



Payment Card Industry (PCI) Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2

June 2018

Section 1: Assessment Information

Instructions for Submissi

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): | N/A | | |
| Contact Name: | Jeremy Gumbley | Title: | CSO | | |
| Telephone: | +1 847 352 48 | E-mail: | security@nmi.com | | |
| Business Address: | 201 Main Street | City: | Roselle | | |
| State/Province: | Illinois | Country: | USA | Zip: | 69172 |
| URL: | https://nmi.com | | | | |

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

| | | | | | |
|------------------------|--------------------------|----------|--------------------------|------|---------|
| Company Name: | Foregenix Ltd | | | | |
| Lead QSA Contact Name: | Shawn Shifflett | Title: | Managing Consultant | | |
| Telephone: | +44 845 309 6232 | E-mail: | sshifflett@foregenix.com | | |
| Business Address: | 8-9 High Street | City: | Marlborough | | |
| State/Province: | Wiltshire | Country: | UK | Zip: | SN8 1AA |
| URL: | http://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. |
| Type of service(s) assessed: | | |
| Hosting Provider: <input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Shared Hosting Provider <input type="checkbox"/> Other Hosting (specify): | Managed Services (specify): <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify): | Payment Processing: <input checked="" type="checkbox"/> POS / card present <input checked="" type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify): |
| <input type="checkbox"/> Account Management | <input type="checkbox"/> Fraud and Chargeback | <input checked="" type="checkbox"/> Payment Gateway/Switch |
| <input type="checkbox"/> Back-Office Services | <input type="checkbox"/> Issuer Processing | <input type="checkbox"/> Prepaid Services |
| <input type="checkbox"/> Billing Management | <input type="checkbox"/> Loyalty Programs | <input type="checkbox"/> Records Management |
| <input type="checkbox"/> Clearing and Settlement | <input type="checkbox"/> Merchant Services | <input type="checkbox"/> Tax/Government Payments |
| <input type="checkbox"/> Network Provider | | |
| <input type="checkbox"/> 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: | Managed Services (specify): | Payment Processing: |
|---|---|--|
| <input type="checkbox"/> Applications / software | <input type="checkbox"/> Systems security services | <input type="checkbox"/> POS / card present |
| <input type="checkbox"/> Hardware | <input type="checkbox"/> IT support | <input type="checkbox"/> Internet / e-commerce |
| <input type="checkbox"/> Infrastructure / Network | <input type="checkbox"/> Physical security | <input type="checkbox"/> MOTO / Call Center |
| <input type="checkbox"/> Physical space (co-location) | <input type="checkbox"/> Terminal Management System | <input type="checkbox"/> ATM |
| <input type="checkbox"/> Storage | <input type="checkbox"/> Other services (specify) | <input type="checkbox"/> Other processing (specify): |
| <input type="checkbox"/> Web | | |
| <input type="checkbox"/> Security services | | |
| <input type="checkbox"/> 3-D Secure Hosting Provider | | |
| <input type="checkbox"/> Shared Hosting Provider | | |
| <input type="checkbox"/> Other Hosting (specify): | | |
| <input type="checkbox"/> Account Management | <input type="checkbox"/> Fraud and Chargeback | <input type="checkbox"/> Payment Gateway/Switch |
| <input type="checkbox"/> Back-Office Services | <input type="checkbox"/> Issuer Processing | <input type="checkbox"/> Prepaid Services |
| <input type="checkbox"/> Billing Management | <input type="checkbox"/> Loyalty Programs | <input type="checkbox"/> Records Management |
| <input type="checkbox"/> Clearing and Settlement | <input type="checkbox"/> Merchant Services | <input type="checkbox"/> Tax/Government Payments |
| <input type="checkbox"/> Network Provider | | |
| <input type="checkbox"/> 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

