



Payment Card Industry Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0.1

Publication Date: August 2024



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

Entity Name: Givex Corporation

Date of Report as noted in the Report on Compliance: 26-FEB-2025

Date Assessment Ended: 11-FEB-2025



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:	Givex Corporation
DBA (doing business as):	Givex
Company mailing address:	Suite 1400-134 Peter Street Toronto, Ontario Canada M5V 2H2
Company main website:	https://www.givex.com
Company contact name:	Derrick Lobo
Company contact title:	Chief Security Officer
Contact phone number:	+1 (416) 350-9660 ext. 254
Contact e-mail address:	derrick.lobo@givex.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:	VikingCloud
Company mailing address:	70 West Madison Street, Suite 400, Chicago, IL 60602, USA
Company website:	https://www.vikingcloud.com/
Lead Assessor name:	William Jones
Assessor phone number:	+1 (833) 907-0702
Assessor e-mail address:	williamjones@vikingcloud.com
Assessor certificate number:	203-504



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:		E-commerce, Payment Gateway
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-hosting services <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Multi-Tenant Service Provider <input type="checkbox"/> Other Hosting (specify):	Managed Services: <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 type="checkbox"/> POI / 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 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 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:

- ☐ 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):

Managed Services:

- ☐ Systems security services
- ☐ IT support
- ☐ Physical security
- ☐ Terminal Management System
- ☐ Other services (specify):

Payment Processing:

- ☐ POI / 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 Role with Payment Cards (ROC Sections 2.1 and 3.1)

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

Givex Corporation (Givex) offers solutions to business-to-business merchant clients for point-of-sale operations, ecommerce, gift cards, loyalty programs and additional non-payment related services. As part of these solutions, Givex receives cardholder data (detailed below) on behalf of their business-to-business clients.

Givex's customers holding Visa, Mastercard, Discover, UnionPay and American Express credit cards, enter credit card information (PAN, card security codes, expiration date, cardholder name) into the Givex



	<p>Corporation branded website using a HTTPS TLS v1.2/1.3 RSA 2048-bit connection. Each client of Givex Corporation has its own webpage for authorization under the givex.com website. The e-commerce application communicates directly with the customer's merchant acquiring bank using either JSON, xml, html, or REST, depending on the Acquirer, and using cypher suite TLS v1.2/1.3 RSA 2048-bit with a 3D Secure authentication server. The card security codes are temporally stored in VRAM of the Givex webserver until the completion of the transaction where the security codes are securely deleted.</p> <p>Cardholder Data (PAN, cardholder name and expiry date) resulting from the transaction is one-way hashed with salt using SHA 256-bit and in turn transmitted and sent on from the web server using Json.rpc with TLS v1.2/1.3 RSA 2048-bit to be stored within the PCI database server that is AES 256-bit encrypted.</p> <p>The system Blackbox 3DSec server connects to the service providers acquirers over a TLS v1.3 RSA 2048-bit connection for the authorization of the transactions. Each payment processor returns the truncated PAN (First six, last four digits) Cardholder Name, and expiry date, in their local databases (Postgres 13.8.12) which is managed by Givex Corporation key management application on the Database server. No sensitive authorization data is ever written to disk (all held temporally in VRAM) which is deleted once the transaction is approved. A receipt containing the last 4 digits of the cardholder PAN is produced by the application for the customer.</p>
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Not Applicable
Describe system components that could impact the security of account data.	Not Applicable



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 following are critical systems components and also the connections in and out of the Cardholder data environment.

Back-end application and database systems that store and process credit card transactions to the Acquires.

3D authentication server – for authentication services

IPS/IDS systems

Workstations for administration

Firewalls for segmentation

Switches- gateway and internal switch

Administrative Workstations

Web Application Firewall (WAF)

Operating systems - NetBSD, Microsoft

Windows 10, Apple O/S FIM

Anti-Virus

SIEM server

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)
Head Office	1	Toronto, Ontario, Canada
Data Centers	2	Toronto, Ontario Canada London, UK



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))	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> 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)	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

If Yes:

Name of Service Provider:	Description of Services Provided:
Equinix Inc.	Colocation Data Centers
Forter Ltd.	Fraud Protection

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: E-commerce, Payment Gateway

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:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 2:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 3:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 6:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 7:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 9:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 10:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 12:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Justification for Approach



