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: AudienceView Ticketing Corp.

Date of Report as noted in the Report on Compliance: December 13, 2024

Date Assessment Ended: November 21, 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:	AudienceView Ticketing Corp.
DBA (doing business as):	
Company mailing address:	200 Wellington St. W., 2nd Floor, Toronto, ON M5C 3C7
Company main website:	www.audienceview.com
Company contact name:	Nancy Galaski
Company contact title:	VP, People Operations & Internal Systems
Contact phone number:	(416) 687-2000
Contact e-mail address:	nancy.galaski@audienceview.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):	
Qualified Security Assessor	
Company name:	MNP LLP
Company mailing address:	255 Longside Dr, Suite 102, Mississauga, ON, L5W 0G7
Company website:	www.mnp.ca
Lead Assessor name:	Melanie Dodson
Assessor phone number:	(905) 607-9777
Assessor e-mail address:	Melanie.Dodson@mnp.ca
Assessor certificate number:	QSA 205-172

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:	AudienceView UPS, Unlimited on-prem and cloud

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):		

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:	The assessment excluded the following: • AudienceView environments hosted in Azure EastUS • Theatremania.ca (AudienceView as a merchant) • AudienceView development and QA environments hosted in Azure WestUS • Fraud Detection Services: Accertify & ThreatMetrix • Merchant owned and managed POS devices, card swipers and P2PE devices • POS, P2PE and card swiper communication protocols

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:	

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.	**Card Data Capture** 1. E-Commerce (Card-Not-Present) Channels: • Card data can be captured using Unlimited, UPS, or a combination of both platforms, depending on the client's configuration and payment method. The migration stage may influence whether one or both systems are in use. • Methods of card data capture include: ○ Gateway-provided iFrames: Hosted fields integrated into the Unlimited UI, currently available for CyberSource configurations. ○ UPS-hosted field iFrames: Offering direct integration for secure data handling. ○ Unlimited Payment Form: Form is used for card data capture. 2. Card-Present Channels: • POS Devices: Operated entirely within the client's environment and provided by gateways and processors. While Unlimited and UPS initiate the transactions using PCI compliant middleware (Tender Retail) and receive responses, they do not access the card data processed by these devices. Bluefin devices (ID TECH SREDKey2) are P2PE validated devices. • IDTech Swiper (card swiper): is installed at the client site and connected to the client's system (computer). The transaction is not encrypted at the device, but data is sent to a web browser where it is encrypted using TLS 1.2 or higher. • ID TECH SREDKey2: For a limited number of clients, AudienceView supports encrypted transactions using the ID TECH SREDKey2 device. The AudienceView generated key is injected into the devices by the vendor ID TECH. These transactions are subsequently decrypted within the AudienceView environment prior to transmission to the payment gateway. 3. Telephony Integration:

	• UPS supports card data capture via telephone lines through integration with Eckoh. In this method: ○ Clients integrate Eckoh into their telephony system. ○ Eckoh captures card data directly from the phone line and transmits it securely to UPS for processing. **Data Storage and Tokenization** 1. Unlimited: • Offers encrypted storage of account data in its databases for clients requiring this functionality. 2. UPS: • Does not store account data or transmit it back to Unlimited. • Supports tokenization through: ○ Compatible gateways configured by AudienceView. ○ TokenEx for cases where gateway-based tokenization is unavailable. • Tokenized account data remains confined to TokenEx, UPS, and associated payment service providers.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	The AudienceView Unlimited product offers a web-based, fully managed e-commerce SaaS solution for box office management and ticketing. Companies that operate performance theatres need to manage seat allocation for shows throughout a season and provide a system for customers to select seats, choose performances, make payments, and more. AudienceView delivers this functionality as a managed service. The solution is deployed, configured, and maintained by AudienceView in a third-party hosting data center, as well as in the Microsoft Azure cloud.
Describe system components that could impact the security of account data.	The critical systems examined in this assessment include: • Servers • Domain Controller • Cisco Routers and Switches • VMware • ESXi hosts • Load balancer – F5 and Azure • Application Gateways - Azure • Firewalls – Cisco, Palo Alto and Azure • Cloudflare web application firewall • Azure Entra access management solution • AlienVault SIEM solution • Microsoft Defender Antivirus solution

	• Microsoft Intune – Endpoint Management Solution • Azure DevOps Code repository • Datadog – Log monitoring • LastPass – Password Manager • Keyvaults • Backups – Azure • Cisco VPN • Microsoft Multifactor authentication (MFA)

