

3/6/2024

TravelWits ("TravelWits")  
5001 Baum Blvd #434  
Pittsburgh, PA 15213

Re: VGS AOC and Summary of Partnership with TravelWits,

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 TravelWits, 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 TravelWits.

VGS is a compliant PCI DSS 3.2.1. 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 TravelWits.

Sincerely,

Tim Nguyen  
General Counsel  
Very Good Security, Inc.  
[Tim.Nguyen@verygoodsecurity.com](mailto:Tim.Nguyen@verygoodsecurity.com)



# **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:	Very Good Security, Inc		DBA (doing business as):		
Contact Name:	Tim Nguyen		Title:	General Counsel	
Telephone:	650.382.2454		E-mail:	tim@verygoodsecurity.com	
Business Address:	207 Powell St, Suite 200		City:	San Francisco	
State/Province:	CA	Country:	USA	Zip:	94102
URL:	https://www.verygoodsecurity.com				

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

Company Name:	Schellman Compliance, LLC				
Lead QSA Contact Name:	James M. Scardelis	Title:	Senior Associate		
Telephone:	+1.866.254.0000 x584	E-mail:	pciocs@schellman.com		
Business Address:	4010 W Boy Scout Boulevard, Suite 600	City:	Tampa		
State/Province:	FL	Country:	USA	Zip:	33607
URL:	https://www.schellman.com/pci-dss-validation				



## 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:	VGS Platform, including the following sub-components: <ul style="list-style-type: none"> <li>▪ VGS Vault</li> <li>▪ VGS API</li> <li>▪ VGS Collect</li> <li>▪ VGS Show</li> <li>▪ VGS Obsidian</li> <li>▪ VGS HTTP Proxy</li> <li>▪ VGS SFTP Proxy</li> <li>▪ VGS ISO/TCP Proxy</li> <li>▪ VGS IVR</li> <li>▪ VGS Mail Proxy</li> <li>▪ VGS Managed File Transfer (MFT)</li> <li>▪ VGS Payment Optimization</li> </ul>	
Type of service(s) assessed:		
<b>Hosting Provider:</b> <input checked="" type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input checked="" 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 checked="" type="checkbox"/> Other Hosting (specify): Tokenization	<b>Managed Services (specify):</b> <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):	<b>Payment Processing:</b> <input type="checkbox"/> POS / card present <input 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):		
<p><b>Note:</b> 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.</p>		


**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: 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  
☐ 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.

VGS offers sensitive data tokenization, vaulting, and de-tokenization services to its customers to help them reduce risk and compliance responsibilities associated with cardholder data storage. Customers direct their sensitive data, which may include cardholder 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.

VGS offers a variety of services for transmission, tokenization, storage, de-tokenization, and payment flow configuration management to their 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 and mobile SDK used for the secure collection and transmission of sensitive data
- VGS Show – JavaScript iFrame used for the revealing of sensitive data
- VGS Obsidian – de-tokenization portal provided to customers to reveal aliased PANs to support investigation workflows
- VGS HTTP Proxy – service for redacting and/or revealing sensitive data from a variety of data types, including JSON, XML, Regex, Form, 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
- VGS IVR – integration of the VGS HTTP Proxy with Twilio Connect for telephony card number entry
- VGS Mail Proxy – service for sensitive data processing through SMTP
- VGS Managed File Transfer (MFT) – service and workflow for redacting, revealing, and processing sensitive data in large batch files
- VGS Payment Optimization – service that offers capabilities for collecting and managing cardholder data, routing authorizations, and managing optimized payment routes



Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.

VGS is responsible for proxying, encrypting, tokenizing, and securely storing cardholder data transmitted to the VGS platform.

### 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):
<i>Example: Retail outlets</i>	3	<i>Boston, MA, USA</i>
Corporate Office	1	San Francisco, CA, USA
AWS Data Centers	3	US East, VA, USA US East, OH, USA EU Central, Frankfurt, Germany
Equinix Data Center	1	Ashburn, VA, USA

### Part 2d. Payment Applications

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.	<input type="checkbox"/> Yes <input type="checkbox"/> 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.*

The VGS cardholder data environment is hosted within the AWS PCI DSS validated cloud infrastructure. Segmentation is achieved using 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.

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:
Amazon Web Services (AWS)	Cloud hosting provider
Equinix, Inc.	Data Center Hosting Provider
Twilio Inc.	Interactive Voice Response (IVR)
Elasticsearch N.V.	Centralized Logging Services and Anti-Malware
Okta	Multi-Factor Authentication

**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:		VGS Platform		
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:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1.2.2 N/A: VGS did not utilize routers.
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2.1.1 N/A: VGS did not utilize wireless networks directly connected to the CDE. 2.2.3 N/A: VGS did not utilize any insecure services, protocols, or daemons. 2.6 N/A: VGS was not a shared hosting provider.
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3.4.1 N/A: VGS did not utilize full disk encryption. 3.6 N/A: VGS did not share cryptographic keys with customers. 3.6.6 N/A: VGS did not use manual clear-text cryptographic key-management operations.
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	4.1.1 N/A: VGS did not utilize wireless networks directly connected to the CDE.
Requirement 5:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	5.1.2 N/A: VGS installed anti-virus software on each system component in the CDE.
Requirement 6:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	6.4.6 N/A: VGS did not have any significant changes occur during the 12 months preceding the review date.
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 N/A: VGS did not allow vendors remote access to the cardholder data environment. 8.5.1 N/A: VGS did not have remote access to customer premises.



Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	9.9 – 9.9.3 N/A: VGS did not maintain card-interaction devices.
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 N/A: VGS did not have any significant changes occur during the 12 months preceding the review date.
Requirement 12:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	A1.1 – A1.4 N/A: VGS was not a shared hosting provider.
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	A2.1 – A2.3 N/A: VGS did not use SSL/Early TLS or POS POI terminals.



## 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>September 15, 2023</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 **September 15, 2023**.

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 *Very Good Security, Inc.* 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 (*Service Provider Company Name*) has not demonstrated full compliance with the PCI DSS.
- Target Date** for Compliance:  
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 r1, 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)**

- |                                     |  |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | No evidence of full track data <sup>1</sup> , CAV2, CVC2, CVN2, CVV2, or CID data <sup>2</sup> , or PIN data <sup>3</sup> 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 <i>Qualys</i>  |

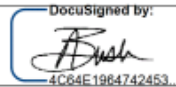
**Part 3b. Service Provider Attestation**

DocuSigned by:  
  
 E014FA05AFE7468

Signature of Service Provider Executive Officer ↑	Date: 9/29/2023
Service Provider Executive Officer Name: <b>Tim Nguyen</b>	Title: <b>General Counsel</b>

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

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

DocuSigned by:  
  
 4C64E1964742453

Signature of Duly Authorized Officer of QSA Company ↑	Date: 9/29/2023
Duly Authorized Officer Name: Adam Bush	QSA Company: Schellman Compliance, LLC

**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.
--	-----------------

<sup>1</sup> 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.

<sup>2</sup> 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.

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

