Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for
Onsite Assessments - Service Providers

Version 3.2.1

Jan 2020

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

Part 1. Service Provider and Qualified Security Assessor Information						

Part 1a. Service Provider Organization Information						
Company Name:	CoreCommerce L.L.C.		DBA (doing business as):	Not Applicable.		
Contact Name:	Mike Hunt		Title:	IT Director		
Telephone:	+91 (814) 182-1734		E-mail:	micheal@devdigital.com		
Business Address:	801 2nd Avenue N		City:	Nashville		
State/Province:	TN	Country:	USA		Zip:	37201
URL:	www.corecommerce.com					

Part 1b. Qualified Security Assessor Company Information (if applicable)						
Company Name:	A-LIGN Compliance and Security, Inc. dba A-LIGN					
Lead QSA Contact Name:	John Bowman		Title:	Senior Consultant		
Telephone:	1-888-702-5446		E-mail:	john.bowman@a-lign.com		
Business Address:	400 N. Ashley Drive, Suite 1325		City:	Tampa		
State/Province:	Florida	Country:	United States		Zip:	33602
URL:	www.a-lign.com					

Part 2. Executive Summary
Part 2a. Scope Verification
Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) assessed:	Payment Services: CoreCommerce Omnichannel Payment Solutions

Type of service(s) assessed:

Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
☒ Applications / software	☐ Systems security services	☐ POS / 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		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Shared Hosting 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): Not Applicable.		

Note*: These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.*

Part 2a. Scope Verification *(continued)*
Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) not assessed:	Not Applicable.

Type of service(s) not assessed:

Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POS / 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		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Shared Hosting 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): Not Applicable.

Provide a brief explanation why any checked services were not included in the assessment:	Not Applicable.

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	CoreCommerce L.L.C (CoreCommerce) provides a web application platform to conduct e-commerce called CoreCommerce. CoreCommerce provides a payment gateway service to multiple payment gateways via the CoreCommerce software service. CoreCommerce is classified as Level 1 service provider.
	CoreCommerce accepts MasterCard, Visa, American Express, and Discover cards as payment. CoreCommerce uses only card-not-present transactions for its customers over a secured connection using HTTPS: TLS v1.2 SHA256.
	Card data enters the CoreCommerce application site when a customer selects the items they want to purchase and "checkout". Customers enter their PAN, name, expiration date, card security code (CVV2, CVC2, CID) on a CoreCommerce hosted checkout form. The cardholder data is stored in VRAM and held until the authorization has completed, at which time it is securely deleted from VRAM space.
	After a transaction has been authorized the payment processor sends back the "transaction id" to capture the funds, and the last four digits of the PAN, card holder name, and expiration date. The data is written to a MySQL database.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Not Applicable.

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility:	Number of facilities of this type	Location(s) of facility (city, country):
Example: Retail outlets	*3*	*Boston, MA, USA*
Corporate Headquarters	1	Brentwood, TN USA
AWS	1	Multiple AWS locations

Part 2d. Payment Applications

Does the organization use one or more Payment Applications? ☒ Yes   ☐ No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
CoreCommerce	9.3.5.1	In-House Developed	☐ Yes ☒ No	

Part 2e. Description of Environment

Provide a **_high-level_** description of the environment covered by this assessment.	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 dial up VPN (username/password) and Google Authenticator multi-factor authentication. The cardholder data environment exists within a CoreCommerce Amazon AWS VPC utilizing EC2 instances.
For example: • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	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 CoreCommerce Managed AWS Security Groups

Does your business use network segmentation to affect the scope of your PCI DSS environment? *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*	☒ Yes ☐ No

Part 2f. Third-Party Service Providers

Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated?	☐ Yes ☒ No

If Yes:

Name of QIR Company:	Not Applicable.
QIR Individual Name:	Not Applicable.
Description of services provided by QIR:	Not Applicable.

Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?	☒ Yes ☐ No

If Yes:

Name of service provider:	Description of services provided:
AWS	Co-Location Hosting
2Checkout	Payment Processor
Asia Pay	Payment Processor
ANZ eGate	Payment Processor
Amazon Pay	Payment Processor
Bambora (Formerly Beanstream)	Payment Processor
Braintree	Payment Processor
CardConnect	Payment Processor
Cybersource	Payment Processor
Elavon	Payment Processor
eProcessing Network	Payment Processor
EVO Merchant Services	Payment Processor
e-WAY	Payment Processor
First Data (FIRSTDATA)	Payment Processor
First Data (LINKPOINT)	Payment Processor
HSBC	Payment Processor
Intuit	Payment Processor
iPay Gateway	Payment Processor
Merchant eSolutions	Payment Processor
Moneris (US +CA)	Payment Processor
NMI	Payment Processor
PagSeguro	Payment Processor
Pay Junction	Payment Processor

