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:** Gor Corporation

**Assessment End Date:** 2026-03-04

**Date of Report as noted in the Report on Compliance:** 2026-03-04

# 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: | Gor Corporation |
| DBA (doing business as): | USAePay, NMI Company |
| Company mailing address: | 1450 American Ln Ste 1200<br>Schaumburg, IL 60173<br>United States |
| Company main website: | https://nmi.com |
| Company contact name: | David Sage |
| Company contact title: | VP, SRE and Information Security |
| Contact phone number: | +1 (800) 617.4850 |
| 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<br>Badbury<br>Swindon<br>Wiltshire<br>SN4 0EU<br>United Kingdom |

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

## Part 2. Executive Summary

### Part 2a. Scope Verification

**Services that were INCLUDED in the scope of the Assessment (select all that apply):**

| | |
|---|---|
| Name of service(s) assessed: | 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): Not Applicable | | |

***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): Not Applicable

| 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. | 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.<br>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 2048-bit connection.<br>The FrontEnd forwards CHD to the BackEnd application, as follows:<br>• If transaction data contains full track or card security code (CVV) the BackEnd stores it in its database.<br>o The database instance is stored on disk with field level encryption that is AES 256-bit encryption.<br>o BackEnd simultaneously assembles an authorization message which is transmitted to processors for authorization via TLS v1.2, (RSA 2048-bit) and direct connections over private point-to- point or IPSEC (AES-256 bit) circuits.<br>o Full track / CVV is deleted upon batch closure.<br>o While the authorization message is compiled, BackEnd hashes PAN using HMAC512 which is stored in the card-store microservice which returns a GUID that gets stored in the internal transaction table to reference the card for recurring transactions.<br>• If the transaction data contains a PIN block the BackEnd extracts PAN, cardholder name, and expiration date from full track data, and stores it in the database.<br>o The database instance is stored on disk with field level encryption that is AES 256-bit encryption.<br>o 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.<br>o When the batch closes, full track and PIN block are deleted by overwriting encrypted fields in the database, card GUID, 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 AES 256-bit encryption.<br>o While the authorization message is compiled, BackEnd hashes PAN using HMAC512 which is stored in the card-store microservice which returns a GUID that gets stored in the internal |

| | |
|---|---|
| | transaction table to reference the card for recurring transactions. |
| Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data. | Transmission:<br>USAePay receives, processes, and transmits cardholder data to provide gateway services for their customers for purposes of authorization.<br>Cardholder data is transmitted over TLS v1.2 or private network to the payment processors.<br><br>Processes:<br>USAePay receives, processes, and transmits cardholder data to provide gateway services for their customers for purposes of authorization.<br>Cardholder data is processed to be encrypted and saved to the backend functions.<br><br>Storage:<br>USAePay receives, processes, and transmits cardholder data to provide gateway services for their customers for purposes of authorization.<br>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<br>• Load balancers<br>• Encryption<br>• Authentication<br>• Databases<br>• Management tools<br>• FIM<br>• IDS/IPS<br>• Virtualization<br>• Switches<br>• Anti-virus<br>• 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.<br>*For example:*<br>• *Connections into and out of the cardholder data environment (CDE).*<br>• *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.*<br>• *System components that could impact the security of account data.* | The USAePay environment is segmented between the corporate and cardholder data processing environments. All employees are either working remotely, Bristol office, Schaumburg office, New York Office or a South African office.<br>USAePay uses dedicated and third-party managed data center facilities to host its CDE. The data center environment are firewalled and contain multiple dedicated network zones used to host applications 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:<br>• Firewalls<br>• Load balancers.<br>• Encryption<br>• Authentication<br>• Databases<br>• Management tools<br>• FIM<br>• IDS/IPS<br>• Virtualization<br>• Switches<br>• Anti-virus<br>• Bespoke Applications.<br>Third-Party Relationships:<br>Reference AOC Part 2f<br>CDE Segmentation:<br>Segmentation is managed by [REDACTED] stateful inspection firewalls. USAePay 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], [REDACTED], [REDACTED], and [REDACTED] |

| | |
|---|---|
| | switches, [REDACTED] switches, and [REDACTED] and [REDACTED] switches.<br><br>Transmission:<br>USAePay receives, processes, and transmits cardholder data to provide gateway services for their customers for purposes of authorization.<br><br>Processes:<br>USAePay receives, processes, and transmits cardholder data to provide gateway services for their customers for purposes of authorization.<br><br>Storage:<br>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.<br>(Refer to the "Segmentation" section of PCI DSS for guidance on segmentation) | ☒ Yes ☐ No |

**Part 2d. In-Scope Locations/Facilities**
**(ROC Section 4.6)**

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this Assessment.

| Facility Type | Total Number of Locations (How many locations of this type are in scope) | Location(s) of Facility (city, country) |
|---|---|---|
| Corporate Office | 1 | Schaumburg, IL, USA |
| Data Center | 1 | [REDACTED], USA |
| Data Center | 1 | [REDACTED], USA |
| GCP | 1 | East, USA |

## 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 | P2PE v3.1 | P2PE v3.1 | 2023-00897.035 | 2026-12-13 |
| Bluefin TECS Engine P2PE | P2PE v3.1 | 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 |
| [REDACTED] | Colocation Data Center |
| [REDACTED] | Colocation Data Center |
| Logz.io | Elasticsearch API and Gateway API log management |
| GCP | Colocation Data Center |

