.4 - Not applicable - This requirement is a best practice until 31 Mar 2025. 12.5.2.1 - Not applicable - This requirement is a best practice until 31 Mar 2025. 12.5.3 - Not applicable - This requirement is a best practice until 31 Mar 2025. 12.6.2 - Not applicable - This requirement is a best practice until 31 Mar 2025. 12.6.3.1 - Not applicable - This requirement is a best practice until 31 Mar 2025. 12.6.3.2 - Not applicable - This requirement is a best practice until 31 Mar 2025. 12.10.4.1 - Not applicable - This requirement is a best practice until 31 Mar 2025. 12.10.7 - Not applicable - This requirement is a best practice until 31 Mar 2025. A1.1.1 - Not applicable A1.1.2 - Not applicable A1.1.3 - Not applicable A1.1.4 - Not applicable A1.2.1 - Not applicable A1.2.2 - Not applicable A1.2.3 - Not applicable A2.1.1 - Not applicable A2.1.2 - Not applicable A2.1.3 - Not applicable
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.*	2024-12-03
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	2025-02-03
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* 2025-03-04*)*.

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

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	
Jules Meyer	
Signature of Service Provider Executive Officer ↗	Date: 2025-03-04
Service Provider Executive Officer Name: Jules Meyer	Title: Director of Platform Architecture

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:
Kiska J Satterfield	
Signature of Lead QSA ↗	Date: 2025-03-04
Lead QSA Name: Kiska Satterfield	
Daniel Farr	
Signature of Duly Authorized Officer of QSA Company ↗	Date: 2025-03-04
Duly Authorized Officer Name: Daniel 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:

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/