



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: Interactive Transaction Solutions Limited

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

Date Assessment Ended: 13-Nov-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:	Interactive Transaction Solutions Limited
DBA (doing business as):	PAYA Gateway
Company mailing address:	1 Westleigh Office Park, Scirocco Close, Moulton Park, Northampton, NN3 6BW United Kingdom
Company main website:	https://www.interactivets.com
Company contact name:	Maverick Phillips
Company contact title:	Infrastructure & Security Manager
Contact phone number:	+44 0333 123 1243
Contact e-mail address:	Maverick.phillips@paya.group

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 W. Madison St. Suite 400, Chicago, IL, 60602, USA
Company website:	https://www.vikingcloud.com
Lead Assessor name:	William Fung
Assessor phone number:	+1 833-907-0702



Assessor e-mail address:	williamfung@vikingcloud.com
Assessor certificate number:	033-005

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:	PAYA 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 checked="" 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 checked="" type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Network Provider		
<input type="checkbox"/> Others (specify):		

Note: These categories are provided for assistance only and are not intended to limit or predetermine an entity's service description. If 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: Mplus

Type of service(s) not assessed:

<p>Hosting Provider:</p> <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):	<p>Managed Services:</p> <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):	<p>Payment Processing:</p> <input type="checkbox"/> POI / 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 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 checked="" type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Network Provider		
<input type="checkbox"/> Others (specify):		

Provide a brief explanation why any checked services were not included in the Assessment:

The Mplus merchant statement systems are for merchant statement services that does not store, process and transmit any cardholder data, these systems are hosting in the network which is isolated from the PAYA Gateway's cardholder data environment (CDE), and it is totally segmented from the PATA Gateway's CDE and on its own discreet Vlan.
 It is not accessible from the PAYA Gateway's CDE and does not consume any PAYA Gateway's CDE services.



**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.

Interactive Transaction Solutions Limited (Hereafter "PAYA Gateway") is a service provider providing payment services to merchants. The following business functions are responsible for the security of the service:

- IT Infrastructure is responsible for the design, security and management of the CDE.
- Software Development is responsible for application security and quality.
- Gateway Services provide customer support for ensuring the data quality and consistency to the acquirers.
- Human Resources ensure that all staff that join the company have external vetting.
- The Change Board is responsible for change management of the CDE.
- Executive Team is accountable for decision making, change approval, incident management and ensuring resources are available.
- Testing is responsible for testing the application prior to deployment on the infrastructure.

Where PAYA Gateway users interact with the gateway directly via the product set, receive clear text cardholder data (secure transmitted via TLS 1.2/1.3 with AES 256bit encryption) will be received via the Internet facing PAYA Gateway application servers hosting PAYA Gateway products, known collectively as ITS Connect.

PAYA Gateway provides card not present solutions via ITS connect application which including an ERP real-time web service for online payments, legacy real-time ERP transaction service, back office PayPage for processing transactions by customers and also provides an iframe for Merchant e-commerce transactions. The iframe page utilises TLS 1.2/1.3 encryption.

PAN, expiration date, cardholder name, card verification code (CVV2, CVC2, CID) received and transmitted from merchants to PAYA Gateway via TLS 1.2/1.3 AES 256-bit. Only PAN cardholder name and expiration date stored in the database (Sample Set-6) with TDE AES 256bit protection, PAN is further encrypted by AES 256-bit.



