



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: Agile Ticketing Solutions, LLC

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

Assessment End Date: August 27, 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:	Agile Ticketing Solutions, LLC
DBA (doing business as):	-
Company mailing address:	3810 Central Pike Suite 301, Hermitage, TN 37076, United States
Company main website:	http://www.agiletix.com/
Company contact name:	Richard Steward
Company contact title:	CEO/ CTO
Contact phone number:	+1 615.360.6700
Contact e-mail address:	rsteward@agiletix.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:	ControlCase
Company mailing address:	Fifty West Corporate Center 3975 Fair Ridge Drive, Suite D T25s, Fairfax, VA 22033
Company website:	https://www.controlcase.com/
Lead Assessor name:	Omar Akkad
Assessor phone number:	+1 (703).483.6383
Assessor e-mail address:	oakkad@controlcase.com

Assessor certificate number:

QSA – 205-893

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:

Events ticketing management solutions

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):

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):

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: None

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 Section 2.1)

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

Agile Ticketing Solutions, LLC (hereafter Agile) is a level 1 PCI DSS Service provider. Agile offers Customer management software such as planning, donor, membership, event ticketing system design, development, operations and marketing technologies for theatres, art houses, performing art centers, museums, film festivals, universities & colleges, garden & tours, state & county fairs etc.

The focus of this assessment is on 'payment system' application and 'payment management' services provided to customers that are hosted in the Agile Ticketing Solutions, LLC production environment. Agile Production environment hosted at third party hosting provider at 'Franklin, Tennessee' and it is the part of PCI Assessment. Agile accepts payment on behalf of their customers through 'Card Present' and 'Card Not Present' channel and helps in processing the payment.

Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.

Card Not Present and Card Present Flow: (WEB and POS Flow)

Store:

After authorization, the encrypted cardholder data is stored during Card Present and Card Not Present transactions using AES-256-bit encryption in the database (DB-MSSQL-CHD-SQLDAT). There is no storage of SAD once the transaction gets approved. The customer information such as name, address, last 4 digits of PAN, BIN, expiry date, tokens are stored in DB-MSSQL-CHD-SQLDAT.

Transmit:

Here is the description of transmitting "Account data" over "Card Not Present" and "Card Present" channel:

Channel1: Card Not Present (WEB Flow)

End user fills account data (PAN, expiry, CVV) through below sub application of 'Agile Ticketing Application' and unique to each customer of agile.

- Customer facing while purchasing ticket:
(https://*.agileticketing.net/websales/)

Further the account data is sent over HTTPS_TLS 1.2 to Agile production Web server. Web server calls a webservice (<https://bal2.agiletx.net/BusinessAccessLayer2/PaymentTransaction.soap>) and requests Agile Production Bal server for validation. The account data is sent for the authorization to the third-party payment processor via third party SDK i.e. 4Dpayment Gateway and E payment Integrator over HTTPS_TLS 1.2. Third party SDK are integrated with 'Agile Ticketing Application'.

Channel2: Card Present (POS Flow)

End user swipes account data (PAN, expiry, full track) using POS at client end and encrypted using DUKPT at the pos level. POS device is integrated with thick client application running at the client end. Please note that legacy POS does not encrypt account data. The Thick client application of Agile is already covered as part of Agile PCI assessment as software is availed by Agile. However, the environment of Agile's client is not part of this assessment as the responsibility lies with Agile's client.

Thick client application calls webservice (<https://prodX.agileticketing.net/BusinessAccessLayer2/PaymentTransaction.soap>) to send account data to Agile production Web server over HTTPS_TLS1.2. Further the Web server decrypts DUKPT swiped data and transmits account data to the third-party payment processor via third party SDK i.e., 4Dpayment Gateway and E payment Integrator over HTTPS_TLS 1.2 for authorization. Third party SDK are inside the 'Agile Ticketing Application'.

Process:

Here is the description of processing "account data" over "Card Not Present" and "Card Present" channel:

Channel1: Card Not Present (WEB Flow)

When account data gets passed from Agile production Webserver to Agile production Bal server by calling a webservice (<https://bal2.agiletx.net/BusinessAccessLayer2/PaymentTransaction.soap>), Bal server provides the process of validation such as mod10 operation. After authorization, the cardholder data is encrypted using AES-256 bit by Bal Server and produces a reference token.

Thus, Agile processes cardholder data by encryption, validation and producing tokens.

Channel2: Card Present (POS Flow)

The Agile production Web server decrypts DUKPT swiped data as part of processing and sends it to the third-party payment processor. After authorization, the cardholder data is encrypted using AES-256 bit by Web Server and produces a reference token.

Thus, Agile processes cardholder data by encryption, decryption and producing tokens.

