Docusign Envelope ID: 8AA8D095-AFEB-445F-9673-8AA06E35D33E



Payment Card Industry
Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0.1

Publication Date: August 2024

Docusign Envelope ID: 8AA8D095-AFEB-445F-9673-8AA06E35D33E

PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: Lightspeed Commerce, Inc.

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

Date Assessment Ended: November 25, 2025

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 8AA8D095-AFEB-445F-9673-8AA06E35D33E

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:	Lightspeed Commerce, Inc.
DBA (doing business as):	Lightspeed POS USA Inc. Lightspeed Payments USA Inc. Lightspeed Commerce USA Inc Lightspeed POS Belgium BVBA Lightspeed Netherlands BV Lightspeed POS Germany GmbH Lightspeed Commerce CH SA Lightspeed POS UK Limited iKentoo SASU Kounta Pty Ltd. Vend, Inc. Vend Pty Limited. Vend Limited. Vend Software UK Limited Chronogolf, Inc. Lightspeed NuORDER Inc. Alcmene S.à r.l. Luxembourg NuORDER Pty Ltd
Company mailing address:	700 St-Antoine Est, Suite 300, Montreal, Quebec, Canada, H2Y 1A6
Company main website:	www.lightspeedhq.com
Company contact name:	Karl Larson
Company contact title:	Vice President, Security
Contact phone number:	+ 1-866-932-1801
Contact e-mail address:	karl.larson@lightspeedhq.com

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 8AA8D095-AFEB-445F-9673-8AA06E35D33E

Part 1b. Assessor (ROC Section 1.1)

Provide the following information for all assessors involved in the Assessment. If there was no assessor for a given assessor type, enter Not Applicable.

PCI SSC Internal Security Assessor(s)	
ISA name(s):	Not applicable.
Qualified Security Assessor	
Company name:	ControlCase
Company mailing address:	Fifty West Corporate Center 3975 Fair Ridge Drive, Suite D T25s, Fairfax, VA 22033
Company website:	www.controlcase.com
Lead Assessor name:	Lead Qualified Security Assessor
Assessor phone number:	Gerald Drake III
Assessor e-mail address:	+1 703.483.6383
Assessor certificate number:	gdrake@controlcase.com

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the Assessment (select all that apply):

Name of service(s) assessed:	Lightspeed e-commerce and retail Card Tokenization Service (CTS); Lightspeed Cloud Point of Sale Application

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		Payment Facilitator for cloud-based point-of-sale (POS) Software application for retail, hospitality, e-commerce merchants and provides an e-commerce payment gateway.
☐ 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

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 8AA8D095-AFEB-445F-9673-8AA06E35D33E

☐ Clearing and Settlement	☒ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☒ Others (specify): Payment Facilitator and card tokenization service		

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.*

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 8AA8D095-AFEB-445F-9673-8AA06E35D33E

Part 2. Executive Summary *(continued)*

Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were NOT INCLUDED in the scope of the Assessment (select all that apply):

Name of service(s) not assessed:	None.

Type of service(s) not assessed:

Hosting Provider:	**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.

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.	Lightspeed Commerce, Inc. (herein referred to as 'Lightspeed') is a PCI DSS Level 1 Service Provider. Lightspeed is a cloud-based application and software-as-a-service (SaaS) development company and Payment facilitator (PayFac), which provides a cloud-based point-of-sale (POS) Software applications for retail, hospitality, e-commerce merchants and provides an e-commerce payment gateway. Lightspeed does not store, process, and/or transmit CHD within their Cloud POS solution but acts as a pass

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 8AA8D095-AFEB-445F-9673-8AA06E35D33E

through to route customer transactions to the appropriate payment gateway.

Lightspeed does not store, process, and/or transmit cardholder data (CHD) in any form. However, the Lightspeed Cloud POS application impacts the security of cardholders in one of the following methods. Hence, the scope of this assessment is limited to the following:

Cloud-based POS – Retail, Hospitality, E-commerce (C, R, and X-series)

Includes AWS-hosted containerized web applications that either integrate with POS devices (iPads) that transmit cardholder directly to payment processors or use an iFrame that redirects to payment pages hosted by PCI-validated payment processors.

Cloud-based POS – Restaurant (K, L, O, G)

The Lightspeed Hospitality POS K, L, O, and G-series infrastructure support merchants (Lightspeed customers) that deploy P2PE POI terminals or PTS compliant magnetic stripe readers at the customer premises. In this implementation, Lightspeed only receives encrypted CHD and is unable to decrypt the CHD, and has no access to the decryption keys of the POI terminals nor the transaction itself.

