



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: Upserve by Lightspeed

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

Date Assessment Ended: November 25, 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:	Upserve by Lightspeed
DBA (doing business as):	Lightspeed Restaurant
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

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:	Gerald Drake III
Assessor phone number:	+1 703.483.6383
Assessor e-mail address:	gdrake@controlcase.com
Assessor certificate number:	203-017



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:		Upserve by Lightspeed	
Type of service(s) assessed:			
Hosting Provider: <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 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):	Managed Services: <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):	Payment Processing: <input checked="" type="checkbox"/> POI / card present <input checked="" type="checkbox"/> Internet / e-commerce <input checked="" type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):	
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input checked="" type="checkbox"/> Payment Gateway/Switch	
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services	
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management	
<input type="checkbox"/> Clearing and Settlement	<input checked="" type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments	
<input type="checkbox"/> Network Provider			
<input type="checkbox"/> 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: None.

Type of service(s) not assessed:

Hosting Provider:

- ☐ Applications / software
- ☐ Hardware
- ☐ Infrastructure / Network
- ☐ Physical space (co-location)
- ☐ Storage
- ☐ Web-hosting services
- ☐ Security services
- ☐ 3-D Secure Hosting Provider
- ☐ Multi-Tenant Service Provider
- ☐ Other Hosting (specify):

Managed Services:

- ☐ Systems security services
- ☐ IT support
- ☐ Physical security
- ☐ Terminal Management System
- ☐ Other services (specify):

Payment Processing:

- ☐ POI / card present
- ☐ Internet / e-commerce
- ☐ MOTO / Call Center
- ☐ ATM
- ☐ Other processing (specify):

☐ Account Management

☐ Fraud and Chargeback

☐ Payment Gateway/Switch

☐ Back-Office Services

☐ Issuer Processing

☐ Prepaid Services

☐ Billing Management

☐ Loyalty Programs

☐ Records Management

☐ Clearing and Settlement

☐ Merchant Services

☐ Tax/Government Payments

☐ Network Provider

☐ Others (specify):

Provide a brief explanation why any checked services were not included in the Assessment:

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.

Upserve by Lightspeed is a PCI DSS Level 1 Service Provider. Upserve by 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 application (Ubergateway which is a payment gateway for Upserve POS and Upserve Online Ordering) for restaurant merchants and provides an e-commerce payment gateway. Upserve by Lightspeed accepts card-present transactions through Upserve by Lightspeed-configured

and merchant-owned fixed and handheld POS devices. Additionally, Upserve by Lightspeed processes card-not-present transactions for eCommerce platforms, providing payment gateway and customer loyalty services to merchant clients. The payment acceptance channels and flows are as follows.

Card-Present:

For card-present swipe, dip, NFC, and manual entry transactions initiated at a merchant-owned Upserve by Lightspeed POS (not in-scope), customer payment card data (full track data) is captured at the POS/POI terminal and immediately encrypted via AES 256-bit encryption. CHD is transmitted over the Internet using TLS v1.2 with strong cipher suites

(TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) to the AWS-hosted Upserve by Lightspeed CDE.

Encrypted inbound transaction packets are directly routed to the Tokenizer application/database to be decrypted, and then re-encrypted with AES 256-bit minimum tokenized keys. The encrypted PAN (AES-256), PAN token, and expiry date are stored in an encrypted AES 256-bit minimum MySQL database.

The Tokenizer application creates a token of the full track data and temporarily stores it in VRAM. The Upserve by Lightspeed Ubergateway uses the Detokenization application to retrieve and decrypt the CHD, holding the full track data, PAN, and expiry in VRAM, and sends it outbound to the payment gateway processor Adyen or First Data. All data is sent over the Internet via a secure connection using TLS v1.2 with strong cipher suites

(TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) for processing, and an authorization code is returned.

After the transaction is complete the token, full track and track equivalent data, PAN, and expiry date are securely deleted from VRAM, and the track token is securely deleted from storage by the Tokenizer application.

Card-not-Present:

For card-not-present online orders, a customer initiates a transaction by logging in at

<https://www.lightspeedhq.com> and providing the Upserve by Lightspeed HQ application full PAN, expiry, and card verification value/code. CHD, from the end-user web browser, is securely transmitted over the Internet, using TLS v1.2 with strong cipher suites

(TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) to Lightspeed implemented load balancers hosted on AWS. From the load balancers, CHD is routed to the Tokenizer application where a token is created for the full PAN. The Ubergateway(Upserve by Lightspeed