	<p>PAYA Gateway also provides card not present solutions for B2B trade counters and B2C solutions such as charity donations including a virtual terminal used by customers to manage payments, Service Portal hosts Card Alias (tokens for cardholder data and subsequent use), Transaction Manager, Batch CSV, Virtual Terminal, Manage Buyers, Manage Products, ITS Direct and G.A.T.S payments for American Express airline data.</p> <p>PAN, expiration date, cardholder name, card verification code (CVV2, CVC2, CID) received and transmitted via TLS 1.2/1.3 AES 256-bit. Only PAN cardholder name and expiration date stored in the database (Sample Set-6) with TDE AES 256bit protection, PAN is further encrypted by AES 256-bit.</p> <p>Some customers settle transactions by file processing via SFTP. Transactions (PAN, expiration date, cardholder name, card verification code (CVV2, CVC2, CID)) are sent in a PGP (AES 256-bit) encrypted 'IN' file which are then processed and results presented in an encrypted 'OUT' file is saved to an out folder to be collected by customers or in some cases is sent to customers.</p> <p>Only PAN cardholder name and expiration date stored in the database (Sample Set-6) with TDE AES 256bit protection, PAN is further encrypted by AES 256-bit.</p> <p>PAYA Gateway also process the transaction from stand-alone or integrated card PCI certified terminals. Track 2 or track 2 equivalent data received from the terminal (via TLS 1.2) and the Track 2 or track 2 equivalent data only held in the VRAM of the payment gateway application servers, the PAN and expiration date is extracted for processing and stored in the database (Sample Set-6) with TDE AES 256bit protection, PAN is further encrypted by AES 256-bit.</p> <p>The Card verification code (CVV2, CVC2, CID) , Track 2 or track 2 equivalent data mentioned in all the above transactions are only held in VRAM on web servers or payment gateway application servers, and then it is securely purged immediately after the authorization has been sent to acquirers via TLS 1.2/1.3 (AES 256-bit) connections, and it is never written to disk.</p>
<p>Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.</p>	<p>Not applicable.</p>
<p>Describe system components that could impact the security of account data.</p>	<p>Not applicable.</p>



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 incoming connection to PAYA Gateway by HTTPS (TLS 1.2/1.3), encrypted VPN through secured network provided by TNS network (UK) or Lyra (France), or SFTP. Outgoing data is sent by PAYA Gateway via SFTP and encrypted VPN networks.

VikingCloud covered the following environments during this assessment:

- Firewalls
- Load Balancers
- Web Application Firewall
- IDS
- Switch
- Database
- Operating Systems
- Terminal Servers
- Virtualization
- Anti-virus
- Anti-phishing solution
- Patching management tools
- Log management and FIM solution
- PAYA Gateway application
- Monitoring Servers
- NAS backup solution
- CCTV and door access systems
- Wireless scanner
- Vulnerability scanner

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)
Data centers	2	Slough, United Kingdom London, United Kingdom
Corporate Office	1	Whiteley, United Kingdom



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:

<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • Could impact the security of the entity’s CDE (for example, vendors providing support via remote access, and/or bespoke software developers). 	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

If Yes:

Name of Service Provider:	Description of Services Provided:
Equinix Inc	Secure Colocation Provider
Rapid7	Security, Managed SOC, No access to the CDE
TNS	Secure network provider that provides connectivity for the transmission of cardholder authorization data between the Payment Gateway and acquirers.
Lyra	Secure network provider that provides connectivity for the transmission of cardholder authorization & capture data between the Payment Gateway and French acquirers.
Endeavour Internet Business Solutions Ltd	Third party EMV 2.x 3DS Authentication Gateway

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: PAYA 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 checked="" 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 type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 7:	<input checked="" type="checkbox"/>	<input 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 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



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

- 1.3.3 - PAYA Gateway does not use wireless networking in their environment(s)

- 2.2.5 - All unnecessary functionality is disabled.

- 2.3.1, 2.3.2 - PAYA Gateway does not use wireless systems to store, process, or transmit cardholder data and that no wireless environments are linked to the CDE.

- 3.3.2 - SAD is only held in VRAM. Once the transaction has completed, the SAD data has a pointer to the data set to zero.

- 3.3.3 - PAYA Gateway does not function as a card issuer.

- 3.4.2 - There is no user can access to full PAN, all PAN is either encrypted, truncated when store or masked when display.

- 3.5.1.2, 3.5.1.3 - PAYA Gateway does not use disk-level or partition-level encryption.

- 4.2.1.2 - PAYA Gateway does not utilize wireless systems to store, process, or transmit cardholder data, and no wireless environments are connected to the CDE.