The Lightspeed Hospitality POS K, L, O, and G-series infrastructure have been excluded from scope as they support merchants (Lightspeed customers) that deploy P2PE POI terminals or PTS compliant magnetic stripe readers deployed at the customer premises. Lightspeed K and L series support P2PE compliant devices and PTS compliant magnetic stripe readers. Lightspeed O and G series support P2PE compliant devices only. The POI terminals (P2PE compliant) and PTS compliant magnetic stripe readers employ encryption technology that comes preconfigured from the payment gateways directly. Lightspeed has no ability to decrypt the CHD, nor do they have any access to the decryption keys.

E-commerce (CTS Platform)

Includes the JavaScript object stored on a Google Cloud bucket. JavaScript is used to call an iFrame within the e-commerce web application to generate a payment page. Cardholder data is transmitted directly from the client's browser to the PCI-validated payment processor.

NuOrder

Lightspeed B2B essentially functions as an e-commerce (eCom) platform. All payment processing follows a Card Not Present (CNP) flow) For NuORDER transactions, all cardholder data is transmitted directly to payment

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 8AA8D095-AFEB-445F-9673-8AA06E35D33E

	processors or use an iFrame that redirects to payment pages hosted by PCI-validated payment processors. **Golf** Lightspeed Golf offers a comprehensive golf course management software solution aimed at optimizing operations and enhancing the overall experience for golf course staff and players. Its features are tailored to meet the specific needs of golf course management, including reservation management, payment processing, sales and inventory management, member management, and customer service. Lightspeed Golf exclusively supports Card Not Present scenarios. While it does not facilitate Card Present transactions on its own, integration with Lightspeed Retail POS (R-Series) or Lightspeed Restaurant POS (L-Series) is required for such transactions. For CNP transactions, all cardholder data is transmitted directly to payment processors or use an iFrame that redirects to payment pages hosted by PCI-validated payment processors. Lightspeed accepts Visa, MasterCard, Discover, American Express, China UnionPay, JCB, Diners Club.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Lightspeed does not store, process, and/or transmit cardholder data (CHD) in any form. However, the Lightspeed Cloud POS application impacts the security of cardholders in one of the following methods. Hence, the scope of this assessment is limited to the following: **Cloud-based POS – Retail, Hospitality, E-commerce (C, R, and X-series)** Includes AWS-hosted containerized web applications that either integrate with POS devices (iPads) that transmit cardholder directly to payment processors or use an iFrame that redirects to payment pages hosted by PCI-validated payment processors. **Cloud-based POS – Restaurant (K, L, O, G)** The Lightspeed Hospitality POS K, L, O, and G-series infrastructure support merchants (Lightspeed customers) that deploy P2PE POI terminals or PTS compliant magnetic stripe readers at the customer premises. In this implementation, Lightspeed only receives encrypted CHD and is unable to decrypt the CHD, and has no access to the decryption keys of the POI terminals nor the transaction itself. The Lightspeed Hospitality POS K, L, O, and G-series infrastructure have been excluded from scope as they

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 8AA8D095-AFEB-445F-9673-8AA06E35D33E

	support merchants (Lightspeed customers) that deploy P2PE POI terminals or PTS compliant magnetic stripe readers deployed at the customer premises. Lightspeed K and L series support P2PE compliant devices and PTS compliant magnetic stripe readers. Lightspeed O and G series support P2PE compliant devices only. The POI terminals (P2PE compliant) and PTS compliant magnetic stripe readers employ encryption technology that comes preconfigured from the payment gateways directly. Lightspeed has no ability to decrypt the CHD, nor do they have any access to the decryption keys. **E-commerce (CTS Platform)** Includes the JavaScript object stored on a Google Cloud bucket. JavaScript is used to call an iFrame within the e-commerce web application to generate a payment page. Cardholder data is transmitted directly from the client's browser to the PCI-validated payment processor. **NuOrder** Lightspeed B2B essentially functions as an e-commerce (eCom) platform. All payment processing follows a Card Not Present (CNP) flow) For NuORDER transactions, all cardholder data is transmitted directly to payment processors or use an iFrame that redirects to payment pages hosted by PCI-validated payment processors. **Golf** Lightspeed Golf offers a comprehensive golf course management software solution aimed at optimizing operations and enhancing the overall experience for golf course staff and players. Its features are tailored to meet the specific needs of golf course management, including reservation management, payment processing, sales and inventory management, member management, and customer service. Lightspeed Golf exclusively supports Card Not Present scenarios. While it does not facilitate Card Present transactions on its own, integration with Lightspeed Retail POS (R-Series) or Lightspeed Restaurant POS (L-Series) is required for such transactions. For CNP transactions, all cardholder data is transmitted directly to payment processors or use an iFrame that redirects to payment pages hosted by PCI-validated payment processors.
Describe system components that could impact the security of account data.	Lightspeed does not store cardholder data in any form. Lightspeed systems do not receive, process, or transmit cardholder data. As a payment facilitator (PayFac), Lightspeed enables clients to accept credit/debit cards for payments for retail, e-commerce,