NCDE Process: (PAX, Moneris flow)

- Moneris provided NST.dll are installed on client end and integrated with thick client application of Agile to transmit account data directly to third-party payment processor i.e., Moneris over HTTPS_TLS 1.2.
- Similarly, PosLink.dll are provided by PAX and integrated with Thick client application of Agile at client end to communicate directly with the third-

	party payment processors i.e. TSYS, Bluefin over HTTPS_TLS1.2 • The Thick client application of Agile is already covered as part of Agile PCI assessment as software is availed by Agile. However, the environment of Agile's client is not part of this assessment as the responsibility lies with Agile's client. • After authorization, auth status, transaction token, name, expiry date, last 4 digits of PAN and BIN are sent to the Agile production Web server over HTTPS_TLS1.2 by calling a webservice (https://prodX.agileticketing.net/BusinessAccessLayer2/PaymentTransaction.soap) and gets stored in DB-MSSQL-CHD-SQLDAT. There is no involvement of sharing SAD or Full PAN with Agile production Web server. • Thus, there is no direct involvement of Agile production environment as part of transmission and processing. No storage of CHD through PAX and Moneris Flow. Thus, marked as NCDE Process.
Describe system components that could impact the security of account data.	The focus of this assessment is on 'payment system' application and 'payment management' services provided to customers that are hosted in the Agile production environment. Agile Production environment hosted at third party hosting provider at 'Franklin, Tennessee' and it is the part of PCI Assessment. Agile accepts payment on behalf of their customers through 'Card Present' and 'Card Not Present' channel and helps in processing the payment. <u>Card Present:</u> Agile accepts payments via in house developed "Thick client application" installed on client end and it calls a webservice to transmit the account data to Agile Production Web server. Further it sends the authorization request to the third-party payment processor via third party SDK i.e. 4DPayment Gateway and E payment Integrator. These third-party SDK are inside Agile Ticketing Application. <u>Card Not Present:</u> Agile accepts payments via in house developed 'Agile Ticketing Application' and sends the authorization request to the third-party payment processor via third party SDK i.e. 4Dpayment Gateway and E payment Integrator. These third-party SDK are inside Agile Ticketing Application. The involvement of third-party payment processors is FDMS, Moneris, Safe save, Bluefin Payment Systems, Bean stream Internet Commerce Inc, Authorize.net, TSYS.

However, Agile does not have direct contract with TYSY, Beanstream, FDMS, Authorize, Moneris. Clients of Agile are in contract with these service providers because of which Agile needs to share Account data with TYSY, Beanstream, FDMS, Authorize, Moneris for processing.

The Agile corporate office is not in the part of the scope as it does not handle, process, store, or transmit cardholder data.

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.*

Role of in-scope Locations:

Card Present and Card Not Present transactions are accepted by Agile production servers that are hosted on Flexential Data and Network Center and transmitted to the third-party service provider for payment processing.

Connection into CDE environment:

i) Card-NOT-Present:

It accepts payments via in house developed 'Agile Ticketing Application' and sends the authorization request to the third-party payment processor via third party SDK i.e. 4DPayment Gateway and E payment Integrator. These third-party SDK are inside Agile Ticketing Application.

ii) Card-Present:

It accepts payments via in house developed "Thick client application" installed on client end and it calls a webservice to transmit the account data to Agile production server. Further it sends the authorization request to the third-party payment processor via third party SDK i.e. 4DPayment Gateway and E payment Integrator. These third-party SDK are inside Agile Ticketing Application.

Technology Used:

- Unified Security Management: Firewall/IDPS/VPN/Logging/FIM
- Incapsula WAF
- Symantec Endpoint Protection Anti-virus
- Windows Server 2016: Web Application Server, Reporting Server, Database Server
- IIS 10 and 8 Web Server
- E Payment Integrator (Third party SDK)
- 4Dpayments Gateway 2016 (Third party SDK)
- Agile Ticketing Application is the master application, and it has sub application as below:

	- Agile Ticketing Application: Portal: – Agile Ticketing Application: Customer facing while purchasing ticket and webservices – Thick Client Application – ControlCase Logging & Monitoring Appliance - Microsoft Azure Recover Services for data backup (SAAS) Additional: Agile does not have direct contracts with TYSY, Beanstream, FDMS, Authorize, Moneris. Client of Agile are in contract with these service providers because of which Agile need to share Account data with TYSY, Beanstream, FDMS, Authorize, Moneris for processing.
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)
<i>Example: Data centers</i>	3	<i>Boston, MA, USA</i>
Data Centers	1	Flexential Data and Network Center 425 Duke Drie Suite 400 Franklin, TN 37067
WAF services	1	Imperva Main IT and Dev Center, Tel Aviv, IL

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 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:
Flexential (Colocation)	Hosting provider
Imperva Incapsula	Cloud based Web Application Firewall
Flexential Corporation (Cloud Operation)	Firewall and WAF management
Bluefin Payment Systems	Payment Gateway
SafeSave/softerware	Payment Gateway
Microsoft Azure	Database backups

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: Events ticketing management solutions

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

Justification for Approach

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

1.2.6 – Agile doesn't have any insecure services, protocols, or ports running in the scope. Hence, this control is not applicable.

