



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: Trend Micro, Inc. – TrendAI Vision One & Trend Cloud One – Endpoint & Workload Security

Date of Report as noted in the Report on Compliance: September 11, 2026

Date Assessment Ended: August 19, 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:	Trend Micro, Inc.
DBA (doing business as):	N/A
Company mailing address:	Irving 225 E John Carpenter Freeway, Suite 1500 Irving, TX 75062
Company main website:	www.trendmicro.com
Company contact name:	Steven Ryan
Company contact title:	Senior Program Manager, Compliance
Contact phone number:	+353 (21) 730-7300
Contact e-mail address:	steven_ryan@trendmicro.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):	N/A
--------------	-----

Qualified Security Assessor

Company name:	Kirkpatrick Price, Inc.
Company mailing address:	4235 Hillsboro Pike, Suite 300 Nashville, TN 37215
Company website:	www.kirkpatrickprice.com
Lead Assessor name:	Randy Bartels
Assessor phone number:	+1-800-977-3154
Assessor e-mail address:	r.bartels@kirkpatrickprice.com
Assessor certificate number:	QSA – 012-006

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: TrendAI Vision One and Trend Cloud One – Endpoint & Workload Security

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:	Customer On-Premise Products All Trend Micro, Inc. products which are implemented on the customer's premises are the direct responsibility of the customer for ongoing management. Such products, even if they integrate with TrendAI Vision One online services, are not included in the scope of this assessment. Cloud One Products Only the Trend Cloud One – Endpoint & Workload Security product was included, as noted above. All other Cloud One products were excluded.
----------------------------------	--

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:

Customer on-premise products should be assessed as part of each customer's PCI DSS assessment.

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.

Trend Cloud One – Endpoint & Workload Security:

Trend Cloud One – Endpoint & Workload Security is not directly involved in the processing, storage, or transmission of cardholder data (CHD). Trend Micro, Inc. offers security capabilities to its customers that customers may implement in their own cardholder data environment (CDE).

By design, the Trend Cloud One – Endpoint & Workload Security service sends only security events and agent operational information to the Trend Cloud One – Endpoint & Workload Security backend. Other than the security policies, security events, contact information (email addresses and names) and license data, no other customer data is stored in Trend Cloud One – Endpoint & Workload Security. Trend Micro, Inc. does not manage or store any customer sensitive card data.

TrendAI Vision One:

There are no components of the TrendAI Vision One platform that transmit, process, or store cardholder data on behalf of Trend Micro, Inc.'s customers.

The following TrendAI Vision One capabilities are potential sources for transmitting or storing cardholder data (CHD), but appropriate controls have been implemented to prevent this and are, therefore, not considered cardholder data environment (CDE) for this assessment:

- TrendAI Vision One Standard Endpoint Protection:
 - o Includes DLP features that can, among other data types, detect and prevent unauthorized actions with CHD. TrendAI Vision One Standard Endpoint Protection logs are filtered at the end point such that no more than the first six and last four digits are retained.
 - o DLP “Forensic Evidence Collection” features allow capturing all data elements from the DLP rule violation. A warning is presented when configuring this feature that it can result in capturing sensitive data and can impact PCI DSS compliance. Customer documentation has also been updated to identify the potential compliance impacts if enabled. It is required to disable this feature in order to use TrendAI Vision One in a PCI DSS-compliant manner.
- Zero Trust Secure Access (ZTSA) Private Access provides SASE-based virtual private network services between remote endpoints and a ZTSA Connector located in a customer's data center. Customer documentation advises users to enable the “Encrypt application traffic using unencrypted protocols” feature to ensure that end-to-end encryption is used between the endpoints and connectors for all clear-text protocols. This configuration is required for all applications using clear-text protocols in order to use TrendAI Vision One in a PCI DSS-compliant manner.
- ZTSA Internet Access (referred to as SWG in the TrendAI Vision One PCI DSS v4.0.1 Applicability Guide) provides a proxy-based service for ZTSA clients