- 4.2.2 - End-user messaging systems are not used to transmit cardholder data under any circumstances.

- 5.2.3 - all systems with the capability to support anti-malware protection have the solution installed and actively running.

- 5.3.2.1 - Malware scans are conducted continuously, eliminating the need for periodic scans.

- 8.2.2 - no group, shared, or generic accounts are used by PAYA Gateway.

- 8.2.3 - PAYA Gateway does not maintain access to customer systems.

- 8.2.5 - There is no terminated user so far in the PAYA Gateway's new environment.

- 8.2.7 - Third parties are not granted access to the PAYA Gateway's environment.

- 8.3.10, 8.3.10.1 - Full PAN or SAD cannot be accessed by the customers.



	<p>8.6.1, 8.6.2 - Systems or applications accounts cannot be used for interactive login.</p> <p>9.2.2 - There are no network access points in publicly accessible areas.</p> <p>9.4.1.1 - There are no offline media backups is used at the time of conducting this assessment.</p> <p>9.4.3 - No physical media containing CHD is created, stored, or transported outside of the CDE.</p> <p>9.4.4, 9.4.5, 9.4.5.1 - no physical media containing CHD is created, stored, or transported outside of the CDE</p> <p>9.4.6 - There is no any hard-copy material with cardholder data.</p> <p>9.5.1, 9.5.1.1, 9.5.1.2, 9.5.1.2.1, 9.5.1.3 - PAYA Gateway does not maintain any POI terminals for their payment services provided.</p> <p>11.2.2 - PAYA Gateway does not have wireless present in their environment(s).</p> <p>11.3.1.3 - There were no significant changes in the environment in the last year.</p> <p>11.4.7 - PAYA Gateway is not a multi-tenant service provider.</p> <p>12.3.2 - PAYA Gateway does not using any customized approach as the control for the PCI DSS requirements.</p> <p>A1 – PAYA Gateway is not a multi-tenant service provider.</p> <p>A2 - PAYA Gateway does not use or maintain any POI device in the CDE and does not use any version of SSL or early versions of TLS.</p> <p>A3 – This assessment is not a Designated Entities Supplemental Validation (DESV)</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>	30-Jul-2025
Date Assessment ended: <i>Note: This is the last date that evidence was gathered, or observations were made.</i>	13-Nov-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 type="checkbox"/> Yes <input checked="" 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-Nov-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*):

<input checked="" type="checkbox"/>	<p>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 Interactive Transaction Solutions Limited has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.</p>								
<input type="checkbox"/>	<p>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 (<i>Service Provider Company Name</i>) has not demonstrated compliance with PCI DSS requirements.</p> <p>Target Date for Compliance: YYYY-MM-DD</p> <p>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.</p>								
<input type="checkbox"/>	<p>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 (<i>Service Provider Company Name</i>) 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.</p> <p>This option requires additional review from the entity to which this AOC will be submitted.</p> <p><i>If selected, complete the following:</i></p> <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <thead> <tr> <th style="width: 35%;">Affected Requirement</th> <th>Details of how legal constraint prevents requirement from being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement from being met						
Affected Requirement	Details of how legal constraint prevents requirement from being met								



Part 3. PCI DSS Validation *(continued)*

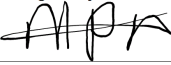
Part 3a. Service Provider Acknowledgement

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:


Signature of Service Provider Executive Officer 	Date: 26-Nov-2025 1:30 PM EST
Service Provider Executive Officer Name: Maverick Phillips	Title: Head of IT & Security

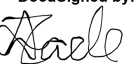
Part 3c. Qualified Security Assessor (QSA) Acknowledgement


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:

Signed by:


Signature of Lead QSA 	Date: 26-Nov-2025 2:15 PM EST
Lead QSA Name: William Fung	

DocuSigned by:


Signature of Duly Authorized Officer of QSA Company 	Date: 26-Nov-2025 2:49 PM EST
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/