



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. - Vision One

Date of Report as noted in the Report on Compliance: September 23, 2025

Date Assessment Ended: July 18, 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:	Trend Micro, Inc.
DBA (doing business as):	
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:	KirkpatrickPrice, 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:

Trend Vision One

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:	<p>Trend Cloud One</p> <p>Specifically for Trend Cloud One features which are integrated into Trend Vision One, the Trend Cloud One implementation of such features is covered by the Trend Cloud One PCI DSS assessment. However, the point at which such features are integrated into Trend Vision One is addressed by this assessment. This specifically includes the Trend Vision One-provided UI and/or API endpoints which can directly impact the security of customer CDEs but does not include the back-end system components which are responsible for performing the associated actions. Refer to the Trend Cloud One PCI DSS Attestation of Compliance for details.</p> <p>Customer On-Premise Products</p> <p>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 Trend Vision One online services, are not included in the scope of this assessment.</p>
----------------------------------	---

Type of service(s) not assessed:

Hosting Provider:	Managed Services:	Payment Processing:
<input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web-hosting services <input checked="" 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):	<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):	<input type="checkbox"/> POI / card present <input type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Account Management <input type="checkbox"/> Back-Office Services <input type="checkbox"/> Billing Management <input type="checkbox"/> Clearing and Settlement <input type="checkbox"/> Network Provider <input type="checkbox"/> Others (specify):	<input type="checkbox"/> Fraud and Chargeback <input type="checkbox"/> Issuer Processing <input type="checkbox"/> Loyalty Programs <input type="checkbox"/> Merchant Services	<input type="checkbox"/> Payment Gateway/Switch <input type="checkbox"/> Prepaid Services <input type="checkbox"/> Records Management <input type="checkbox"/> Tax/Government Payments

Provide a brief explanation why any checked services were not included in the Assessment:	Trend Cloud One capabilities are assessed separately.
---	---



Customer on-premise products should be assessed as part 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.

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

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

- Trend Vision One Standard Endpoint Protection:
 - o Includes DLP features that can, among other data types, detect and prevent unauthorized actions with CHD. Trend 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 Trend Vision One in a PCI DSS-compliant manner.
- Zero Trust Secure Access (ZTSA) Private Access provides SASE-based VPN 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 Trend Vision One in a PCI DSS-compliant manner.
- ZTSA Internet Access (referred to as SWG in the Trend 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.



	<ul style="list-style-type: none"> • 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.
<p>Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.</p>	<p>Trend Micro, Inc.'s customers use the Trend Vision One platform to manage the configurations and any detections or alerts as they are implemented in their own CDEs. As such, the Trend Vision One platform impacts the security of each customer's CDE.</p> <p>The Trend 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.</p> <p>All of the Trend Vision One services are then integrated into a common Service Platform, including public UI- and API-based access schemes</p>
<p>Describe system components that could impact the security of account data.</p>	<p>The Trend 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.</p> <p>All of the Trend Vision One services are then integrated into a common Service Platform, including public UI- and API-based access schemes.</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.*

Trend 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 Trend 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 Trend 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.

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>
AWS and Microsoft Azure Regions	7	US, Europe, Japan, Singapore, Australia, India, Dubai
Corporate Offices	0	No corporate office locations were deemed to be in-scope





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:

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

If Yes:

Name of Service Provider:	Description of Services Provided:
Amazon Web Services	Cloud hosting
Microsoft Azure	Cloud hosting

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: Trend Vision One

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 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 observed documented ports, services, and protocols for all in-scope Trend Vision One services, along with corresponding AWS inbound rules and outbound rules, API gateway authorizers, API model details, load balancer listeners and rules, and security groups, for in-scope Trend Vision One services and verified that no insecure services, protocols, or ports are in use.

1.3.1 – 1.3.3; 1.4.4; 1.5.1; 3.1.1 - 3.7.9; 4.1.1 - 4.2.2; 6.5.5; 7.2.6; 8.2.1; 9.4.1 - 9.4.5.1; 10.2.1.1 - The assessor interviewed personnel, reviewed documentation, and observed demonstrations of Trend Vision One and determined that environments do not transmit, process, or store CHD.

2.2.2 - Through interviews, review of inventories, and examination of system components configurations, assessor noted that no system components used in Trend Vision One include using any form of default user account

2.2.3 - Through interviews, review of inventories, review of system architecture diagrams, and examination of system components configurations, the assessor noted that all functions are implemented as micro-services, which necessitate implementing only one primary function per system component.

2.2.5 - The assessor observed documented ports, services, and protocols for all in-scope Trend Vision One services, along with corresponding AWS inbound rules and outbound rules, API gateway authorizers, API model details, load balancer listeners and rules, and security groups for in-scope Trend Vision One services and verified that no insecure services, protocols, or ports are in use.

2.3.2 - The assessor interviewed personnel and observed data flows and access methods for managing system component and verified that, in all cases, corporate office locations and related wireless networks are out of scope for this PCI DSS assessment.