***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<br>More than one response may be selected for a given requirement. Indicate all responses that apply. | | | | Select If Below Method(s) Was Used | |
|---|---|---|---|---|---|---|
| | In Place | Not Applicable | Not Tested | Not in Place | Customized Approach | Compensating Controls |
| Requirement 1: | ☒ | ☒ | ☐ | ☐ | ☐ | ☐ |
| Requirement 2: | ☒ | ☒ | ☐ | ☐ | ☐ | ☐ |
| Requirement 3: | ☒ | ☒ | ☐ | ☐ | ☐ | ☐ |
| Requirement 4: | ☒ | ☒ | ☐ | ☐ | ☐ | ☐ |
| Requirement 5: | ☒ | ☒ | ☐ | ☐ | ☐ | ☐ |
| Requirement 6: | ☒ | ☒ | ☐ | ☐ | ☐ | ☐ |
| Requirement 7: | ☒ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Requirement 8: | ☒ | ☒ | ☐ | ☐ | ☐ | ☐ |
| Requirement 9: | ☒ | ☒ | ☐ | ☐ | ☐ | ☐ |
| Requirement 10: | ☒ | ☒ | ☐ | ☐ | ☐ | ☐ |
| Requirement 11: | ☒ | ☒ | ☐ | ☐ | ☐ | ☐ |
| Requirement 12: | ☒ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Appendix A1: | ☐ | ☒ | ☐ | ☐ | ☐ | ☐ |
| Appendix A2: | ☐ | ☒ | ☐ | ☐ | ☐ | ☐ |

**Justification for Approach**

| | |
|---|---|
| For any Not Applicable responses, identify which sub-requirements were not applicable and the reason. | 1.2.3 - Not Applicable – No wireless is used in the CHD.<br>1.2.6 - Not Applicable – No insecure protocols are used.<br>1.3.3 - Not Applicable - No wireless is used in the CHD.<br>2.2.5 - Not Applicable - No insecure protocols are used.<br>2.3.1 - Not Applicable - No wireless is used in the CHD.<br>2.3.2 - Not Applicable - No wireless is used in the CHD.<br>3.3.3 - Not Applicable – USAePay is not an issuer.<br>3.5.1.2 - Not Applicable – USAePay does not use disk-level or partition level encryption.<br>3.5.1.3 - Not Applicable - USAePay does not use disk-level or partition level encryption.<br>3.7.9 - Not Applicable – USAePay does not share keys with customers.<br>4.2.1.2 - Not Applicable - No wireless is used in the CHD.<br>4.2.2 - Not Applicable – No CHD is sent by end user messaging.<br>5.3.3 - Not Applicable – No removable media is in use.<br>6.4.1 - Not Applicable - This requirement has been superseded by requirement 6.4.2<br>8.2.3 - Not Applicable – No customer access is allowed into the CDE.<br>8.2.7 - Not Applicable - No third-party access is allowed into the CDE.<br>8.3.10 - Not Applicable - This requirement has been superseded by requirement 8.3.10.1<br>8.3.10.1 - Not Applicable - USAePay does not use password/passphrases as the only authentication factor.<br>9.4.4 - Not Applicable - No removable media is in use.<br>9.4.5 - Not Applicable - No removable media is in use.<br>9.4.5.1 - Not Applicable - No removable media is in use.<br>9.4.6 - Not Applicable - No removable media is in use.<br>10.7.1 - Not Applicable - This requirement has been superseded by requirement 10.7.2<br>11.4.4 - Not Applicable – No re-test was needed.<br>A1.1.1 - Not Applicable - USAePay is not a Multi-Tenant Service Provider.<br>A1.1.2 - Not Applicable - USAePay is not a Multi-Tenant Service Provider.<br>A1.1.3 - Not Applicable - USAePay is not a Multi-Tenant Service Provider.<br>A1.1.4 - Not Applicable - USAePay is not a Multi-Tenant Service Provider.<br>A1.2.1 - Not Applicable - USAePay is not a Multi-Tenant Service Provider.<br>A1.2.2 - Not Applicable - USAePay is not a Multi-Tenant Service Provider.<br>A1.2.3 - Not Applicable - USAePay is not a Multi-Tenant Service Provider.<br>A2.1.1 - Not Applicable - USAePay does not have any POS/POI devices included in this assessment.<br>A2.1.2 - Not Applicable - USAePay does not have any POS/POI devices included in this assessment. |

| | |
|---|---|
| | A2.1.3 - Not Applicable - USAePay does not have any POS/POI devices included in this assessment. |
| 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:<br>***Note:*** *This is the first date that evidence was gathered, or observations were made.* | 2025-12-15 |
| Date Assessment ended:<br>***Note:*** *This is the last date that evidence was gathered, or observations were made.* | 2026-01-27 |
| 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* 2026-03-04*)*.

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: 2026-01-27

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: 03/10/2026 |
| Service Provider Executive Officer Name: David Sage | Title: VP, SRE and 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.<br>If selected, describe all role(s) performed: Not Applicable |

Leonardo Lima Ferla

| | |
|---|---|
| *Signature of Lead QSA ↗* | Date: 03/10/2026 |
| Lead QSA Name: Leonardo Lima Ferla | |

Ricardo dos Santos

| | |
|---|---|
| *Signature of Duly Authorized Officer of QSA Company ↗* | Date: 03/09/2026 |
| 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.<br>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/*