Security Standards Council®

Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

Revision 2

September 2022

Document Changes

Date	Version	Description
September 2022	3.2.1 Revision 2	Updated to reflect the inclusion of UnionPay as a Participating Payment Brand.

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS).* Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

Part 1. Service Provider and Qualified Security Assessor Information

Part 1a. Service Provider Organization Information

Company Name:	Network Merchants, LLC		DBA (doing business as):	OMNI Pay	
Contact Name:	Jules Meyers		Title:	Director of Platform Architecture (Interim Head of Security)	
Telephone:	+44 7900 495 399		E-mail:	jules.meyer@nmi.com	
Business Address:	1450 American Lane, Suite 1200		City:	Schaumburg	
State/Province:	IL	Country:	United States	Zip:	60173
URL:	https://nmi.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:	Foregenix Ltd				
Lead QSA Contact Name:	Bradley Taylor		Title:	Security Analyst	
Telephone:	+44 845 309 6232		E-mail:	btaylor@foregenix.com	
Business Address:	1 Watts Barn, Bradbury		City:	Swindon	
State/Province:	Wiltshire	Country:	United Kingdom	Zip:	SN4 0EU
URL:	https://www.foregenix.com				

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):		
Name of service(s) assessed:	Network Merchants, LLC. OMNI Pay	
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 you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.*

Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check 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 Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder 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 and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder 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.

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility	Number of facilities of this type	Location(s) of facility (city, country)
Corporate Office	1	Schaumberg, IL USA
Hosted Data Center [redacted]	1	[redacted]
Hosted Data Center [redacted]	1	[redacted]

Part 2d. Payment Application

Does the organization use one or more Payment Applications? ☐ Yes ☒ No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
Not applicable.	Not applicable.	Not applicable.	☐ Yes ☒ No	Not applicable.

Part 2e. Description of 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 POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	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.
Does your business use network segmentation to affect the scope of your PCI DSS environment? *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*	☒ Yes ☐ No

Part 2f. Third-Party Service Providers	
Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated?	☐ Yes ☒ No
If Yes:	
Name of QIR Company:	Not applicable.
QIR Individual Name:	Not applicable.
Description of services provided by QIR:	Not applicable.
Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?	☒ Yes ☐ No
If Yes:	

Name of service provider:	**Description of services provided:**
ACI Worldwide Corp.	Transaction Processing
[redacted]	Data Center
[redacted]	Data Center
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 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as "Not Tested" or "Not Applicable" in the ROC.
- **None** – All sub-requirements of that requirement were marked as "Not Tested" and/or "Not Applicable" in the ROC.

For all requirements identified as either "Partial" or "None," provide details in the "Justification for Approach" column, including:

- Details of specific sub-requirements that were marked as either "Not Tested" and/or "Not Applicable" in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

***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 Pay

PCI DSS Requirement	**Details of Requirements Assessed**			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	☒	□	□	
Requirement 2:	□	☒	□	2.1.1 - Not Applicable – No wireless AP are used within the enclave. 2.2.3 – Not Applicable – No insecure service or protocols. 2.6 – Not Applicable - Not a hosting provider.
Requirement 3:	□	☒	□	3.4.1 – Not Applicable – No disk encryption is used. 3.6 – Not Applicable – Is not a service provider that shares keys.
Requirement 4:	□	☒	□	4.1.1 – Not Applicable – CHD is not transmitted over wireless Aps.
Requirement 5:	□	☒	□	5.1.2 – Not Applicable – All systems are monitored by Anti-malware.
Requirement 6:	□	☒	□	6.4.6 – Not Applicable – No significate changes noted during the assessment.
Requirement 7:	☒	□	□	
Requirement 8:	□	☒	□	8.1.5 – Not Applicable - No vendor accounts are in use that are not required MSSP user accounts.

				8.5.1 – Not Applicable - NMI does not remotely access customer locations.
Requirement 9:	☐	☒	☐	9.5.1 - Not Applicable - NMI does not maintain offsite storage locations. 9.6.2 - Not Applicable - No media is sent off site. 9.6.3 - Not Applicable - No media is sent off site. 9.7 - Not Applicable - No media is sent off site. 9.7.1 - Not Applicable - No media is sent off site. 9.9 - Not Applicable - No terminals are in scope for this assessment. 9.9.1 - Not Applicable - No terminals are in scope for this assessment. 9.9.2 - Not Applicable - No terminals are in scope for this assessment. 9.9.3 - Not Applicable - No terminals are in scope for this assessment.
Requirement 10:	☒	☐	☐	
Requirement 11:	☐	☒	☐	11.1.1 – Not Applicable - No wireless AP are used within the enclave.11.2.3 - Not Applicable – No significate changes noted during the assessment.
Requirement 12:	☒	☐	☐	
Appendix A1:	☐	☐	☒	All - Not Applicable – Not a shared hosting provider.
Appendix A2:	☐	☐	☒	All - Not Applicable – No insecure protocols or service.

Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	15 Mar 2024
Have compensating controls been used to meet any requirement in the ROC?	☐ Yes ☒ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes ☐ No
Were any requirements not tested?	☐ Yes ☒ No
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated 15 Mar 2024***.***

Based on the results documented in the ROC noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (***check one):***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby Network Merchants, LLC has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby Network Merchants, LLC has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: Not Applicable. An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with the payment brand(s) before completing Part 4.*
☐	**Compliant but with Legal exception:** One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

Signatory(s) confirms:
(Check all that apply)

☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version 3.2.1, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
☐	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☒	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☒	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

Part 3a. Acknowledgement of Status (continued)	
☒	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor Qualys

Part 3b. Service Provider Attestation	
Jules Meyer	
Signature of Service Provider Executive Officer ↑	*Date:* 15 Mar 2024
Service Provider Executive Officer Name: ***Jules Meyer***	*Title:* ***Director of Platform Architecture (Interim Head of Security)***

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)	
If a QSA was involved or assisted with this assessment, describe the role performed:	*The QSA assessed NMI OMNI Pay against all requirements in the PCI DSS version 3.2.1 standard and validated systems, collected evidence and documentation provided.*

Bradley Taylor	
Signature of Duly Authorized Officer of QSA Company ↑	*Date:* 15 Mar 2024
Duly Authorized Officer Name: Bradley Taylor	*QSA Company:* Foregenix Ltd.

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)	
If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	Not Applicable.

[1] Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

[2] The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

[3] Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present

within the transaction message.

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with the applicable payment brand(s) before completing Part 4.

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 a firewall configuration to protect cardholder data	☒	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	
3	Protect stored cardholder data	☒	☐	
4	Encrypt transmission of cardholder data across open, public networks	☒	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	
6	Develop and maintain secure systems and applications	☒	☐	
7	Restrict access to cardholder data by business need to know	☒	☐	
8	Identify and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholder data	☒	☐	
10	Track and monitor all access to network resources and cardholder data	☒	☐	
11	Regularly test security systems and processes	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	☒	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☒	☐	