	to access public internet sites. Internet traffic is decrypted in the backend and evaluated for policy and security issues. Customer documentation advises to implement rules which disable inspection and policy enforcement for traffic which could contain CHD. This ensures that the traffic is not decrypted by the SWG infrastructure and uses the original website's TLS session for end-to-end encryption. • The AI Application Security "AI Guard" and "AI Scanner" components could receive CHD as part of either prompts or responses. Customers documentation advises users to use the "on-prem / self-hosted" deployment option to process all prompts and responses. Additionally, assessor reviewed engineering documentation for these components to confirm that they employ: - o A client-side redaction feature to prevent CHD from being transmitted to the backend - o Active detection, rejection, and purge mechanisms to prevent any CHD that might enter the environment from being propagated further. These services are included in the scope of the assessment as they could impact the security a customer's CDE but are not considered CDE directly.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Trend Cloud One – Endpoint & Workload Security: Trend Cloud One – Endpoint & Workload Security services are not directly involved in the processing, storage, or transmission of cardholder data. Trend Cloud One – Endpoint & Workload Security secures servers (physical, virtual, or cloud workloads), networks, applications, containers, cloud storage, and infrastructure and helps to protect sensitive card data in customer's CDE through a wide range of security controls. Central management consoles provide the ability to easily drill down for details and allow for administrators to implement policies and manage security events. A console for the Trend Cloud One – Endpoint & Workload Security service is used as the management component of the system providing the ability to easily drill down for details and allow for administrators to implement policies for firewall rules, vulnerability shielding, system integrity, and alert generation, as well as assign administration roles for DSA. The DSA is a high-performance, small footprint, software component installed on a computer to provide protection. This component is the policy enforcement point for all protection functionality on customer cloud workloads using an agent. The nature of that protection depends on the rules and security settings that each DSA receives from the Trend Cloud One – Endpoint & Workload Security Console. Additionally, the DSA sends regular heartbeats and pushes security event logs and various other data points to the Trend Cloud One – Endpoint & Workload Security console.

	DSA is installed on a cloud workload belonging to the customer. This cloud workload could be involved in the processing, storage, or transmission of cardholder data. By design, the DSA sends only security events and agent operational information to the Trend Cloud One – Endpoint & Workload Security Console and none of this data contains customer card holder data. No other data flow exists. Through Workload Security, a protection policy is applied to these DSAs that generate security events which are aggregated in Workload Security. Workload Security servers are installed in the Trend Cloud One – Endpoint & Workload Security network, which connect to DSAs installed in the customer CDE. TrendAI Vision One: Trend Micro, Inc.'s customers use the TrendAI Vision One platform to manage the configurations and any detections or alerts as they are implemented in their own CDEs. As such, the TrendAI Vision One platform impacts the security of each customer's CDE. The TrendAI Vision One platform is a collection of individual services, each implemented separately using combinations of AWS and Microsoft Azure-based compute, storage, and network resources. Compute resources include virtual machines, container/orchestration services and server-less technologies (e.g. AWS Lambda). Storage resources include object-, block-, and database-based services. Networking resources include virtual networking capabilities native to each cloud provider. All the TrendAI Vision One services are then integrated into a common Service Platform, including public UI- and API-based access schemes.
Describe system components that could impact the security of account data.	Trend Cloud One – Endpoint & Workload Security: Trend Cloud One – Endpoint & Workload Security services are not directly involved in the processing, storage, or transmission of cardholder data. Trend Cloud One – Endpoint & Workload Security secures servers (physical, virtual, or cloud workloads), networks, applications, containers, cloud storage, and infrastructure and helps to protect sensitive card data in customer's CDE through a wide range of security controls. Central management consoles provide the ability to easily drill down for details and allow for administrators to implement policies and manage security events. A console for the Trend Cloud One – Endpoint & Workload Security service is used as the management component of the system providing the ability to easily drill down for details and allow for administrators to implement policies for firewall rules, vulnerability shielding, system integrity, and alert generation, as well as assign administration roles for DSA. The DSA is a high-performance, small footprint, software component installed on a computer to provide protection. This component is the policy enforcement point for all

protection functionality on customer cloud workloads using an agent. The nature of that protection depends on the rules and security settings that each DSA receives from the Trend Cloud One – Endpoint & Workload Security console. Additionally, the DSA sends regular heartbeats and pushes security event logs and various other data points to the Trend Cloud One – Endpoint & Workload Security console.