| | |
|---|--|
| <p>Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.</p> | <p>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 are out of scope of this assessment.</p> <p>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 1.2. Card not-present channels transactions capture CHD (PAN, cardholder name, card verification code, and expiration date).</p> <p>Encrypted (AES 256-bit) CHD (PAN, cardholder name, expiration date) and truncated PAN (first six (6) / last four (4)) are stored in [REDACTED] databases with a retention period of thirty-six (36) months.</p> |
| <p>Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.</p> | <p><u>Transmission:</u> NMI transmits CHD via public Internet encapsulate using TLS v1.2 to upstream processors for transaction processing.</p> <p><u>Processes:</u> NMI processes CHD (PAN, cardholder name, expiration date, card verification code, full track data) as they function as a payment gateway.</p> <p><u>Storage:</u> Encrypted (AES 256-bit) CHD (PAN, cardholder name, expiration date) and truncated (first six (6) / last four (4)) PAN are stored for reporting and recurring transaction processing with a retention period of thirty-six (36) months.</p> |

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 | Roselle, IL USA |
| Hosted Data Center (██████████) | 1 | ██████████ |
| Hosted Data Center (██████████) | 1 | ██████████ |

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. | Not applicable. | 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.*

Third-Party Relationships:

AOC Part 2f

CDE Segmentation:

Segmentation is managed by ██████████ 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 ██████████ firewalls and ██████████ 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 (last four (4)) 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:

[Redacted]

Data Center

[Redacted]

Data Center

ACI Worldwide Corp.

Payment Processor

Bambora Inc.

Payment Processor

BlueSnap, Inc.

Payment Processor

Cardworks Servicing, LLC.

Payment Processor

Checkout Ltd

Payment Processor

Chronopay LLC

Payment Processor

Cielo S.A.

Payment Processor

Credomatic

Payment Processor

Credorax Bank Ltd

Payment Processor

Elavon, Inc.

Payment Processor

Electronic Payment Exchange

Payment Processor

Evertec Group, LLC

Payment Processor

EVO Payments, Inc.

Payment Processor

First Data Buypass

Payment Processor

| | |
|--|-------------------|
| First Data Corporation | Payment Processor |
| Global Payments Direct, Inc. | Payment Processor |
| Heartland Payment Systems, LLC. | Payment Processor |
| Ingenico, Inc. | Payment Processor |
| Integratpay Pty Ltd | Payment Processor |
| Intuit Inc. | Payment Processor |
| IPpay LLC | Payment Processor |
| JetPay, LLC | Payment Processor |
| Mercadotecnia Ideas Y Tecnologia | Payment Processor |
| Merchant e-Solutions | Payment Processor |
| Merchant Partners | Payment Processor |
| Moneris Solutions | Payment Processor |
| National Merchants Association | Payment Processor |
| NCR Payment Solutions, LLC | Payment Processor |
| Nuvei Technologies | Payment Processor |
| Official Payments Corp. | Payment Processor |
| Pay360 by Capita | Payment Processor |
| Payment World | Payment Processor |
| Paymentech, LLC. (Subsidiary of Chase) | Payment Processor |
| Paynamics Technologies, Inc. | Payment Processor |
| PayPal, Inc. | Payment Processor |
| Paysafe | Payment Processor |
| Payvision B.V. | Payment Processor |
| Plug & Pay Technologies, Inc. | Payment Processor |
| Processing.com LLC. | Payment Processor |
| Propay Inc. | Payment Processor |
| RS2 Smart Processing | Payment Processor |
| SIA Transact Pro | Payment Processor |
| Skrill Limited | Payment Processor |
| TSYS International | Payment Processor |
| US Alliance Group, Inc. | Payment Processor |
| Valitor UK Ltd | Payment Processor |
| Vantiv | Payment Processor |
| Vesta Corporation | Payment Processor |
| Wirecard Processing LLC | Payment Processor |
| WorldPay US, Inc. | Payment Processor |

| | |
|---------------------|-------------------|
| Worldpay, Inc. | Payment Processor |
| ACI Worldwide Corp. | Payment Processor |

