



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: Ecwid, Inc.

Date of Report as noted in the Report on Compliance: November 25, 2025

Date Assessment Ended: November 25, 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: | Ecwid, Inc. |
| DBA (doing business as): | N/A |
| Company mailing address: | 460 Park Avenue South, 7th Floor, New York City, NY, 10016 |
| Company main website: | www.ecwid.com |
| Company contact name: | Kirill Kazakov |
| Company contact title: | SRE Manager |
| Contact phone number: | (410) 236-6551 |
| Contact e-mail address: | kirill.kazakov@lightspeedhq.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: | www.controlcase.com |
| Lead Assessor name: | Lead Qualified Security Assessor |
| Assessor phone number: | Gerald Drake III |
| Assessor e-mail address: | +1 703.483.6383 |



| | | | |
|--|--|---|--|
| Assessor certificate number: | | gdrake@controlcase.com | |
| 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-series E-commerce platform | |
| 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 checked="" 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: 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 Sections 2.1 and 3.1)

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

Ecwid, Inc. (Ecwid) provides a Software-as-a-Service (SaaS) shopping cart widget that can be embedded into customer's websites, blogs, or Facebook pages as well as a fully hosted e-commerce store-builder platform. The Ecwid widget, shopping cart, and hosted web sites is a cloud-based solution that has integrations with 40 plus online payment gateways.

Ecwid's web hosting and payment widget systems host the payment web forms only, which facilitate payments



| | |
|--|--|
| | <p>for customers to one of the integrated 40 plus supported payment gateways. Ecwid does not store, process, or transmit CHD within their environment. Ecwid provides payment facilitation services for their customers. CHD including full primary account number (PAN), expiration date, and CVV2, CVC2, CID, or CAV2 is transmitted directly from customer browsers to the merchant's (customer) selected payment processors via JavaScript inclusions or iFrames that are provided and maintained by the selected payment processors directly.</p> <p>CHD is never stored or processed by Ecwid's systems; only a token and last 4 digits of the PAN are received from the merchant processors for storage. Ecwid's merchants process all transactions using their own merchant IDs, with the merchants selecting whichever payment gateway/processor of their choosing and determining all settlement activities and chargebacks. All of which are handled directly between the merchants and their selected payment processor and/or acquiring bank.</p> |
| Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data. | <p>Ecwid does not store, process, or transmit CHD, but provides web hosting and payment applications that allow customer's to communicate directly with the payment processor and facilitate payments. These payment applications have the ability impact the security of cardholder data, so Ecwid has chosen to include the entirety of the payment application system within the scope of their assessment.</p> |
| Describe system components that could impact the security of account data. | <p>Ecwid never captures, stores, processes, or transmits cardholder data. As a payment facilitator (PayFac), Ecwid enables merchants (clients) to accept credit/debit cards for payments for e-commerce transactions. Ecwid only stores the information sent by the respective Payment processors such as last 4 digits or first 6 and last 4 digits of PAN, Expiry Date, and Authorization Code.</p> <p>Ecwid does not have any additional services that would impact on the security of account data.</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.

Ecwid, Inc. (Ecwid) provides a Software-as-a-Service (SaaS) shopping cart widget that can be embedded into customer’s websites, blogs, or Facebook pages as well as a fully hosted e-commerce store-builder platform. The Ecwid widget, shopping cart, and hosted web sites is a cloud-based solution that has integrations with 40 plus online payment gateways.

Ecwid’s Cardholder Data Environment (CDE) is hosted on the AWS Platform as a Service (PaaS) and virtual private clouds (VPC) across three availability zones in the AWS US East Region (us-east-1), two availability zones in Europe Central Region (eu-central-1), and three availability zones in Asia Pacific Sydney Region (ap-southeast-2). Ecwid does not store or process cardholder data within its hosting environment. Ecwid hosts payment web forms and widgets that are displayed to merchant customer’s browsers. These web forms contain either JavaScript inclusions or iFrames provided by the customer’s selected payment processor, and the CHD is transmitted from the client browsers directly to the payment processor, never passing through Ecwid’s systems.

