

Payment Card Industry Data Security Standard

Entity Name: ParkMobile, LLC.
Scope Name: ParkMobile Electronic
Parking Solutions
(EPS)
Assessment End Date: December 12, 2025
Date of Report: December 19, 2025



Attestation of Compliance for Report on Compliance – Service Providers Version 4.0.1

Publication Date: August 2024

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:	ParkMobile, LLC.
DBA (doing business as):	Not Applicable
Company mailing address:	1075 Peachtree St NE, Suite 3100, Atlanta GA, 30309
Company main website:	https://ParkMobile.io
Company contact name:	Ori Fragman
Company contact title:	Head of Global Information Security & Cyber Resilience
Contact phone number:	+31611694923
Contact e-mail address:	ori.fragman@arrive.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:	Aprio, LLP.
Company mailing address:	2002 Summit Boulevard, Suite 120 Atlanta, GA 30319 – 1498
Company website:	aprio.com
Lead Assessor name:	Christopher Wright
Assessor phone number:	404-984-3600
Assessor e-mail address:	Christopher.Wright@Aprio.com
Assessor certificate number:	206-311

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:

ParkMobile Electronic Parking Solutions (EPS)

Type of service(s) assessed:

Hosting Provider:

- Applications / software
- Hardware
- Infrastructure / Network
- Physical space (co-location)
- Storage
- Web-hosting services
- Security services
- 3-D Secure Hosting Provider
- Multi-Tenant Service Provider
- Other Hosting (specify):
Not Applicable

Managed Services:

- Systems security services
- IT support
- Physical security
- Terminal Management System
- Other services (specify):
Not Applicable

Payment Processing:

- POI / card present
- Internet / e-commerce
- MOTO / Call Center
- ATM
- Other processing (specify):
Not Applicable

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 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 – Any services not explicitly listed as in-scope	
Type of service(s) not 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): Not Applicable	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): Not Applicable	Payment Processing: <input type="checkbox"/> POI / card present <input type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify): Not Applicable
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input 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 type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Network Provider		
<input type="checkbox"/> Others (specify): Not Applicable		
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.	Transmission: ParkMobile accepts payment cards through its payment applications for purchasing temporary parking spaces. Cardholder data (CHD) is transmitted securely to Chase Paymentech through Cybersource via HTTPS/TLSv1.2+ to facilitate e-commerce transactions on behalf of customers. Storage: ParkMobile does not store cardholder data in its databases for Reservations or Phonixx. ParkMobile uses Cybersource Token Management Service to
---	---

	<p>tokenize payment data. Only tokenized values are stored, ensuring sensitive cardholder information is never retained within ParkMobile systems.</p> <p>Processing: ParkMobile provides integrated solutions for managing parking-related functions, including cashless payment methods for on- and off-street parking (Phonixx), ParkMobile 360 (PM360), and ParkMobile Reservations.</p>
<p>Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.</p>	<p>ParkMobile transmits cardholder data and stores payment tokens using solutions that are published, configured, and managed within its AWS Cloud-hosted infrastructure. In addition, ParkMobile oversees the secure development and ongoing maintenance of all applications that collect account data, ensuring adherence to security best practices throughout the software lifecycle.</p>
<p>Describe system components that could impact the security of account data.</p>	<p><u>Systems that could impact the security of account data are listed below in Part 2c in greater detail and are as follows:</u></p> <ul style="list-style-type: none"> • EC2 Virtual Servers (Windows/Linux) • Security Groups • AWS load balancers • Kubernetes clusters and nodes • Okta & Active Directory IAM mechanisms • GuardDuty IDS/IPS • AWS WAF • WS Workspaces • Employee Workstations • Terraform

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.*

The ParkMobile cardholder data environment (CDE) is hosted within an AWS Cloud infrastructure and includes systems and services that store (tokenized CHD), process, or transmit account data, as well as components that could impact the security of that data.

Connections Into and Out of the CDE

- HTTP traffic to the ParkMobile web application for customer interactions and payment processing.
- Internal connections within the AWS Virtual Private Cloud (VPC) supporting application and database components.
- Secure connections to payment processors (e.g., Chase Paymentech)

for transaction authorization and settlement.

Critical System Components and Components Impacting Security

- **AWS Infrastructure Components**
 - EC2 Virtual Servers
 - AWS Load Balancers
 - Security Groups
 - Kubernetes clusters and nodes
 - AWS WAF (Web Application Firewall)
 - GuardDuty IDS/IPS
- **Identity and Access Management**
 - Okta and Active Directory IAM mechanisms
- **Application and Data Components**
 - ParkMobile payment applications
 - Cybersource Token Management Service (for tokenization of cardholder data)
 - Databases for application data (excluding sensitive cardholder data)
- **Administrative and Operational Tools**
 - Terraform (Infrastructure as Code)
 - Employee Workstations
 - AWS Workspaces for secure remote access

Additional Security Practices

- ParkMobile manages the secure development and maintenance of all applications that collect account data, ensuring adherence to security best practices throughout the software lifecycle.
- Cardholder data is never stored in ParkMobile systems; only tokenized values are retained, reducing risk exposure.