Payment Express	Payment Processor
PayPal Web Payments Pro	Payment Processor
Plug N Pay	Payment Processor
PSiGate	Payment Processor
Quantun Gateway	Payment Processor
Sage Moto	Payment Processor
Sage Pay (Protx)	Payment Processor
Sage Payments	Payment Processor
Skipjack	Payment Processor
Stripe	Payment Processor
TSYS	Payment Processor
USA EPay	Payment Processor
Worldpay	Payment Processor

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

Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** - The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the ROC
- **Partial** - One or more sub-requirements of that requirement were marked as "Not Tested" or "Not Applicable" in the ROC
- **None** - All sub-requirements of that requirement were marked as "Not Tested" and/or "Not Applicable" in the ROC

For all requirements identified as either "Partial" or "None," provide details in the "Justification for Approach" column, including:

- Details of specific sub-requirements that were marked as either "Not Tested" and/or "Not Applicable" in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

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 Omnichannel Payment Solutions

PCI DSS Requirement	Details of Requirements Assessed			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	☐	☒	☐	1.2.2 - Not Applicable. There are no routers present in the CoreCommerce CDE. 1.2.3 - Not Applicable. There are no wireless networks that connect to or are located within the CoreCommerce CDE.
Requirement 2:	☐	☒	☐	2.1.1 - Not Applicable. There are no wireless environments connected to the CDE or transmitting cardholder data. 2.6 - Not Applicable. CoreCommerce is not a shared hosting provider.
Requirement 3:	☐	☒	☐	3.2.a - Not Applicable. CoreCommerce is not an issuer. 3.4.1 - Not Applicable. Disk encryption is not used. 3.5.x - 3.6.8.b - Not Applicable. No cryptographic solution was in use that required key management.
Requirement 4:	☐	☒	☐	4.1.1 - Not Applicable. No wireless devices were in scope.
Requirement 5:	☒	☐	☐	
Requirement 6:	☒	☐	☐	
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	8.1.5 - Not Applicable. CoreCommerce does not allow third parties or vendors access to the CDE.

				8.7.x - Not Applicable. Cardholder data is never stored. Only the last 4 digits are retained.
Requirement 9:	☐	☒	☐	9.5.1 - 9.6.x - Not Applicable. No cardholder data is stored. No backup media is in scope. 9.7.x - Not Applicable. No cardholder data is stored. No backup media is in scope. 9.8.x - Not Applicable. CoreCommerce does not record cardholder data onto any hardcopy materials. 9.9.x - Not Applicable. There are no card swipe or POS devices in the CoreCommerce environment.
Requirement 10:	☒	☐	☐	
Requirement 11:	☒	☐	☐	
Requirement 12:	☒	☐	☐	
Appendix A1:	☐	☐	☒	Not Applicable. CoreCommerce is not a shared hosting provider.
Appendix A2:	☐	☐	☒	Not Applicable. CoreCommerce does not have POS or POI devices.

Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	24 January 2020
Have compensating controls been used to meet any requirement in the ROC?	☐ Yes ☒ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes ☐ No
Were any requirements not tested?	☐ Yes ☒ No
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated 24 January 2020.

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

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby CoreCommerce L.L.C. has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *(Service Provider Company Name)* has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with the payment brand(s) before completing Part 4.*
☐	**Compliant but with Legal exception:** One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *3.2.1*, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
☐	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☒	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☒	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

Part 3a. Acknowledgement of Status (continued)

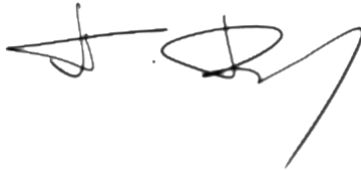| ☒	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor: Alert Logic.

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	*Date:* **January 30, 2020**
Service Provider Executive Officer Name: **Peter Marcum**	*Title:* **Managing Partner**

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	*The assessor provided PCI DSS advisory and assessment services, which included observation of controls, interviews with key personnel, and review of policies and procedures.*

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* **January 30, 2020**
Duly Authorized Officer Name: **Petar Besalev, Senior VP Cybersecurity and Privacy Services'**	*QSA Company:* **A-LIGN**

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	Not Applicable.

---

[1] Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

[2] The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

[3] Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with the applicable payment brand(s) before completing Part 4.

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 a firewall configuration to protect cardholder data	☒	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	
3	Protect stored cardholder data	☒	☐	
4	Encrypt transmission of cardholder data across open, public networks	☒	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	
6	Develop and maintain secure systems and applications	☒	☐	
7	Restrict access to cardholder data by business need to know	☒	☐	
8	Identify and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholder data	☒	☐	
10	Track and monitor all access to network resources and cardholder data	☒	☐	
11	Regularly test security systems and processes	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	☐	☐	Not Applicable.
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☐	☐	Not Applicable.