	1.3.3 – There are no wireless networks in the Agile production environment. Hence, this control is not applicable. 1.5.1 – Agile has not used any insecure services, protocols, and ports. Hence, this control is not applicable. 2.3.1, 2.3.2 – There are no wireless networks in the Agile environment. Hence, these controls are not applicable. 3.3.2 - SAD is data that is not stored by the assessed entity. Hence, this control is not applicable. 3.3.3 - The scoped environment does not support issuing services. Hence, this control is not applicable. 3.4.2 - No one has access to full PAN. Hence, this control is not applicable. 3.5.1.1 - Hashes are not used to render PAN unreadable. Hence, this control is not applicable. 3.5.1.2 , 3.5.1.3- Disk Encryption is not utilized in the assessed entity. Hence, this control is not applicable. 3.6.1.3 - Access to clear text cryptographic key components is not in place. Hence, this control is not applicable. 3.7.6 - Manual cleartext cryptographic key-management operations are not in place in the scoped environment. Hence, this control is not applicable. 3.7.9 – The assessed entity does not share keys with customers . Hence, this controls are not applicable. 4.2.1.2 – There are no wireless networks in the Agile production environment. Hence, this control is not applicable. 4.2.2 – Agile never sends unprotected PANs by end-user messaging technologies. Hence, this control is not applicable. 5.3.3 – Agile does not use removable media in the scoped environment. Hence, this control is not applicable.
--	---

6.4.1 - This requirement is superseded by Requirement 6.4.2. Hence, this control is not applicable.

6.5.2 - No significant change occurred in the environment within the past 12 months. Hence, this control is not applicable.

8.2.2 - Agile is not using any group, shared, or generic accounts in PCI scope. Hence, this control is not applicable.

8.2.3 - Agile doesn't have access to customer premises. Hence, this control is not applicable.

8.2.7 - Agile does not provide access to any third-party vendor. Hence, this control is not applicable.

8.3.10 - This requirement has been superseded by Requirement 8.3.10.1. Hence, this control is not applicable.

8.6.1, 8.6.2, 8.6.3 - Agile does not use shared authentication or access technologies. Hence, these controls are not applicable.

9.4.1, 9.4.1.1, 9.4.1.2, 9.4.2, 9.4.3, 9.4.4, 9.4.5, 9.4.5.1, 9.4.6, 9.4.7 - Agile does not backup cardholder data on any external media backup tapes, any other electronic media, or any hardcopy paper media. Hence, these controls are not applicable.

9.5.1, 9.5.1.1, 9.5.1.2, 9.5.1.2.1, 9.5.1.3 - Agile doesn't have any POI device in the scope. Hence, these controls are not applicable.

10.7.1 - This requirement is superseded by requirement 10.7.2. Hence, this control is not applicable.

11.3.1.3, 11.3.2.1 - No significant change occurred in the environment within the past 12 months. Hence, these controls are not applicable.

11.4.5, 11.4.6 - Agile included all components in scope. Hence, these controls are not applicable.

11.4.7 - Agile is not a multi-tenant service provider. Hence, this control is not applicable.

12.3.2 - No customized approach has been performed for targeted risk analysis.. Hence, this control is not applicable.

	12.5.3 – No significant change occurred in the environment within the past 12 months. Hence, these controls are not applicable. Appendix A1: Agile is not a shared hosting provider. Hence, these controls are not applicable. Appendix A2: Agile is not using SSL/Early TLS for Card-Present POS POI Terminal Connections. Hence, these controls are not applicable.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	Not Applicable

Section 2 Report on Compliance

(ROC Sections 1.2 and 1.3.2)

Date Assessment began: Note: <i>This is the first date that evidence was gathered, or observations were made.</i>	May 01, 2026
Date Assessment ended: Note: <i>This is the last date that evidence was gathered, or observations were made.</i>	August 27, 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 (*Date of Report as noted in the ROC* **October 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 <i>Agile Ticketing Solutions, LLC</i>. Environment 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 (<i>Service Provider Company Name</i>) 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 (<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. This option requires additional review from the entity to which this AOC will be submitted. <i>If selected, complete the following:</i> <table border="1"> <thead> <tr> <th>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> </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)

☒	The ROC was completed according to <i>PCI DSS</i> , Version <i>4.0.1</i> 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

Richard Steward

Signature of Service Provider Executive Officer ↑

Date: **October 05, 2026**

Service Provider Executive Officer Name: **Richard Steward**

Title: **CEO/ CTO**

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:

Signature of Lead QSA ↑

Date: **October 05, 2026**

Lead QSA Name: **Omar Akkad**

Signature of Duly Authorized Officer of QSA Company ↑

Date: **October 05, 2026**

Duly Authorized Officer Name: **Iftikhar Ahmed**

QSA Company: **ControlCase**

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:

Part 4. Action Plan for Non-Compliant Requirements

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

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

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