<p>For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.</p>	<p>2.2.5-No Insecure service, Protocols , Or Daemons are present in the Givex cardholder data environment.</p> <p>2.3.1, 2.3.2 - Givex does not use wireless to store, process or transmit cardholder data</p> <p>3.3.2, 3.4.2, 3.5.1.1, 3.5.1.2, 4.2.1.1, 5.2.3.1, 5.3.2.1, 5.3.3, 5.4.1, 6.3.2, 6.4.2, 6.4.3, 7.2.4, 7.2.5, 7.2.5.1, 8.3.10.1, 8.4.3, 8.5.1, 8.6.1, 8.6.2, 8.6.3, 10.4.1.1, 10.4.2.1, 10.7.2, 11.3.1.1, 11.3.1.2, 11.4.7, 11.5.1.1, 11.6.1, 12.3.1, 12.3.3, 12.3.4, 12.5.2.1, 12.5.3, 12.6.2, 12.6.3.1, 12.6.3.2, 12.10.4.1, 12.10.7 - This requirement is a best practice until 31-MAR-2025</p> <p>3.3.1.1- Track data is not received by Givex.</p> <p>3.3.3 Givex does not provide issuing services</p> <p>3.5.1.3- Givex does not use partition level or disk encryption,</p> <p>3.6.1.3-Givex does not use cleartext encryption keys</p> <p>3.7.9- Givex does not share Cryptographic keys with its customers</p> <p>4.2.1.2-, Givex does not use wireless connect to, store, process or transmit cardholder data</p> <p>4.2.2 - No end user messaging is used for transmitting PAN</p> <p>5.2.3 - no systems within the Givex environment are not at risk for Malware.</p> <p>8.2.3-Givex does not have access to its customers' premises</p> <p>8.2.7 - Third Parties have no access to the Givex environment.</p> <p>8.3.6 - Givex uses Multifactor Authentication for all user access</p> <p>8.3.9 - Givex uses Multifactor Authentication for all user access</p> <p>8.3.10 - Givex customers do not have access to cardholder data</p> <p>9.4.3- No media is sent outside the facility</p> <p>9.4.4- No media is sent outside the facility</p> <p>9.4.5- No Backup media within the Gives environment.</p> <p>9.4.6 - no hardcopy material I the Givex environment</p> <p>9.4.7 - No Backup media within the Givex environment</p> <p>9.5.1- 9.5.1.3 - No POI devices in the Givex environment</p> <p>12.3.2-Givex does not use the customized approach.</p> <p>A1.1.1 – A1.2.3-Givex is not a multi-Tenant service provider.</p> <p>A2.1.1- A2.1.3- Givex does not have POI's in its environment.</p>
<p>For any Not Tested responses, identify which sub-requirements were not tested and the reason.</p>	<p>Not Applicable</p>



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>	24-SEP-2024
Date Assessment ended: <i>Note: This is the last date that evidence was gathered, or observations were made.</i>	11-FEB-2025
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any testing activities performed remotely?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> 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 26-Feb-2025.

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 *Givex Corporation* 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 *(Service Provider Company Name)* has not demonstrated compliance with PCI DSS requirements.
Target Date for Compliance: YYYY-MM-DD
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 *(Service Provider Company Name)* 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)

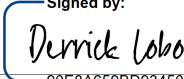
Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:

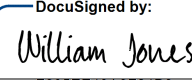

(Select all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to <i>PCI DSS</i> , Version 4.0.1 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 the Assessment in all material respects.
<input checked="" type="checkbox"/>	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

Signed by:  90E8A659BD93450...	
Signature of Service Provider Executive Officer ↑	Date: 2/27/2025
Service Provider Executive Officer Name: Derrick Lobo	Title: Chief Security Officer

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:	<input checked="" type="checkbox"/> QSA performed testing procedures.
	<input type="checkbox"/> QSA provided other assistance. If selected, describe all role(s) performed:
DocuSigned by:  F605EE49A6F24B8...	
Signature of Lead QSA ↑	Date: 2/27/2025
Lead QSA Name: William Jones	
DocuSigned by:  C2C6D1BD0A9C4E4...	
Signature of Duly Authorized Officer of QSA Company ↑	Date: 2/27/2025
Duly Authorized Officer Name: Michael Aminzade	QSA Company: Vikingcloud Inc.

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

If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:	<input type="checkbox"/> ISA(s) performed testing procedures.
	<input type="checkbox"/> ISA(s) provided other assistance. 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	<input type="checkbox"/>	<input type="checkbox"/>	
2	Apply secure configurations to all system components	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored account data	<input type="checkbox"/>	<input type="checkbox"/>	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems and networks from malicious software	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and software	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to system components and cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identify users and authenticate access to system components	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
10	Log and monitor all access to system components and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Test security systems and networks regularly	<input type="checkbox"/>	<input type="checkbox"/>	
12	Support information security with organizational policies and programs	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	<input 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 type="checkbox"/>	<input type="checkbox"/>	

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/