5.2.3 - The assessor observed system configurations and Cloud One Workload Security console and verified that there are not currently any system components for which this requirement applies.

6.4.1 - This requirement is addressed via 6.4.2.

6.4.3 - The assessor examined workflows, interviewed personnel, and observed product demonstrations and verified that there are no payment page scripts within the product for which this requirement could apply.

8.2.3 - The assessor interviewed Jun-Hua Li, Distinguished Technologist, and determined that Trend Micro, Inc. does not maintain user credentials to login to their customer environments.

8.2.7 - The assessor interviewed Jake Shih, Senior Staff Engineer, and determined that no third parties are provided access to any part of the Trend Vision One platform. All support is provided exclusively through Trend Micro, Inc. personnel.



	<p>8.3.10; 8.3.10.1 - The assessor observed that in order to meet PCI DSS requirements, customers must implement SAML-based federation to meet PCI DSS requirements.</p> <p>8.4.2 - The assessor noted through interviews and observations that Trend Micro, Inc. does not maintain a cardholder data environment.</p> <p>8.6.1; 8.6.3 - The assessor observed user access lists and verified there are no system and application accounts.</p> <p>9.5.1 – 9.5.1.3 - The assessor interviewed personnel, reviewed documentation, and observed demonstrations of Trend Vision One and verified that the environments do not include any POI devices.</p> <p>10.4.2; 10.4.2.1 - The assessor interviewed personnel and reviewed technology stack design and verified that all other logs are related to application performance and are not in-scope.</p> <p>10.7.1 - This requirement has been superseded by 10.7.2 below</p> <p>11.3.1.3; 11.3.2; 11.3.2.1 - The assessor determined that 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.</p> <p>11.4.5; 11.4.6 - There is no CDE</p> <p>11.4.7 - The assessor interviewed relevant personnel and observed Trend Vision One product demonstrations and verified that Vision One does provide multi-tenant services for which this requirement is relevant.</p> <p>11.6.1 - The assessor interviewed personnel, reviewed documentation, and observed demonstrations of Trend Vision One and verified that the Trend Vision One environment does not include any payment pages.</p> <p>Appendix 1 - Assessor reviewed documentation, interviewed SMEs, and observed technical implementation data and verified that the Trend Vision One technology stack does not provide this level of access to customers.</p> <p>Appendix 2 - No SSL or early TLS present in the environment.</p>
<p>For any Not Tested responses, identify which sub-requirements were not tested and the reason.</p>	



Section 2 Report on Compliance

(ROC Sections 1.2 and 1.3)

Date Assessment began: <i>Note: This is the first date that evidence was gathered, or observations were made.</i>	April 21, 2025
Date Assessment ended: <i>Note: This is the last date that evidence was gathered, or observations were made.</i>	July 18, 2025
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any testing activities performed remotely?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No



Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated *(Date of Report as noted in the ROC September 23, 2025)*.

Indicate below whether a full or partial PCI DSS assessment was completed:

- Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.
- Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the ROC noted above, each signatory identified in any of Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document *(select one)*:

<input checked="" type="checkbox"/>	<p>Compliant: All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall COMPLIANT rating; thereby Trend Micro, Inc. has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.</p>								
<input type="checkbox"/>	<p>Non-Compliant: Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall NON-COMPLIANT rating; thereby <i>(Service Provider Company Name)</i> has not demonstrated compliance with PCI DSS requirements.</p> <p>Target Date for Compliance: YYYY-MM-DD</p> <p>An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.</p>								
<input type="checkbox"/>	<p>Compliant but with Legal exception: One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall COMPLIANT BUT WITH LEGAL EXCEPTION rating; thereby <i>(Service Provider Company Name)</i> has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction.</p> <p>This option requires additional review from the entity to which this AOC will be submitted.</p> <p><i>If selected, complete the following:</i></p> <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <thead> <tr> <th style="width: 35%;">Affected Requirement</th> <th>Details of how legal constraint prevents requirement from being met</th> </tr> </thead> <tbody> <tr> <td style="height: 20px;"> </td> <td> </td> </tr> <tr> <td style="height: 20px;"> </td> <td> </td> </tr> <tr> <td style="height: 20px;"> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement from being met						
Affected Requirement	Details of how legal constraint prevents requirement from being met								



Part 3. PCI DSS Validation (continued)

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:

(Select all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to <i>PCI DSS</i> , Version 4.0.1 and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
<input checked="" type="checkbox"/>	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

DocuSigned by:

Jonah Peng

77F84D67E0C34EF...

Signature of Service Provider Executive Officer ↑	Date: September 23, 2025
Service Provider Executive Officer Name:	Title: 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:

Randy Bartels

Signature of Lead QSA ↑	Date: September 23, 2025
Lead QSA Name: Randy Bartels	

Joseph Kirkpatrick

Signature of Duly Authorized Officer of QSA Company ↑	Date: September 23, 2025
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	<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/