

**VGS**

The World's Leader
in Payment Tokenization

Very Good Security, Inc.
E: security@verygoodsecurity.com
P: +1 (844) 847-0232

9/25/2026

Payment Kit LLC ("Payment Kit")
1111B South Governors Avenue
Dover, Delaware 19904

Re: VGS AOC and Summary of Partnership with Payment Kit,

To Whom It May Concern:

I am writing this letter on behalf of Very Good Security ("VGS") and attaching it with our Attestation of Compliance ("AOC") to confirm that VGS is contractually partnering with Payment Kit, to provide managed data security services including tokenization as well as secure and compliant routing and storage of sensitive cardholder data.

VGS manages the security of cardholder data on behalf of Payment Kit.

VGS is a compliant PCI DSS 4.0 level 1 Service Provider (see our [Visa Global Service Provider Listing](#) as well as our attached AOC). On an annual basis, our systems are reviewed during an onsite assessment by a QSA, we engage an ASV for quarterly vulnerability scans, and conduct an annual penetration test as well as bi-annual segmentation testing.

Please let us know if you have any questions regarding our work with Payment Kit.

Sincerely,

Tim Nguyen
General Counsel
Very Good Security, Inc.
Tim.Nguyen@verygoodsecurity.com



PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: Very Good Security, Inc.

Date of Report as noted in the Report on Compliance: September 05, 2026

Date Assessment Ended: August 21, 2026



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:	Very Good Security, Inc.
DBA (doing business as):	
Company mailing address:	207 Powell St, Suite 200, San Francisco, CA 94102
Company main website:	https://www.verygoodsecurity.com
Company contact name:	Tim Nguyen
Company contact title:	General Counsel
Contact phone number:	650.382.2454
Contact e-mail address:	tim@verygoodsecurity.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:	Schellman Compliance, LLC
Company mailing address:	4010 W Boy Scout Boulevard, Suite 600, Tampa, FL 33607
Company website:	https://www.schellman.com/services/pci-compliance
Lead Assessor name:	Ray Price
Assessor phone number:	1.866.254.0000
Assessor e-mail address:	pciocs@schellman.com
Assessor certificate number:	QSA (204-183), PCIP (1003-797)

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: VGS Platform, including the following sub-components: VGS Vault, VGS API, VGS Collect, VGS Show, VGS Obsidian, VGS HTTP Proxy, VGS SFTP Proxy, VGS ISO/TCP Proxy, VGS Mail Proxy, VGS Managed File Transfer (MFT), VGS Card Management Platform (CMP)

Type of service(s) assessed:

Hosting Provider:

- ☒ Applications / software
- ☐ Hardware
- ☐ Infrastructure / Network
- ☐ Physical space (co-location)
- ☒ Storage
- ☐ Web-hosting services
- ☐ Security services
- ☐ 3-D Secure Hosting Provider
- ☐ Multi-Tenant Service Provider
- ☒ Other Hosting (specify): Tokenization

Managed Services:

- ☐ Systems security services
- ☐ IT support
- ☐ Physical security
- ☐ Terminal Management System
- ☐ Other services (specify): Not applicable.

Payment Processing:

- ☐ POI / card present
- ☐ Internet / e-commerce
- ☐ MOTO / Call Center
- ☐ ATM
- ☐ Other processing (specify): Not applicable.

☐ 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: All other VGS services not expressly specified

Type of service(s) not assessed:

Hosting Provider:

- ☐ Applications / software
- ☐ Hardware
- ☐ Infrastructure / Network
- ☐ Physical space (co-location)
- ☐ Storage
- ☐ Web-hosting services
- ☐ Security services
- ☐ 3-D Secure Hosting Provider
- ☐ Multi-Tenant Service Provider
- ☐ Other Hosting (specify):
Tokenization

Managed Services:

- ☐ Systems security services
- ☐ IT support
- ☐ Physical security
- ☐ Terminal Management System
- ☐ Other services (specify):
Not applicable.

Payment Processing:

- ☐ POI / card present
- ☐ Internet / e-commerce
- ☐ MOTO / Call Center
- ☐ ATM
- ☐ Other processing (specify):
Not applicable.

☐ 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 Sections 2.1 and 3.1)

Describe how the business stores, processes, and/or transmits account data.

VGS offers sensitive data tokenization (or "Aliasing"), vaulting, and detokenization services to its customers to help them reduce risk and compliance responsibilities associated with cardholder data storage. Customers direct their sensitive data to the VGS platform for tokenization and vaulting. Once processed and tokenized, data is encrypted and stored inside the Vault database. Additionally, a de-tokenization service allows certain customers to send a de-tokenization request to reveal certain tokenized data. Encrypted sensitive data may include, but is not



	limited to, cardholder data containing PAN and expiry date. VGS customers have the ability and responsibility to define what sensitive data is transmitted for tokenization and secure storage by the VGS platform. During the onboarding process, VGS instructs customers not to store sensitive authentication data.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	VGS is responsible for proxying, encrypting, tokenizing, and securely storing cardholder data transmitted to the VGS platform.
Describe system components that could impact the security of account data.	System components that could impact the security of account data include Elastic Compute instances (EC2) and Kubernetes containers running within the VGS AWS production environment. Additionally, VGS used various AWS services to support its tokenization service, including Relational Database Service (RDS), Key Management Service (KMS), and AWS Cloud Storage (S3).



