corecommerce

Payment Card Industry (PCI) Data Security Standard

Attestation of Compliance

Prepared for:

CoreCommerce LLC

Date:

04 December 2025

A-LIGN

A-LIGN.COM

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: CoreCommerce LLC

Date of Report as noted in the Report on Compliance: 04 December 2025

Date Assessment Ended: 04 December 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:	CoreCommerce LLC
DBA (doing business as):	Not Applicable.
Company mailing address:	102 Woodmont Blvd, Suite 125, Nashville, Tennessee 37205 USA
Company main website:	https://www.corecommerce.com
Company contact name:	Kris Graffagnino
Company contact title:	CTO
Contact phone number:	+1 (615) 550-5523
Contact e-mail address:	info@corecommerce.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:	A-LIGN Compliance and Security, Inc. dba A-LIGN
Company mailing address:	400 N Ashley Drive, Suite 1325, Tampa, Florida 33602 USA
Company website:	https://www.A-LIGN.com
Lead Assessor name:	Ernesta Burke
Assessor phone number:	+1 (888) 702-5446
Assessor e-mail address:	ernesta.burke@A-LIGN.com
Assessor certificate number:	QSA, 206-370

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:	Payment Services: CoreCommerce Shopping Cart Services, Payment Processing Services, Virtual Terminal, Hosted Payments Page, PCC (point-click-care) application for payment card processing for a long-term healthcare facility

Type of service(s) assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☒ Applications / software	☐ Systems security services	☐ POI / card present
☐ Hardware	☐ IT support	☒ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web-hosting services		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service Provider		
☐ Other Hosting (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:	Not Applicable.

Type of service(s) not assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POI / card present
☐ Hardware	☐ IT support	☐ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web-hosting services		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service Provider		
☐ Other Hosting (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. All services provided by CoreCommerce were included within the scope of this 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.	CoreCommerce provides secure online payment services that allow customers to make card payments through its shopping platform and related applications. The shopping cart feature enables customers to enter their card details on a secure CoreCommerce checkout page to complete purchases. This information is used only to authorize the transaction and is removed immediately after authorization. For record-keeping, only limited details-such as the last four digits of the card number-are retained.

	CoreGateway supports payment processing through secure connections and uses tokenization to protect card data. When customers choose to store their card information for recurring payments or refunds, the data is encrypted and kept in a secure environment. These measures help reduce risk and ensure compliance with industry standards. The Payment Care Center (PCC) application is designed for healthcare facilities to manage payments, including one-time and recurring options. When recurring payments are set up, card details are stored securely in an encrypted vault. Only partial card information is kept for audit purposes. All services follow strict security practices and comply with PCI DSS requirements to protect cardholder data (CHD).
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	CoreCommerce provides online store hosting and payment processing services. It allows businesses to run their websites and connect to a secure payment system for handling card transactions. The payment system works separately from the websites and does not directly manage or access them. When processing payments, CoreCommerce offers options like authorizing a payment, completing it later, canceling, refunding, or making a sale. If a customer requests, the payment system can securely store card details to make future purchases easier. In these cases, the system uses the full card number to handle refunds, chargebacks, and repeat transactions. Card details are kept in an encrypted database and are never shown on the website or shared with customers. Customer service and sales teams cannot see this information. Only a small group of system administrators can access it, and even then, under strict controls and monitoring. These activities-such as payment processing, storing card data, and administrator access-are critical because they affect the security of account information. To protect this data, CoreCommerce uses encryption, limits access by role, and separates duties to reduce risk and meet industry security standards.
Describe system components that could impact the security of account data.	CoreCommerce utilizes AWS systems to run its environment. AWS ECR is utilized to host system components in their environments. Multiple supporting systems are in place to protect the AWS environment, such as Network Security Controls, VPN with MFA, and IDS systems. Databases are hosted within these parameters to store the business' critical data components.

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.*	CoreCommerce only accepts credit cards through a custom e-commerce application, as a service to its customers. CoreCommerce employees have no direct connections into the CDE. CoreCommerce support staff must connect with a VPN and multi-factor authentication. The cardholder data environment exists within a CoreCommerce Amazon AWS environment. Assessor reviewed the following components as part of the assessment: - Network Segments - Databases - Web Servers - Multi-Factor VPN - Anti-Virus - FIM - IDS - E-Commerce Web Application and payment gateway - CoreCommerce Managed AWS Security Groups - AWS ECR
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)
Example: Data centers	*3*	*Boston, MA, USA*
Datacenter - AWS	2	Ashburn, VA, United States (US-East-1, US-East-2)
Corporate HQ	1	Nashville, TN, United States

Part 2. Executive Summary *(continued)*

Part 2e. PCI SSC Validated Products and Solutions (ROC Section 3.3)

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions*?

☐ Yes ☒ No

Provide the following information regarding each item the entity uses from PCI SSC's Lists of Validated Products and Solutions:

Name of PCI SSC validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which Product or Solution Was Validated	PCI SSC Listing Reference Number	Expiry Date of Listing
Not Applicable.	Not Applicable.	Not Applicable.	Not Applicable.	Not Applicable.