	<p>payment gateway) holds the token, PAN, and expiry in virtual RAM (VRAM) and sends the transaction data outbound to the payment processor (First Data or Adyen) for payment authorization, using TLS v1.2 with strong cipher suites (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256). Adyen or First Data returns an authorization code once the transaction is approved. CHD is then securely deleted from VRAM by the Tokenizer application.</p> <p>Loyalty Program:</p> <p>CHD is also received from merchant processing reports. These reports are retrieved via SFTP from Adyen or First Data. PANs are encrypted (AES 256-bit minimum) and tokenized. The token is associated with the purchase details from the processing report to provide transaction analytics to merchants. A token, and therefore a PAN, can also be associated with a guest for loyalty program purposes.</p>
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	<p>Upserve by Lightspeed accepts card-present and card-not-present through merchant owned Upserve by Lightspeed POS devices and through eCommerce platform for the purposes of providing payment gateway and customer loyalty services to merchant clients. Payment is processed through Adyen or First Data via upstream transmission of CHD token, PAN, and expiry date. Also, Upserve by Lightspeed receives PAN online directly from customers for the purposes of establishing customer loyalty accounts.</p> <p>Upserve by Lightspeed is a Level 1 service provider that delivers services to its customers. The following third-party service providers and payment processors provide significant services for Upserve by Lightspeed:</p> <p>Amazon AWS:</p> <p>Upserve by Lightspeed cardholder data environment is hosted on AWS using EC2, VPC, ECS, Security Groups, OpenSearch, and other services. AWS maintains a current PCI DSS v4.0.1 AOC and Responsibility Matrix.</p> <p>First Data and Adyen:</p> <p>Upserve by Lightspeed utilizes Adyen and First Data as a payment processing service provider. Adyen and First Data maintain a current PCI DSS v4.0.1 AOC</p>
Describe system components that could impact the security of account data.	<p>Upserve by Lightspeed is a Level 1 service provider. Upserve by 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</p>



	<p>application (Ubergateway which is a payment gateway for Upserve POS and Upserve Online Ordering) for restaurant merchants and provides an e-commerce payment gateway. The following third-party service providers and payment processors perform significant services for Upserve by Lightspeed:</p> <p>Amazon AWS:</p> <p>Upserve by Lightspeed cardholder data environment is hosted on AWS using EC2, VPC, ECS, Security Groups, OpenSearch, and other services. AWS maintains a current PCI DSS v4.0.1 AOC and Responsibility Matrix.</p> <p>First Data and Adyen:</p> <p>Upserve by Lightspeed utilizes Adyen and First Data as a payment processing service provider. Adyen and First Data maintain a current PCI DSS v4.0.1 AOC and Responsibility Matrix.</p>
--	--



Part 2. Executive Summary (continued)

Part 2c. Description of Payment Card Environment

<p>Provide a high-level description of the environment covered by this Assessment.</p> <p><i>For example:</i></p> <ul style="list-style-type: none">• <i>Connections into and out of the cardholder data environment (CDE).</i>• <i>Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.</i>• <i>System components that could impact the security of account data.</i>	<p>Upserve by Lightspeed is a PCI DSS Level 1 Service Provider. Upserve by 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 application (Ubergateway which is a payment gateway for Upserve POS and Upserve Online Ordering) for restaurant merchants within the United States and provides an e-commerce payment gateway.</p> <p>The Upserve by Lightspeed platform is made up of restaurant-specific point of sale (POS) software, payments, and analytics, online ordering, loyalty, inventory, and marketing tools. Hardware devices include iPad and Android handheld devices, ID Tech and MagTek card swipe devices and are provided to merchant customers by Upserve by Lightspeed that have Upserve by Lightspeed encryption keys to send cardholder data (CHD) to Adyen or First Data, as a payment processor.</p> <p>Upserve by Lightspeed accepts card-present transactions through Upserve by Lightspeed-configured and merchant-owned fixed and handheld POS devices. Additionally, Upserve by Lightspeed processes card-not-present transactions for eCommerce platforms, providing payment gateway and customer loyalty services to merchant clients. The payment acceptance channels and flows are as follows.</p> <p>Card-Present:</p> <ul style="list-style-type: none">• For card-present swipe, dip, NFC, and manual entry transactions initiated at a merchant-owned Upserve by Lightspeed POS (not in-scope), customer payment card data (full track data) is captured at the POS/POI terminal and immediately encrypted via AES 256-bit minimum encryption. CHD is transmitted over the Internet using TLS v1.2 with strong cipher suites to the AWS-hosted Lightspeed CDE. Encrypted inbound transaction packets are directly routed to the Tokenizer application/database to be decrypted, and then re-encrypted with AES 256-bit
--	---

minimum tokenized keys. The encrypted PAN (AES-256 minimum), token, and expiry date are stored in an encrypted MySQL database.