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 8AA8D095-AFEB-445F-9673-8AA06E35D33E

	and hospitality transactions. Their service provides their client's in-depth analysis into their day-to-day business. LightSpeed only stores the information sent by the respective Payment processors such as last 4 digits or first 6 and last 4 digits of PAN, Expiry Date, Authorization Code

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 8AA8D095-AFEB-445F-9673-8AA06E35D33E

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.*	Lightspeed is a PCI DSS Level 1 Service Provider. Lightspeed is a cloud-based application and software-as-a-service (SaaS) development company and Payment facilitator (PayFac), which provides a cloud-based point-of-sale (POS) Software applications for retail, hospitality, e-commerce merchants and provides an e-commerce payment gateway. Lightspeed does not store, process, and/or transmit CHD within their Cloud POS solution but acts as a pass through to route customer transactions to the appropriate payment gateway. However, the Lightspeed Cloud POS application impacts the security of cardholders in one of the following methods. Hence, the scope of this assessment is limited to the following: **Cloud-based POS – Retail, Hospitality, E-commerce (C, R, and X-series)** Includes AWS-hosted containerized web applications that either integrate with POS devices (iPads) that transmit cardholder directly to payment processors or use an iFrame that redirects to payment pages hosted by PCI-validated payment processors. **Cloud-based POS – Restaurant (K, L, O, G)** The Lightspeed Hospitality POS K, L, O, and G-series infrastructure support merchants (Lightspeed customers) that deploy P2PE POI terminals or PTS compliant magnetic stripe readers at the customer premises. In this implementation, Lightspeed only receives encrypted CHD and is unable to decrypt the CHD and has no access to the decryption keys of the POI terminals nor the transaction itself. The Lightspeed Hospitality POS K, L, O, and G-series infrastructure have been excluded from scope as they support merchants (Lightspeed customers) that deploy P2PE POI terminals or PTS compliant magnetic stripe readers deployed at the customer premises. Lightspeed K and L series support P2PE compliant devices and PTS compliant magnetic stripe readers. Lightspeed O and G series support P2PE compliant devices only. The POI terminals (P2PE compliant) and

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 8AA8D095-AFEB-445F-9673-8AA06E35D33E

	PTS compliant magnetic stripe readers employ encryption technology that comes preconfigured from the payment gateways directly. Lightspeed has no ability to decrypt the CHD, nor do they have any access to the decryption keys. **E-commerce (CTS Platform)** Includes the JavaScript object stored on a Google Cloud bucket. JavaScript is used to call an iFrame within the e-commerce web application to generate a payment page. Cardholder data is transmitted directly from the client's browser to the PCI-validated payment processor. **NuOrder** Lightspeed B2B essentially functions as an e-commerce (eCom) platform. All payment processing follows a Card Not Present (CNP) flow.) For NuORDER transactions, all cardholder data is transmitted directly to payment processors or use an iFrame that redirects to payment pages hosted by PCI-validated payment processors. **Golf** Lightspeed Golf offers a comprehensive golf course management software solution aimed at optimizing operations and enhancing the overall experience for golf course staff and players. Its features are tailored to meet the specific needs of golf course management, including reservation management, payment processing, sales and inventory management, member management, and customer service. Lightspeed Golf exclusively supports Card Not Present scenarios. While it does not facilitate Card Present transactions on its own, integration with Lightspeed Retail POS (R-Series) or Lightspeed Restaurant POS (L-Series) is required for such transactions. For CNP transactions, all cardholder data is transmitted directly to payment processors or use an iFrame that redirects to payment pages hosted by PCI-validated payment processors.
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

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 8AA8D095-AFEB-445F-9673-8AA06E35D33E