* For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components, appearing on the PCI SSC website (www.pcisecuritystandards.org) (for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions), and Mobile Payments on COTS (MPoC) products.

Part 2. Executive Summary *(continued)*

Part 2f. Third-Party Service Providers (ROC Section 4.4)

For the services being validated, does the entity have relationships with one or more third-party service providers that:

• 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:
Amazon Web Services	On-demand cloud computing platform that hosts the entity application/services
Ixopay, Inc.	The entity is responsible for managing the firewall rulesets and internal network architecture
Fortra Alert Logic	This entity is responsible for tokenizing credit card info so that it is not stored in the product databases

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: Payment Services: CoreCommerce Shopping Cart Services, Payment Processing Services, Virtual Terminal, Hosted Payments Page, PCC (point-click-care) application for payment card processing for a long-term healthcare facility

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: Not Applicable. No insecure services, daemons, or protocols were identified. 1.3.3: Not Applicable. No wireless networks connecting to the CDE or transmitting CHD are present. 2.2.5: Not Applicable. No insecure services, daemons, or protocols were identified. 2.3.1 - 2.3.2: Not Applicable. No wireless networks connecting to the CDE or transmitting CHD are present. 3.3.2: Not Applicable. SAD is stored only within memory prior to authorization and is overwritten/flushed after the authorization process is finished. 3.3.3: Not Applicable. The entity is not an issuer. 3.4.2: Not Applicable. The entity does not store CHD. 3.5.1.1: Not Applicable. No PAN hashes were present in the environment. 3.5.1.2 - 3.5.1.3: Not Applicable. Disk encryption is not used for encrypting CHD. 3.6.1 - 3.6.1.2: Not Applicable. Account data was not stored in an encrypted format. 3.6.1.3: Not Applicable. Manual clear-text cryptographic key-management operations are not used. 3.6.1.4 - 3.7.8: Not Applicable. No cryptographic keys are utilized in the environment at this time. 3.7.9: Not Applicable. No cryptographic keys were shared with customers. 4.2.1.2: Not Applicable. No wireless networks connecting to the CDE or transmitting CHD are present. 4.2.2: Not Applicable. End-user messaging technologies are not used for CHD transmission. 5.2.3 - 5.2.3.1: Not Applicable. All in-scope system components were considered to be at risk for malware. 5.3.2.1: Not Applicable. Continuous behavioral analysis of systems and processes is performed by the anti-malware solution. 6.4.1: Not Applicable. This requirement is not applicable after 31 March 2025. 6.4.2: Not Applicable. No web interfaces or web applications are present. 6.4.3: Not Applicable. The entity doesn't utilize any payment pages. 6.5.2: Not Applicable. No significant changes have occurred in the past 12 months. 8.2.2: Not Applicable. Group, generic, or other shared accounts were not present on any in-scope system component. 8.2.3: Not Applicable. The entity does not have access to customer premises. 8.3.9: Not Applicable. All authentication into in-scope systems requires MFA.

	8.3.10: Not Applicable. This requirement is not applicable after 31 March 2025. 8.6.1 - 8.6.2: Not Applicable. Interactive login was not possible or permitted within the in-scope environment. 9.2.2: Not Applicable. AWS does not make any network jacks publicly available within its service offering. 9.4.1: Not Applicable. Cardholder data was not handled or stored in any media. 9.4.1.1 - 9.4.1.2: Not Applicable. No offline media backups containing CHD were utilized. 9.4.2 - 9.4.7: Not Applicable. Cardholder data was not handled or stored on any removable media or paper. 9.5.1 - 9.5.1.3: Not Applicable. The entity does not utilize POS/POI within the environment. 10.4.2.1: Not Applicable. All audit logs were analyzed by an automated mechanism, including logs from connected to systems. 10.7.1: Not Applicable. This requirement is not applicable after 31 March 2025. 11.3.1.3, 11.3.2.1: Not Applicable. No significant changes have occurred in the past 12 months. 11.4.7: Not Applicable. The entity is not a multi-tenant service provider. 12.3.2: Not Applicable. No requirements have been met with the customized approach. A1.1.1 - A1.2.3: Not Applicable. The entity is not a multi-tenant service provider. A2.1.1 - A2.1.3: Not Applicable. The entity did not utilize POS/POI terminals.
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: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*	04 June 2025
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	04 December 2025
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 04 December 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 **CoreCommerce LLC** 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: 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)

☒	The ROC was completed according to *PCI DSS*, 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.

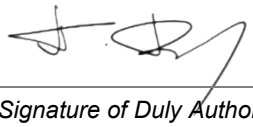
Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↗	Date: 10 February 2026
Service Provider Executive Officer Name: Kris Graffagnino	Title: CTO

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:	☒ QSA performed testing procedures.
	☐ QSA provided other assistance. If selected, describe all role(s) performed: Not Applicable.

Signature of Lead QSA ↗	Date: 04 December 2025
Lead QSA Name: Ernesta Burke	



Signature of Duly Authorized Officer of QSA Company ↗	Date: 10 February 2026
Duly Authorized Officer Name: Petar Besalev, EVP Cybersecurity and Compliance Services	QSA Company: A-LIGN

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/