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, Inc. | | |
|---------------------------|-------------------------------------|-------------------------------------|--------------------------|---|
| PCI DSS Requirement | Details of Requirements Assessed | | | Justification for Approach <small>(Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)</small> |
| | Full | Partial | None | |
| Requirement 1: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Requirement 2: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 2.1.1 – No in-scope wireless. 2.2.3 – No insecure services, protocols, or daemons. 2.6 – NMI is not a shared hosting provider. |
| Requirement 3: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 3.4.1 – Full disk encryption is not used. 3.6 – NMI does not share symmetric keys for transmission or storage of CHD. |
| Requirement 4: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 4.1.1 – No in-scope wireless. |
| Requirement 5: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 5.1.2 – All systems are protected by anti-malware. |
| Requirement 6: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 6.4.6 – No significant change has occurred in this assessment cycle. |
| Requirement 7: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Requirement 8: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 8.1.5 – No non-MSSP vendor accounts are in use. 8.5.1 – NMI does not remotely access customer locations. |

| | | | | |
|-----------------|-------------------------------------|-------------------------------------|-------------------------------------|--|
| Requirement 9: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <p>9.5.1 – NMI does not maintain offsite storage locations.</p> <p>9.6.[2-3] – NMI does not send media offsite.</p> <p>9.7 - NMI does not send media offsite.</p> <p>9.7.1 - NMI does not send media offsite.</p> <p>9.8.1 – CHD is never stored in hard copy format.</p> <p>9.9 – No payment terminals are in scope for this assessment.</p> <p>9.9.[1-3] - No payment terminals are in scope for this assessment.</p> |
| Requirement 10: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Requirement 11: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 11.2.3 - No significant change has occurred in this assessment cycle. |
| Requirement 12: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Appendix A1: | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | |
| Appendix A2: | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | |

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: | <i>27 Mar 2020</i> |
| Have compensating controls been used to meet any requirement in the ROC? | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No |
| Were any requirements in the ROC identified as being not applicable (N/A)? | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| Were any requirements not tested? | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No |
| Were any requirements in the ROC unable to be met due to a legal constraint? | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No |

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated **27 Mar 2020**.

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**):

| <input checked="" type="checkbox"/> | <p>Compliant: All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby <i>Network Merchants, LLC</i>. has demonstrated full compliance with the PCI DSS.</p> | | | | |
|-------------------------------------|---|----------------------|--|-----------------|-----------------|
| <input type="checkbox"/> | <p>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 <i>Network Merchants, LLC</i>. has not demonstrated full compliance with the PCI DSS.</p> <p>Target Date for Compliance:</p> <p>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. <i>Check with the payment brand(s) before completing Part 4.</i></p> | | | | |
| <input type="checkbox"/> | <p>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.</p> <p><i>If checked, complete the following:</i></p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th style="text-align: center;">Affected Requirement</th> <th style="text-align: center;">Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">Not applicable.</td> <td style="text-align: center;">Not applicable.</td> </tr> </tbody> </table> | Affected Requirement | Details of how legal constraint prevents requirement being met | Not applicable. | Not applicable. |
| Affected Requirement | Details of how legal constraint prevents requirement being met | | | | |
| Not applicable. | Not applicable. | | | | |

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

| | |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | The ROC was completed according to the <i>PCI DSS Requirements and Security Assessment Procedures</i> , Version 3.2.1, and was completed according to the instructions therein. |
| <input checked="" type="checkbox"/> | All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects. |
| <input type="checkbox"/> | I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization. |
| <input checked="" type="checkbox"/> | I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times. |
| <input checked="" type="checkbox"/> | 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)

- | | |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | 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. |
| <input checked="" type="checkbox"/> | ASV scans are being completed by the PCI SSC Approved Scanning Vendor |

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑

Date: 27 March 2020

Service Provider Executive Officer Name: Jeremy Gumbley

Title: CSO

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:

Performed PCI DSS assessment during onsite visit, performed remediation, performed remote assessment follow-up, performed evidence review, authored ROC and AOC.

Signature of Duty Authorized Officer of QSA Company ↑

Date: 27 Mar 2020

Duty Authorized Officer Name: Shawn Shifflett

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