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*
Cloud Hosting Providers	6	AWS Regions: • Lightspeed Retail POS (R-Series): Amazon Web Services (us-east-1) • Lightspeed Retail POS (X-Series): Amazon Web Services (us-west-2) • Lightspeed Restaurant POS (K-Series): (eu-west-1) • Lightspeed Restaurant POS (O-Series): Amazon Web Services (ap-northeast-1, ap-southeast-2) • Lightspeed Restaurant POS (L-Series): Amazon Web Services (us-east-1, eu-west-1, eu-central-1, ap-southeast-1, ap-southeast-2) • Lightspeed Restaurant POS (G-Series): Amazon Web Services (eu-central-1)
Cloud Hosting Providers	4	GCP • US multi-regional GCS Buckets • Lightspeed eCom (C-Series): (europe-west-4, us-east-4) • Lightspeed Golf: (us-east-1) • Lightspeed B2B (NuORDER): (us-west-1)

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 8AA8D095-AFEB-445F-9673-8AA06E35D33E

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.

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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	Cloud Hosting Provider
Google Cloud Platform	Cloud Hosting Provider
Cayan	Payment Processor
BridgePay	Payment Processor
Moneris	Payment Processor
Stripe	Payment Processor
Worldline	Payment Processor
WorldPay	Payment Processor
Adyen	Payment Processor
Windcave	Payment Processor
Zettle	Payment Processor
Sumup	Payment Processor
First Data	Payment Processor
Yoco	Payment Processor
Block, Inc. – Square Inc.	Payment Processor
Paymentsense	Payment Processor
Payroc	Payment Processor
Mollie	Payment Processor
Spreedly	Payment Processor

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

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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: Lightspeed e-commerce and retail Card Tokenization Service (CTS); Lightspeed Cloud Point of Sale Application

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. The assessor noted that there are no insecure services, protocols and ports in the scoped environment.** **1.3.3 - Not Applicable. The assessor noted that wireless networks are not utilized in the scoped environment.**

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 8AA8D095-AFEB-445F-9673-8AA06E35D33E

	1.4.4 - Not Applicable. The assessor noted that cardholder data is not stored in the scoped environment. **2.2.5 - Not Applicable. The assessor noted that insecure services, protocols, or daemons are not utilized in the scoped environment.** **2.3.1 - Not Applicable. The assessor noted that there are no in-scope wireless networks.** **2.3.2 - Not Applicable. The assessor noted that there are no in-scope wireless networks.** **Requirement 3 – Not applicable. The assessor confirmed Lightspeed does not store any cardholder data in their environment.** **Requirement 4 - Not Applicable. Lightspeed does not store, process, and/or transmit CHD within their Cloud POS solution.** **5.2.3 – Not applicable. There are no system components at risk for malware for the current scoped environment.** **5.2.3.1 – Not applicable. There are no system components at risk for malware for the current scoped environment.** **5.3.3 - Not Applicable. Removable Electronic Media is not used in the scoped environment.** **6.4.1 - Not applicable. Requirement 6.4.1 has been superseded by requirement 6.4.2.** **6.5.2 - The assessor noted that there were no significant changes in Lightspeed Commerce, Inc.'s scoped environment. Hence, this control is not applicable.** **6.5.5 - The assessor noted that no cardholder data is stored, processed, or transmitted in the Lightspeed Commerce, Inc. scoped environment. Therefore, this control is not applicable.** **6.5.6 - The assessor noted that no cardholder data is stored, processed, or transmitted in the Lightspeed Commerce, Inc. scoped environment. Therefore, this control is not applicable.** **7.2.6 - Not Applicable. No cardholder data stored in the environment.** **8.2.2 - The assessor noted that group, shared, or generic accounts are not created or used for any of the sampled systems. The assessor also noted**

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 8AA8D095-AFEB-445F-9673-8AA06E35D33E

	that the shared authentication credentials are not permitted within the scope. **8.2.3 - Not Applicable. The assessed entity does not have any third parties that have remote access.** **8.2.7 - Not Applicable. The assessor noted that no users outside of the assessed entity are allowed access to the servers; internal user access is the only permitted access.** **8.3.9 - The assessor noted that the passwords/passphrases are not the only factor used for access. MFA is in place to provide all access to the environment. Hence this control is not applicable.** **8.3.10 - The assessor noted that the passwords/passphrases are not the only factor used for access. MFA is in place to provide all access to the environment. Hence this control is not applicable.** **8.3.10.1 - The assessor noted that the passwords/passphrases are not the only factor used for access. MFA is in place to provide all access to the environment. Hence this control is not applicable.** **8.6.1 - Not Applicable. This requirement is NA because there are no systems or applications accounts that can be used for interactive login in the assessment scope.** **8.6.2 - Not Applicable. This requirement is NA because there are no systems or applications accounts that can be used for interactive login in the assessment scope.** **8.6.3 - Not Applicable. This requirement is NA because there are no systems or applications accounts that can be used for interactive login in the assessment scope.** **9.4.1 - Not Applicable. The assessor reviewed that cardholder data is not being stored in any of the media. Hence, this control is not applicable.** **9.4.1.1 - Not Applicable. The assessor reviewed that cardholder data is not being stored in any of the media. Hence, this control is not applicable.** **9.4.1.2 - Not Applicable. The assessor reviewed that cardholder data is not being stored in any of the media. Hence, this control is not applicable.**