- The Tokenizer application creates a token of the full track data and temporarily stores it in VRAM. The Upserve by Lightspeed Ubergateway uses the Detokenization application to retrieve token and detokenize it, holding the full track, PAN, and expiry in VRAM, and sends it outbound to the payment gateway processor Adyen or First Data. All data is sent over the Internet via a secure connection using TLS v1.2 with strong cipher suites for processing, and an authorization code is returned. After the transaction is complete the track token, full track and track equivalent data, PAN, and expiry date are securely deleted from VRAM, and the track token is securely deleted from storage by the Tokenizer application.

Card-not-Present:

- For card-not-present online orders, a customer initiates a transaction by logging in at <https://www.lightspeedhq.com> and providing the Upserve by Lightspeed HQ application full PAN, expiry, and card verification value/code. CHD, from the end-user web browser, is securely transmitted over the Internet, using TLS v1.2 with strong cipher suites to Upserve by Lightspeed hosted on AWS. CHD is routed to the Tokenizer application where a token is created for the full PAN. The Ubergateway, Upserve payment gateway, holds the token, PAN, and expiry in VRAM and sends the transaction data outbound to the payment processor (First Data) for payment authorization, using TLS v1.2 with strong cipher suites. Adyen or First Data returns an authorization code once the transaction is approved. CHD is then securely deleted from VRAM by the Tokenizer application.

Loyalty Program:

- CHD is also received from merchant processing reports. These reports are retrieved via SFTP from Adyen or First Data. PANs are encrypted (AES 256-bit



	minimum) and tokenized. The token is associated with the purchase details from the processing report to provide transaction analytics to merchants. A token, and therefore a PAN, can also be associated with a guest for loyalty program purposes.
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)	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> 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
Amazon Web Services (AWS) Cloud Hosting Provider	1	Northern Virginia, USA (us-east-1)



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.	N/A	N/A	N/A	N/A

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



Part 2. Executive Summary (continued)

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

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

• Store, process, or transmit account data on the entity’s behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage))	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> 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)	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
• Could impact the security of the entity’s CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

If Yes:

Name of Service Provider:	Description of Services Provided:
Amazon Web Services	Cloud Hosting Provider
First Data	Payment Processor
Adyen, N. V.	Payment Processor

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: Lightspeed Payment Gateway

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 checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input checked="" 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 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 checked="" 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 - Not Applicable. The assessor noted that there are no insecure services, protocols and ports in the scoped environment.

1.2.8 – Not applicable. There are no server-based technologies used for implementing routing or firewall rules.

1.3.3 - Not Applicable. The assessor noted that there is no wireless network in scope.

2.2.5 - Not Applicable. The assessor reviewed and found that no insecure services, protocols, or daemons are utilized within the scope of this assessment.

2.3.1 - Not Applicable. The assessor noted that no wireless networks are present within the Upserve by Lightspeed PCI DSS-scoped environment.

2.3.2 - Not Applicable. The assessor noted that no wireless networks are present within the Upserve by Lightspeed PCI DSS-scoped environment.

3.3.2 - Not Applicable. The assessor noted that there is no authorization process, and SAD is not stored in the scoped environment.

3.3.3 - Not Applicable. The assessor noted that assessed entity is not an issuer.

3.4.1 - Not Applicable. The assessor noted that the full PAN is not displayed anywhere in the scoped environment.

3.4.2 - Not Applicable. The assessor noted that the full PAN is not displayed anywhere in the scoped environment.

3.5.1.2 – Not applicable. The assessor reviewed the scoped environment and noted that no removable media was used for disk encryption.

3.5.1.3 – Not applicable. The assessor reviewed the scoped environment and noted that no removable media was used for disk encryption.

3.6.1.3 - Not Applicable. The assessor noted that clear text cryptographic key components are not used.

3.7.2 - The assessor noted that the keys are not distributed. Hence, this control is not applicable.

3.7.6 - Not Applicable. The assessor noted that manual cleartext cryptographic key-management operations are not in place in the scoped environment.

4.2.1.1 - Not Applicable. This control is marked as not applicable; no inventory of trusted keys and certificates is maintained.

4.2.1.2 - Not Applicable. As Upserve by Lightspeed PCI DSS does not have Wireless Access Points installed in its Card Processing Environment.

4.2.2 - Not Applicable. The assessed entity does not transmit Cardholder Data (CHD) over end-user messaging technologies such as an email, Chat, or Short Message Service (SMS), to block any emails where PAN is included.