CHD is never stored or processed by Ecwid’s systems; only a token and last 4 digits of the PAN are received from the merchant processors for storage. Ecwid’s merchants process all transactions using their own merchant IDs, with the merchants selecting whichever payment gateway/processor of their choosing and determining all settlement activities and chargebacks. All of which are handled directly between the merchants and their selected payment processor and/or acquiring bank.

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) |
|-------------------------|---|---|
| Cloud Hosting Providers | 3 | AWS Regions: <ul style="list-style-type: none">US-east-1 / United States (Virginia)Eu-central-1 / EU (Frankfurt)Ap-southeast-2 / Australia (Sydney) |



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. | N/A | N/A | N/A | N/A |

* 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 checked="" type="checkbox"/> Yes <input type="checkbox"/> No |

If Yes:

| Name of Service Provider: | Description of Services Provided: |
|---------------------------|-----------------------------------|
| Amazon Web Services | Cloud Hosting Provider |

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



Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment (ROC Section 1.8.1)

Indicate below all responses provided within each principal PCI DSS requirement.

For all requirements identified as either “Not Applicable” or “Not Tested,” complete the “Justification for Approach” table below.

Note: One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.

Name of Service Assessed: E-Series E-commerce Platform

| 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 type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Requirement 4: | <input 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

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

1.2.6 - The assessor noted that there are no insecure services, protocols and ports in the scoped environment. Hence this control is not applicable.

1.2.8 - Assessor noted that no routers are in scope, AWS security groups are used as a virtual firewall. Hence this control is not applicable.

| | |
|--|---|
| | <p>1.3.3 - The assessor noted that wireless networks are not utilized in the scoped environment. Hence this control is not applicable.</p> <p>1.4.4 - The assessor noted that cardholder data is not stored in the scoped environment. Hence this control is not applicable.</p> <p>2.2.5 - The assessor noted that insecure services, protocols, or daemons are not utilized in the scoped environment. Hence this control is not applicable.</p> <p>2.3.1 - Not Applicable. The assessor noted that there are no in-scope wireless networks.</p> <p>2.3.2 - The assessor noted that there are no in-scope wireless networks. Hence this control is not applicable.</p> <p>Requirement 3 –Assessor noted that Ecwid does not store CHD or SAD data in its scoped PCI DSS environment. Hence this control is not applicable.</p> <p>Requirement 4 - Not applicable. Assessor noted that Ecwid does not store CHD or SAD data in its scoped PCI DSS environment. Hence this control is not applicable.</p> <p>5.2.3 –There are no system components not at risk for malware for the current scoped environment. Hence this control is not applicable.</p> <p>5.2.3.1 –There are no system components not at risk for malware for the current scoped environment. Hence this control is not applicable.</p> <p>5.3.3 - Removable Electronic Media is not used in the scoped environment. Hence this control is not applicable.</p> <p>6.4.1 - As control 6.4.1 has been superseded by control 6.4.2. Hence this control is not applicable.</p> <p>6.5.2 - The assessor noted that there were no significant changes in Ecwid's scoped environment. Hence, this control is not applicable.</p> <p>7.2.6 - No cardholder data stored in the environment. Hence this control is not applicable.</p> <p>8.2.2 - The assessor noted that group, shared, or generic accounts are not created or used for any of the sampled systems. The assessor also noted that the shared authentication credentials are not permitted within the scope. Hence this control is not applicable.</p> |
|--|---|

8.2.3 - The assessed entity does not have any third parties that have remote access. Hence this control is not applicable.

8.2.7 - The assessor noted that no users outside of the assessed entity are allowed access to the servers; internal user access is the only permitted access. Hence this control is not applicable.

8.3.9 - The assessor noted that the passwords/passphrases are not the only factor used for access. MFA is in place to provide all access to the environment. Hence this control is not applicable.

8.3.10 - The assessor noted that the passwords/passphrases are not the only factor used for access. MFA is in place to provide all access to the environment. Hence this control is not applicable.