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 8AA8D095-AFEB-445F-9673-8AA06E35D33E

	9.4.2 - Not Applicable. The assessor reviewed that cardholder data is not being stored in any of the media. Hence, this control is not applicable. **9.4.3 - Not Applicable. The assessor reviewed that cardholder data is not being stored in any of the media. Hence, this control is not applicable.** **9.4.4 - Not Applicable. The assessor reviewed that cardholder data is not being stored in any of the media. Hence, this control is not applicable.** **9.4.5 - Not Applicable. The assessor reviewed that cardholder data is not being stored in any of the media. Hence, this control is not applicable.** **9.4.5.1 - Not Applicable. The assessor reviewed that cardholder data is not being stored in any of the media. Hence, this control is not applicable.** **9.4.6 - Not Applicable. The assessor reviewed that cardholder data is not being stored in any of the media. Hence, this control is not applicable.** **9.4.7 - Not Applicable. The assessor reviewed that cardholder data is not being stored in any of the media. Hence, this control is not applicable.** **9.5.1 – 9.5.1.3 - Not Applicable. The assessor reviewed that no POI devices are used in the scoped environment. Hence, this control is not applicable.** **10.2.1.1 - Not Applicable. No cardholder data stored.** **10.7.1 - Not Applicable. This requirement is superseded by Requirement 10.7.2.** **11.3.1.3 - Not Applicable. During the review of the scoped environment, the assessor noted that there were no significant changes in the environment during the current compliance cycle.** **11.3.2.1 - Not Applicable. During the review of the scoped environment, the assessor noted that there were no significant changes in the environment during the current compliance cycle.** **11.4.5 - Not Applicable. The assessor noted that segmentation is not used in the scoped environment.** **11.4.6 - Not Applicable. The assessor noted that segmentation is not used in the scoped environment.**

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 8AA8D095-AFEB-445F-9673-8AA06E35D33E

	11.4.7 - Not Applicable. Lightspeed Commerce is not a multi-tenant service provider. **12.3.2 - Not Applicable. During the review of the scoped environment, the assessor noted that no customized approach was used.** **Appendix A1 – Not applicable. Lightspeed is not a multi-tenant service provider.** **Appendix A2 – Not applicable. No POI terminals in the scope of the assessment.**
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	**Not applicable.**

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 8AA8D095-AFEB-445F-9673-8AA06E35D33E

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.*	2025-06-24
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	2025-11-25
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

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 8AA8D095-AFEB-445F-9673-8AA06E35D33E

Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated *(Date of Report as noted in the ROC* **November 25, 2025***)*.

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

☒ **Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.

☐ **Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

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

☒	**Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT** rating; thereby (*Lightspeed Commerce, Inc.)* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby *(Service Provider Company Name)* has not demonstrated compliance with PCI DSS requirements. **Target Date** for Compliance: *YYYY-MM-DD* An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.
☐	**Compliant but with Legal exception:** One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Service Provider Company Name)* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction. This option requires additional review from the entity to which this AOC will be submitted. *If selected, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement from being met

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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

DocuSigned by:
Dan Micak
F2B9CC5E68FE478...

Signature of Service Provider Executive Officer ↑	
Service Provider Executive Officer Name: **Dan Micak**	Title: **Chief Legal Officer & Company Secretary**

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:	☒ QSA performed testing procedures.
	☐ QSA provided other assistance. If selected, describe all role(s) performed:

Signature of Lead QSA ↑	Date: **November 25, 2025**
Lead QSA Name: **Gerald Drake III**	
Signature of Duly Authorized Officer of QSA Company ↑	Date: **November 25, 2025**
Duly Authorized Officer Name: **Pramod Deshmane**	QSA Company: **ControlCase**

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:	☐ ISA(s) performed testing procedures.
	☐ ISA(s) provided other assistance. If selected, describe all role(s) performed:

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: 8AA8D095-AFEB-445F-9673-8AA06E35D33E

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/

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.