	<p>5.2.3 - Not applicable. As Antivirus is installed in all system components, there are no system components that are not at risk for malware.</p> <p>5.2.3.1 - Not applicable. As Antivirus is installed in all system components, there are no system components that are not at risk for malware.</p> <p>5.3.3 - Not applicable. Removable Electronic Media is not used in the scoped environment.</p> <p>6.4.1 - Not Applicable, this requirement is superseded by Requirement 6.4.2.</p> <p>6.5.2 - Not Applicable. The assessor reviewed and noted that this control is not applicable as there is no significant change.</p> <p>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 that the shared authentication credentials are not permitted within the scope.</p> <p>8.2.3 - Not Applicable. The assessor noted that the assessed entity does not implement or maintain access to customer environments.</p> <p>8.2.7 - Not Applicable. The assessor noted that the assessed entity does not allow Third-party Service Providers access to CDE. Therefore, no third-party accounts are enabled within the security groups.</p> <p>8.3.9 - Not Applicable. The assessor noted that the passwords/ passphrases are not the only factor used for access. MFA is in place for all access to the environment.</p> <p>8.3.10 - Not Applicable, this requirement is superseded by Requirement 8.3.10.1.</p> <p>8.3.10.1 - Not Applicable. The assessor noted that the passwords/ passphrases are not the only factor used for access. MFA is in place for all access to the environment.</p> <p>8.6.1 - Not Applicable. There are no systems or applications accounts that can be used for interactive login in the assessment scope.</p> <p>8.6.2 - Not Applicable. There are no systems or applications accounts that can be used for interactive login in the assessment scope.</p> <p>8.6.3 - Not Applicable. There are no systems or applications accounts that can be used for interactive login in the assessment scope.</p> <p>9.4.1 – Not applicable. The assessor noted that cardholder data is not stored in media devices in the scoped environment.</p>
--	--

	<p>9.4.1.1 - Not applicable. The assessor noted that cardholder data is not stored in media devices in the scoped environment.</p> <p>9.4.1.2 - Not applicable. The assessor noted that cardholder data is not stored in media devices in the scoped environment.</p> <p>9.4.2 - Not applicable. The assessor noted that cardholder data is not stored in media devices in the scoped environment.</p> <p>9.4.3 - Not applicable. The assessor noted that cardholder data is not stored in media devices in the scoped environment.</p> <p>9.4.4 - Not applicable. The assessor noted that cardholder data is not stored in media devices in the scoped environment.</p> <p>9.4.5 - Not applicable. The assessor noted that cardholder data is not stored in media devices in the scoped environment.</p> <p>9.4.5.1 - Not applicable. The assessor noted that cardholder data is not stored in media devices in the scoped environment.</p> <p>9.4.6 - Not applicable. The assessor noted that cardholder data is not stored in media devices in the scoped environment.</p> <p>9.4.7 - Not applicable. The assessor noted that cardholder data is not stored in media devices in the scoped environment.</p> <p>9.5.1 - Not Applicable. The assessor reviewed that no POI device was used for the scoped environment.</p> <p>9.5.1.1 - Not Applicable. The assessor reviewed that no POI device was used for the scoped environment.</p> <p>9.5.1.2 - Not Applicable. The assessor reviewed that no POI device was used for the scoped environment.</p> <p>9.5.1.2.1 - Not Applicable. The assessor reviewed that no POI device was used for the scoped environment.</p> <p>9.5.1.3 - Not Applicable. The assessor reviewed that no POI device was used for the scoped environment.</p> <p>10.7.1 - The Assessor noted that this requirement is superseded by requirement 10.7.2.</p> <p>11.3.1.3 - Not Applicable. The assessor noted that there is no significant change in the environment.</p> <p>11.3.2.1 - Not Applicable. The assessor noted that there is no significant change in the environment.</p>
--	--



	<p>11.4.7 - Not Applicable. Lightspeed Commerce Payment Gateway PCI DSS is not a multi-tenant service provider.</p> <p>12.3.2 - Not Applicable. No customized approach has been performed for targeted risk analysis.</p> <p>12.5.3 - Not Applicable. As there have been no significant changes in the past few years.</p> <p>Appendix A1 – Not applicable. Upserve by Lightspeed is not a multi-tenant service provider.</p> <p>Appendix A2 – Not applicable. Upserve by Lightspeed does not have any in-scope or connected POI terminals.</p>
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: <i>Note: This is the first date that evidence was gathered, or observations were made.</i>	2025-06-24
Date Assessment ended: <i>Note: This is the last date that evidence was gathered, or observations were made.</i>	2025-11-25
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 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 (Upserve by Lightspeed.) 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



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 <i>4.0.1</i> 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:

Dan Micak

F2B9CC5E68FE478...

Signature of Service Provider Executive Officer ↑

Service Provider Executive Officer Name: **Dan Micak**

Title: **Chief Legal Officer**

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]

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:



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/