DSA is installed on a cloud workload belonging to the customer. This cloud workload could be involved in the processing, storage, or transmission of cardholder data. By design, the DSA sends only security events and agent operational information to the Trend Cloud One - Endpoint & Workload Security console and none of this data contains customer card holder data. No other data flow exists. Through Workload Security, a protection policy is applied to these DSAs that generate security events which are aggregated in Workload Security. Workload Security servers are installed in the Trend Cloud One - Endpoint & Workload Security network, which connect to DSAs installed in the customer CDE.

TrendAI Vision One:

Trend Micro, Inc.'s customers use the TrendAI Vision One platform to manage the configurations and any detections or alerts as they are implemented in their own CDEs. As such, the TrendAI Vision One platform impacts the security of each customer's CDE.

The TrendAI Vision One platform is a collection of individual services, each implemented separately using combinations of AWS and Microsoft Azure-based compute, storage, and network resources. Compute resources include virtual machines, container/orchestration services and server-less technologies (e.g. AWS Lambda). Storage resources include object-, block-, and database-based services. Networking resources include virtual networking capabilities native to each cloud provider.

All the TrendAI Vision One services are then integrated into a common Service Platform, including public UI- and API-based access schemes.

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.*

TrendAI Vision One:

TrendAI Vision One Platform is an integrated set of cybersecurity tools developed to provide organizations with a unified framework and UI for threat intelligence, detection, and mitigation. At its core, it utilizes a distributed architecture comprising endpoint agents, network sensors, and cloud-based analytics engines.

There are no components of the TrendAI Vision One platform that transmit, process, or store cardholder data on behalf of Trend Micro, Inc.'s customers.

The environment covered by this assessment includes AWS accounts and Microsoft Azure subscriptions, Docker containers for TrendAI Vision One services, virtual networking configurations, source code management tools, CI/CD pipeline components, application and infrastructure code, and security and infrastructure tooling for managing the in-scope environments.

Trend Cloud One – Endpoint & Workload Security :

Trend Cloud One – Endpoint & Workload Security is based on Trend Micro's Deep Security Agent (DSA) and provides an extensive set of security protections for server-based workloads, including:

- o Intrusion Detection and Prevention
- o Anti-Malware
- o Bidirectional Firewall
- o Web Reputation
- o Integrity Monitoring
- o Log Inspection
- o Events and Reports
- o Application Control

By design, the services do not send the content of sensitive data files to the Trend Cloud One – Endpoint & Workload Security management environment. The Deep Security Agent used in Cloud One Workload Security sends only security events and agent operational information to the Trend Cloud One – Endpoint & Workload Security Console and none of this data contains customer sensitive data.

	Trend Cloud One – Endpoint & Workload Security is entirely hosted within AWS using a combination of EC2, Docker containers w/ ECS, Lambda, RDS, DynamoDB, and S3. All administrative connections to the Trend Cloud One – Endpoint & Workload Security environment are only through AWS Systems Manager (SSM Agent) allowed only for privileged users.
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>
Cloud Hosting Provider – AWS (Trend Cloud One - Endpoint & Workload Security)	11	- Asia Pacific (Mumbai) - Asia Pacific (Singapore) - Asia Pacific (Sydney) - Asia Pacific (Tokyo) - Africa (Cape Town) - Canada (Montreal) - Europe (Frankfurt) - Europe (London) - Middle East (UAE) - US East (N. Virginia) - US East 2 (Ohio)
AWS and Microsoft Azure Regions (TrendAI Vision One)	21	AWS: - Asia Pacific (Mumbai) - Asia Pacific (Singapore) - Asia Pacific (Sydney) - Asia Pacific (Tokyo) - Asia Pacific (Yakarta) - Europe (Frankfurt) - Europe (London) - Middle East (UAE) - US East (N. Virginia) - Canada (Central) - Africa (Cape Town)