Indicate whether the environment includes segmentation to reduce the scope of the Assessment.

(Refer to the “Segmentation” section of PCI DSS for guidance on segmentation)

Yes No

**Part 2d. In-Scope Locations/Facilities
(ROC Section 4.6)**

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this Assessment.

Facility Type	Total Number of Locations (How many locations of this type are in scope)	Location(s) of Facility (city, country)
AWS Datacenter	1	US-East-1 / N. Virginia, USA

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.

♦ 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, Payment Applications (PA-DSS), Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, and Contactless Payments on COTS (CPoC) solutions.

Part 2. Executive Summary *(continued)*

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

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

<ul style="list-style-type: none"> • Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage)) 	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
<ul style="list-style-type: none"> • Manage system components included in the entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers) 	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
<ul style="list-style-type: none"> • Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers). 	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

If Yes:

Name of Service Provider:	Description of Services Provided:
Chase Paymentech Services	Payment Processor
Amazon Web Services	Hosting Provider
Snowflake, Inc.	Data Warehouse Platform
EasyPark AB	E-commerce
CyberSource	Tokenization Services

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: ParkMobile Electronic Parking Solutions (EPS)

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 checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 9:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 10:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 12:	<input checked="" type="checkbox"/>	<input 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"/>
Appendix A3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Justification for Approach

<p>For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.</p>	<p>1.2.6 There are no insecure services, protocols, or ports in use.</p> <p>1.3.3 There are no wireless networks or technologies in the entity's cardholder data environment.</p>
--	---

	1.4.4	ParkMobile only store the Last 4 digits, & hashed Value of the Cardholder's Name.
	2.2.5	There are no insecure services, protocols, or ports in use.
	2.3.1	There are no wireless networks or technologies in the entity's cardholder data environment.
	2.3.2	There are no wireless networks or technologies in the entity's cardholder data environment.
	3.1.1	ParkMobile only store a payment token, the last 4 digits,& hashed Value of the Cardholder's Name.
	3.2.1	ParkMobile only store a payment token, the last 4 digits,& hashed Value of the Cardholder's Name.
	3.3.1.1	Track data is never captured by ParkMobile.
	3.3.1.3	PIN data is never captured by ParkMobile.
	3.3.2	CVC is only ever present in volatile memory and is never written to disk.
	3.3.3	ParkMobile is not an issuer and does not support issuing services.
	3.4.1	ParkMobile only store a payment token, the last 4 digits,& hashed Value of the Cardholder's Name.
	3.4.2	ParkMobile only store a payment token, the last 4 digits,& hashed Value of the Cardholder's Name.
	3.5.1	ParkMobile only store a payment token, the last 4 digits,& hashed Value of the Cardholder's Name.
	3.5.1.1	ParkMobile only store a payment token, the last 4 digits,& hashed Value of the Cardholder's Name.
	3.5.1.2	ParkMobile only store a payment token, the last 4 digits,& hashed Value of the Cardholder's Name.
	3.5.1.3	ParkMobile only store a payment token, the last 4 digits,& hashed Value of the Cardholder's Name.
	3.6	ParkMobile only store a payment token, the last 4 digits,& hashed Value of the Cardholder's Name.
	3.7	ParkMobile only store a payment token, the last 4 digits,& hashed Value of the Cardholder's Name.
	4.2.1.2	There are no wireless networks or technologies in the entity's cardholder data environment.
	4.2.2	ParkMobile does not send PAN via end-user messaging technologies.
	5.3.2.1	The assessor reviewed AV configurations and vendor documentation to verify that real-time scans are performed as opposed to regularly scheduled scans.