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 VGS cardholder data environment is hosted within AWS's PCI DSS validated cloud infrastructure. Segmentation is achieved through Virtual Private Clouds (VPCs) and AWS security groups. Incoming traffic containing cardholder data is intercepted by a series of forward and reverse proxies, followed by auto-scaling data processing nodes responsible for data tokenization, encryption, and storage. The in-scope applications, tokenization, encryption, and payment flow configuration management services as well as supporting infrastructure are hosted within AWS. Third-party connectivity network equipment is hosted at Equinix.

VGS offers a variety of services for transmission, tokenization, storage, detokenization, and payment flow configuration management to its customers, including the following:

- VGS Vault - service for secure storage of sensitive data
- VGS API - tokenization API for storing, retrieving, and managing sensitive data within VGS Vault
- VGS Collect – JavaScript iFrame (used to interact, manipulate, or dynamically create an HTML document) and mobile SDK (software tools used to build mobile applications) used for the secure collection and transmission of sensitive data
- VGS Show – JavaScript iFrame used for the revealing of sensitive data
- VGS Obsidian – detokenization portal provided to customers to reveal aliased Primary Account Number (PANs) to support investigation workflows
- VGS HTTP Proxy – service for redacting and/or revealing sensitive data from a variety of data types, including JavaScript Object Notation (JSON) and Extensible Markup Language (XML) both a text-based data format used to store and transmit structured data, Regular Expression (Regex) a sequence of special characters that defines a search pattern, (Form) an interface used to collect, display, and process user input, HTML, and PDF
- VGS SFTP Proxy – service for redacting and/or revealing sensitive data in batch



	files via SFTP GET and SFTP PUT operations • VGS ISO/TCP Proxy – service for aliasing and revealing payment card data in ISO 8583 format (an international standard format used by financial systems to exchange electronic transactions made with credit or debit cards) • VGS Mail Proxy – service for sensitive data processing through Simple Mail Transfer Protocol (SMTP), a standard set of rules to send and route emails across the Internet. • VGS Managed File Transfer (MFT) – Service and workflow for redacting, revealing, and processing sensitive data in large batch files • VGS Card Management Platform (CMP) – service that offers capabilities for collecting and managing cardholder data, routing authorizations, and managing optimized payment routes
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)
AWS Data Centers	Three (3)	US East, VA, USA US East, OH, USA EU Central, Frankfurt, Germany
Equinix Data Center	One (1)	Ashburn, VA, 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
Not applicable.	Not applicable.	Not applicable.	Not applicable.	Not applicable.

* For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components, appearing on the PCI SSC website (www.pcisecuritystandards.org) (for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions), and Mobile Payments on COTS (MPoC) products.

Part 2. Executive Summary (continued)

Part 2f. Third-Party Service Providers
(ROC Section 4.4)

For the services being validated, does the entity have relationships with one or more third-party service providers that:

• Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage))	☒ Yes ☐ No
• Manage system components included in the entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers)	☒ Yes ☐ No
• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	☒ Yes ☐ No

If Yes:

Name of Service Provider:	Description of Services Provided:
Amazon Web Services (AWS)	Cloud hosting services
Equinix	Data center hosting services
Elasticsearch	Centralized logging
Okta	Identity provider
Orca Security	Enterprise Infrastructure Monitoring

Note: Requirement 12.8 applies to all entities in this list.



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:
Amazon Web Services (AWS)	Cloud hosting services
Equinix	Data center hosting services
Elasticsearch	Centralized logging
Okta	Identity provider

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: VGS Platform, including the following sub-components: VGS Vault, VGS API, VGS Collect, VGS Show, VGS Obsidian, VGS HTTP Proxy, VGS SFTP Proxy, VGS ISO/TCP Proxy, VGS Mail Proxy, VGS Managed File Transfer (MFT), VGS Card Management Platform (CMP)

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If a Compensating Control(s) Was Used
	In Place	Not Applicable	Not Tested	Not in Place	
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:	☐	☒	☐	☐	☐
Appendix A3:	☐	☒	☐	☐	☐



Justification for Approach

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.

2.3.1 – 2.3.2, 4.2.1.2: VGS did not have wireless networks within or connected to the in-scope environment.

3.3.2: Sensitive authentication data (SAD) was only stored in non-persistent (volatile) memory prior to authorization and was automatically deleted after one hour; SAD was never written to persistent storage.

3.4.2: VGS personnel had no ability to view the full PAN, and cardholder data repositories did not contain cleartext PAN.

3.5.1.1: VGS did not use hashing to render PAN unreadable.

3.5.1.2 – 3.5.1.3: VGS encrypted cardholder data at the field level within the database and did not use disk-level or partition-level encryption.