		Azure: • Australia East, New South Wales • Canada Central, Toronto • Central India, Pune • East US2, Virginia • Indonesia Central, Yakarta • Japan East, Tokyo • South Africa North, Johannesburg • Southeast Asia, Singapore • UAE North • UK South, London • West Europe, Netherlands

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
N/A	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:

• 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:
Trend Cloud One - Endpoint & Workload Security:	
Amazon Web Services	Cloud hosting
GitHub	Source code management and CI pipeline
TrendAI Vision One:	
Amazon Web Services	Cloud hosting
Microsoft Azure	Cloud hosting
GitHub	Source code management and CI pipeline

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: TrendAI Vision One and Trend Cloud One – Endpoint & Workload Security

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:	☒	☒	☐	☐	☐
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, 2.2.5: No insecure services, protocols, or ports are in use.

2.2.2: No system components used in TrendAI Vision One or Trend Cloud One - Endpoint & Workload Security include using any form of default user account.

2.2.3: All functions are implemented as micro-services, which necessitate implementing only one primary function per system component.

2.3.1 – 2.3.2, 11.2.2: There are no wireless networks in scope.

1.3.1 – 1.3.3, 1.4.4, 1.5.1, Requirement 3 & Requirement 4, 6.5.5, 7.2.6, 9.4.1 – 9.4.5.1, 10.2.1.1: The Trend Cloud One - Endpoint & Workload Security and TrendAI Vision One environments do not transmit, process, or store CHD.

5.2.3: There are not currently any system components for which this requirement applies.

6.4.1: This requirement has been superseded by 6.4.2.

6.4.3: There are no payment page scripts within the Trend Cloud One - Endpoint & Workload Security and TrendAI Vision One products for which this requirement could apply.

8.2.3: The organization does not maintain remote access to customer premises.

8.2.7: The organization does not allow service providers remote access.

8.3.10 – 8.3.10.1: Customers must implement SAML-based federation to meet PCI DSS requirements.

8.4.1 – 8.4.2, 11.4.6: Trend Micro, Inc. does not maintain a CDE.

8.6.1, 8.6.3: There are no system and application accounts.

9.5.1 – 9.5.1.3: The TrendAI Vision One and Trend Cloud One - Endpoint & Workload Security environments do not include any POI devices.

10.4.2 – 10.4.2.1: All other logs are related to application performance and are not in-scope.

10.7.1: This requirement has been superseded by 10.7.2 as of March 31, 2025.

11.3.1.3, 11.3.2.1: External scans are performed weekly with one scan being submitted monthly for ASV validation for delivery of an Attestation of Scan Compliance. As such, additional "significant change" scans are not needed for compliance with this requirement.

11.4.7 & A1: TrendAI Vision One and Trend Cloud One – Endpoint & Workload Security do not provide multi-tenant services as defined by PCI FAQ 1221 (dated 2025) for which this requirement is relevant.

11.6.1: The TrendAI Vision One and Trend Cloud One - Endpoint & Workload Security environments do not include any payment pages.

	A2: The TrendAI Vision One and Trend Cloud One - Endpoint & Workload Security environments do not include any POI devices.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	N/A

Section 2 Report on Compliance

(ROC Sections 1.2 and 1.3)

Date Assessment began: Note: <i>This is the first date that evidence was gathered, or observations were made.</i>	2026-4-21
Date Assessment ended: Note: <i>This is the last date that evidence was gathered, or observations were made.</i>	2026-8-19
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 2026-9-11)*.

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 Trend Micro, 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 <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> <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)*

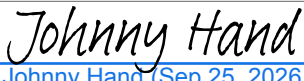
Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:

(Select all that apply)

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

 Johnny Hand (Sep 25, 2026 08:58:08 EDT)	
Signature of Service Provider Executive Officer ↑	Date: YYYY-MM-DD 2026-09-25
Service Provider Executive Officer Name: Johnny Hand	Title: Global CISO

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: 2026-09-11
Lead QSA Name: Randy Bartels	
	
Signature of Duly Authorized Officer of QSA Company ↑	Date: 2026-09-11
Duly Authorized Officer Name: Joseph Kirkpatrick	QSA Company: Kirkpatrick Price, 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:	☐ 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	☐	☐	

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/