8.3.10.1 - The assessor noted that the passwords/passphrases are not the only factor used for access. MFA is in place to provide all access to the environment. Hence this control is not applicable.

8.6.1 - This control is NA because there are no systems or applications accounts that can be used for interactive login in the assessment scope. Hence this control is not applicable.

8.6.2 - This control is NA because there are no systems or applications accounts that can be used for interactive login in the assessment scope. Hence this control is not applicable.

8.6.3 - This control is NA because there are no systems or applications accounts that can be used for interactive login in the assessment scope. Hence this control is not applicable.

9.4.1 - The assessor reviewed that cardholder data is not being stored in any of the media. Hence, this control is not applicable. Hence this control is not applicable.

9.4.1.1 - The assessor reviewed that cardholder data is not being stored in any of the media. Hence, this control is not applicable.

9.4.1.2 - The assessor reviewed that cardholder data is not being stored in any of the media. Hence, this control is not applicable.

9.4.2 - The assessor reviewed that cardholder data is not being stored in any of the media. Hence, this control is not applicable.

9.4.3 - The assessor reviewed that cardholder data is not being stored in any of the media. Hence, this control is not applicable.

9.4.4 - The assessor reviewed that cardholder data is not being stored in any of the media. Hence, this control is not applicable.

9.4.5 - The assessor reviewed that cardholder data is not being stored in any of the media. Hence, this control is not applicable.

9.4.5.1 - The assessor reviewed that cardholder data is not being stored in any of the media. Hence, this control is not applicable.

9.4.6 - The assessor reviewed that cardholder data is not being stored in any of the media. Hence, this control is not applicable.

9.4.7 - The assessor reviewed that cardholder data is not being stored in any of the media. Hence, this control is not applicable.

9.5.1 – 9.5.1.3 - The assessor reviewed that no POI devices are used in the scoped environment. Hence, this control is not applicable.

10.2.1.1 - No cardholder data stored. Hence this control is not applicable.

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

11.3.1.3 - During the review of the scoped environment, the assessor noted that there were no significant changes in the environment during the current compliance cycle. Hence this control is not applicable.

11.3.2.1 - During the review of the scoped environment, the assessor noted that there were no significant changes in the environment during the current compliance cycle. Hence this control is not applicable.

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

12.3.2 - During the review of the scoped environment, the assessor noted that no customized approach was used. Hence this control is not applicable.



| | |
|---|---|
| | <p>12.5.3 - The assessor noted that there are no significant changes in the scoped environment. Hence this control is not applicable.</p> <p>Appendix A1 – Not applicable. Ecwid is not a multi-tenant service provider.</p> <p>Appendix A2 – Not applicable. No POI terminals in the scope of the assessment.</p> |
| For any Not Tested responses, identify which sub-requirements were not tested and the reason. | Not applicable. |



Section 2 Report on Compliance

(ROC Sections 1.2 and 1.3)

| | |
|---|---|
| Date Assessment began: <i>Note: This is the first date that evidence was gathered, or observations were made.</i> | 2025-06-24 |
| Date Assessment ended: <i>Note: This is the last date that evidence was gathered, or observations were made.</i> | 2025-11-25 |
| 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 (Date of Report as noted in the ROC November 25, 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 (Ecwid, Inc.) has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.

☐ **Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby (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:



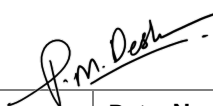

(Select all that apply)

| | |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | The ROC was completed according to <i>PCI DSS</i> , Version <i>4.0.1</i> 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

| | |
|---|---|
| DocuSigned by:  F2B9CC5E68FE478... | |
| Signature of Service Provider Executive Officer  | |
| Service Provider Executive Officer Name: Dan Micak | Title: Chief Legal Officer & Company Secretary |

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: |
|  | |
| Signature of Lead QSA  | Date: November 25, 2025 |
| Lead QSA Name: Gerald Drake III | |
|  | |
| Signature of Duly Authorized Officer of QSA Company  | Date: November 25, 2025 |
| Duly Authorized Officer Name: Pramod Deshmane | 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: | <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/