3.6.1.3: VGS did not have access to cleartext cryptographic key components; the key-encrypting key was managed within AWS KMS and the data-encrypting key was stored encrypted in the VGS database.

3.7.6: VGS did not perform manual cleartext cryptographic key management operations.

3.7.9: VGS did not share cryptographic keys with customers.

4.2.1.2: There were no wireless networks within or connected to the in-scope environment.

4.2.2: VGS did not receive or transmit cardholder data over end-user messaging technologies.

5.2.3 – 5.2.3.1: Malware software was implemented on all system components capable of installing such software.

5.3.2.1: Periodic malware scans were not applicable, as continuous scanning was in place for all system components.

6.4.1: This requirement has been superseded by Requirement 6.4.2 as of March 31, 2025.

8.2.3: No remote access to customer premises was available to users.

8.2.7: VGS did not permit third-party users access to the CDE.

8.3.9: Passwords were not used as the only authentication factor; VGS required multi-factor authentication through Okta in addition to a password.

8.3.10: This requirement has been superseded by Requirement 8.3.10.1 as of March 31, 2025.

8.3.10.1: VGS did not provide customer users access to cardholder data.

8.6.1: Interactive login accounts were not present on applications and/or systems.

9.4.6: VGS did not maintain hard-copy media containing cardholder data.

9.5.1 – 9.5.1.3, A2.1.1 – A2.1.3: VGS did not maintain any POS/POI devices.

10.7.1: This requirement has been superseded by Requirement 10.7.2 as of March 31, 2025.

11.4.7, A1.1.1 – A1.1.4, A1.2.1 – A1.2.3: VGS was not a multi-tenant service provider.

12.3.2: The customized approach was not used to fulfill any requirements in this assessment.

12.5.3: No significant changes to VGS's organization structure occurred during the previous 12 months.

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)

Date Assessment began: <i>Note: This is the first date that evidence was gathered, or observations were made.</i>	April 29, 2026
Date Assessment ended: <i>Note: This is the last date that evidence was gathered, or observations were made.</i>	August 21, 2026
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 September 05, 2026.

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 In Place or Not Applicable, resulting in an overall **COMPLIANT** rating; thereby *Very Good Security, Inc.* 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 *Very Good Security, Inc.* has not demonstrated compliance with PCI DSS requirements.
Target Date for Compliance: Not Applicable.
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 In Place or Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *Very Good Security, Inc.* 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 3. PCI DSS Validation *(continued)*

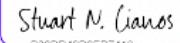
Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:

(Select all that apply)

☒	The ROC was completed according to <i>PCI DSS</i> , 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.

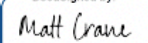
Part 3b. Service Provider Attestation

Signed by:	
 9300D4508ED7416... <i>Signature of Service Provider Executive Officer</i> ↑	
Date: 9/16/2026	
Service Provider Executive Officer Name: Stu Cianos	Title: Sr. Director, Security & Compliance

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: Not applicable.	

Signed by:	
 3B5295C4F931422 <i>Signature of Lead QSA</i> ↑	
Date: 9/17/2026	
Lead QSA Name: Ray Price	

DocuSigned by:	
 70708E160B6B696D <i>Signature of Duly Authorized Officer of QSA Company</i> ↑	
Date: 9/17/2026	
Duly Authorized Officer Name: Matt Crane	QSA Company: Schellman Compliance, LLC

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:	☐ ISA(s) performed testing procedures.
	☐ ISA(s) provided other assistance.
If selected, describe all role(s) performed: Not applicable.	

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has Non-Compliant results noted in Section 3.

If asked to complete this section, select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement below. For any "No" responses, include the date the entity expects to be compliant with the requirement and provide a brief description of the actions being taken to meet the requirement.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
1	Install and maintain network security controls	☒	☐	Refer to part 2g for requirement applicability.
2	Apply secure configurations to all system components	☒	☐	Refer to part 2g for requirement applicability.
3	Protect stored account data	☒	☐	Refer to part 2g for requirement applicability.
4	Protect cardholder data with strong cryptography during transmission over open, public networks	☒	☐	Refer to part 2g for requirement applicability.
5	Protect all systems and networks from malicious software	☒	☐	Refer to part 2g for requirement applicability.
6	Develop and maintain secure systems and software	☒	☐	Refer to part 2g for requirement applicability.
7	Restrict access to system components and cardholder data by business need to know	☒	☐	Refer to part 2g for requirement applicability.
8	Identify users and authenticate access to system components	☒	☐	Refer to part 2g for requirement applicability.
9	Restrict physical access to cardholder data	☒	☐	Refer to part 2g for requirement applicability.
10	Log and monitor all access to system components and cardholder data	☒	☐	Refer to part 2g for requirement applicability.
11	Test security systems and networks regularly	☒	☐	Refer to part 2g for requirement applicability.
12	Support information security with organizational policies and programs	☒	☐	Refer to part 2g for requirement applicability.
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	☒	☐	Refer to part 2g for requirement applicability.
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☒	☐	Refer to part 2g for requirement applicability.

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/>