	<p>6.2.3.1 Automated code checks are utilized via GitHub Advanced Security rather than manual code checks.</p> <p>6.4.1 As of March 31, 2025, this control was superseded by Requirement 6.4.2.</p> <p>6.5.2 There were no significant changes occurred in the past year.</p> <p>7.2.6 ParkMobile only store a payment token, the last 4 digits,& hashed Value of the Cardholder's Name.</p> <p>8.2.2 There are no shared, group, or generic IDs utilized in the CDE.</p> <p>8.2.3 ParkMobile does not connect to their customer environments.</p> <p>8.2.7 There are no third parties with remote access to CDE.</p> <p>8.3.10 This requirement has been superseded by Requirement 8.3.10.1 as of March 31, 2025.</p> <p>8.3.10.1 ParkMobile only store a payment token, the last 4 digits,& hashed Value of the Cardholder's Name.</p> <p>8.3.11 Physical and logical security tokens are not utilized to access the CDE.</p> <p>8.6 Interactive login is disabled for all system/application accounts in the CDE.</p> <p>9.4 There is no media generated or stored in the entity's cardholder data environment.</p> <p>9.5 There are no Point-of-Sale or Point-of-Interaction devices in the entity's cardholder data environment..</p> <p>10.2.1.1 ParkMobile only store a payment token, the last 4 digits,& hashed Value of the Cardholder's Name.</p> <p>10.4.2 During observations with INT-Log, the assessor verified that all logs are sent to the DataDog SIEM.</p> <p>10.7.1 This requirement has been superseded by Requirement 10.7.2 as of March 31, 2025.</p> <p>11.3.1.3 No significant changes occurred in the past year.</p> <p>11.3.2.1 No significant changes occurred during the past year.</p> <p>11.4.7 ParkMobile is not a multi-tenant service provider.</p> <p>12.3.2 The customized approach was not utilized as a part of this audit.</p> <p>12.3.4 The assessor reviewed the process last year and interviewed INT-GRC to confirm that the process was in place. However, since the Parkmobile application is currently being decommissioned, this process is no longer applicable.</p> <p>12.5.3 The assessor reviewed the 2025 ParkMobile Audit and Accountability Roles and Responsibilities and verified that there</p>
--	---

	<p>are no significant changes in organizational structure.</p> <p>A1 ParkMobile is not a multi-tenant service provider.</p> <p>A2 There are no Point-of-Sale or Point-of-Interaction devices in the entity's cardholder data environment.</p>
<p>For any Not Tested responses, identify which sub-requirements were not tested and the reason.</p>	<p>Not Applicable</p>

Section 2 Report on Compliance

(ROC Sections 1.2 and 1.3)

Date Assessment began: <i>Note: This is the first date that evidence was gathered, or observations were made.</i>	October 6, 2025
Date Assessment ended: <i>Note: This is the last date that evidence was gathered, or observations were made.</i>	December 12, 2025
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any testing activities performed remotely?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated *(Date of Report as noted in the ROC December 19, 2025).*

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

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

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

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

Part 3. PCI DSS Validation *(continued)*

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:

(Select all that apply)

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

Part 3b. Service Provider Attestation

Ori Fragman

Signature of Service Provider Executive Officer ↑	Date: December 19, 2025
Service Provider Executive Officer Name: Ori Fragman	Title: Head of Global Information Security & Cyber Resilience

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:

QSA performed testing procedures.

QSA provided other assistance.

If selected, describe all role(s) performed: Not Applicable

Christopher Wright

Signature of Lead QSA ↑	Date: December 19, 2025
Lead QSA Name: Christopher Wright	

Shane Peden

Signature of Duly Authorized Officer of QSA Company ↑	Date: December 19, 2025
Duly Authorized Officer Name: Shane Peden	QSA Company: Aprio, LLP.

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: Not Applicable

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/

CERTIFICATE *of* SIGNATURE

REF. NUMBER
VYYIJ-JEZ9I-KXYJR-RHD57

DOCUMENT COMPLETED BY ALL PARTIES ON
19 DEC 2025 23:40:56
UTC

SIGNER

SHANE PEDEN

EMAIL
SHANE.PEDEN@APRIO.COM

TIMESTAMP

SENT
19 DEC 2025 17:31:53

VIEWED
19 DEC 2025 19:35:28

SIGNED
19 DEC 2025 19:35:40

SIGNATURE



IP ADDRESS
71.56.63.1

LOCATION
MARIETTA, UNITED STATES

RECIPIENT VERIFICATION

EMAIL VERIFIED
19 DEC 2025 19:35:28

ORI FRAGMAN

EMAIL
ORI.FRAGMAN@ARRIVE.COM

SENT
19 DEC 2025 17:31:53

VIEWED
19 DEC 2025 23:28:14

SIGNED
19 DEC 2025 23:30:03



IP ADDRESS
83.86.163.87

LOCATION
AMSTELVEEN, THE NETHERLANDS

RECIPIENT VERIFICATION

EMAIL VERIFIED
19 DEC 2025 23:28:14



CERTIFICATE *of* SIGNATURE

REF. NUMBER
VYYIJ-JEZ9I-KXYJR-RHD57

DOCUMENT COMPLETED BY ALL PARTIES ON
19 DEC 2025 23:40:56
UTC

SIGNER

CHRISTOPHER WRIGHT

EMAIL
CHRISTOPHER.WRIGHT@APRIO.COM

TIMESTAMP

SENT
19 DEC 2025 17:31:53

VIEWED
19 DEC 2025 17:48:01

SIGNED
19 DEC 2025 23:40:56

SIGNATURE



IP ADDRESS
172.225.247.20

LOCATION
ATLANTA, UNITED STATES

RECIPIENT VERIFICATION

EMAIL VERIFIED
19 DEC 2025 17:48:01