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 AudienceView Unlimited product offers a web-based, fully managed e-commerce SaaS solution for box office management and ticketing. The solution is deployed, configured, and maintained by AudienceView in a third-party hosting data center, as well as in the Microsoft Azure cloud. **Card Data Capture** 1. E-Commerce (Card-Not-Present) Channels: • Card data can be captured using Unlimited, UPS, or a combination of both platforms, depending on the client's configuration and payment method. The migration stage may influence whether one or both systems are in use. • Methods of card data capture include: ○ Gateway-provided iFrames: Hosted fields integrated into the Unlimited UI, currently available for CyberSource configurations. ○ UPS-hosted field iFrames: Offering direct integration for secure data handling. ○ Unlimited Payment Form: Form is used for card data capture. 2. Card-Present Channels: • POS Devices: Operated entirely within the client's environment and provided by gateways and processors. While Unlimited and UPS initiate the transactions using PCI compliant middleware (Tender Retail) and receive responses, they do not access the card data processed by these devices. Bluefin devices (ID TECH SREDKey2) are P2PE validated devices. • IDTech Swiper (card swiper): is installed at the client site and connected to the client's system (computer). The transaction is not encrypted at the device, but data is sent to a web browser where it is

encrypted using TLS 1.2 or higher.

- ID TECH SREDKey2: For a limited number of clients, AudienceView supports encrypted transactions using the ID TECH SREDKey2 device. The AudienceView generated key is injected into the devices by the vendor ID TECH. These transactions are subsequently decrypted within the AudienceView environment prior to transmission to the payment gateway.

3. Telephony Integration:
   - UPS supports card data capture via telephone lines through integration with Eckoh. In this method:
     - Clients integrate Eckoh into their telephony system.
     - Eckoh captures card data directly from the phone line and transmits it securely to UPS for processing.

Data Storage and Tokenization

1. Unlimited:
   - Offers encrypted storage of account data in its databases for clients requiring this functionality.
2. UPS:
   - Does not store account data or transmit it back to Unlimited.
   - Supports tokenization through:
     - Compatible gateways configured by AudienceView.
     - TokenEx for cases where gateway-based tokenization is unavailable.
   - Tokenized account data remains confined to TokenEx, UPS, and associated payment service providers.

Indicate whether the environment includes segmentation to reduce the scope of the Assessment. (Refer to the "Segmentation" section of PCI DSS for guidance on segmentation)	☒ Yes ☐ No

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

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

Facility Type	**Total Number of Locations** **(**How many locations of this type are in scope)	**Location(s) of Facility** (city, country)
Example: Data centers	*3*	*Boston, MA, USA*
Azure Cloud environment	1	North Europe
Equinix / Q9 Data center	1	Markham, Canada
Corporate Office	1	Toronto, Canada

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
Merchant Connect Multi	4.2	Secure Software Framework	22-45.00143.002	01-Apr-2025
Merchant Connect Multi	5.0	Secure Software Framework	22-45.00143.001.aaa	01-Apr-2025

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

Part 2. Executive Summary *(continued)*

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

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

• Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage))	☒ Yes ☐ No
• Manage system components included in the entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers)	☒ Yes ☐ No
• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	☐ Yes ☒ No

If Yes:

Name of Service Provider:	**Description of Services Provided:**
Bluefin	Payment Gateway
Braintree	Payment Gateway
CyberSource	Payment Gateway
PayPal	Payment Gateway
Tender Retail	Payment Gateway - only EMV
TouchNet	Payment Gateway
Worldpay	Payment Gateway
Eckoh	Phone line card data capture
TokenEx	Card data tokenization
Microsoft Azure	Hosting of application infrastructure
AlienVault SIEM (AT&T Cybersecurity Unified Security Management (USM))	Security Information & Event Management
DataDog	Security Information & Event Management
Q9 / Equinix	Hosting of infrastructure
ONX/CBTS	Managed Service Provider
Cloudflare	Infrastructure
Cisco DUO	Multifactor authentication

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: AudienceView UPS, Unlimited Onprem and Unlimited Cloud

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 - No insecure services on NSCs. 1.3.3 - Wireless Network is not present. 2.2.5 - No insecure services on system components. 2.3.1 - 2.3.2 - Wireless Network is not present. 3.3.2 - This requirement is a best practice until 31 March 2025. 3.3.3 - This requirement is a best practice until 31 March 2025. 3.4.2 - This requirement is a best practice until 31 March 2025. 3.5.1.1 - 3.5.1.3 - This requirement is a best practice until 31 March 2025. 3.6.1.1 - This requirement is a best practice until 31 March 2025. 3.7.9 - The entity does not share any keys with the customers. 4.2.1.1 - This requirement is a best practice until 31 March 2025. 4.2.1.2 - Wireless Network is not present. 4.2.2 - The entity does not use end-user messaging technologies. 5.2.3 - AudienceView UPS and Unlimited has implemented anti-malware solution on all the in scope systems. 5.2.3.1 - This requirement is a best practice until 31 March 2025. 5.3.2.1 - This requirement is a best practice until 31 March 2025. 5.3.3 - This requirement is a best practice until 31 March 2025. 5.4.1 - This requirement is a best practice until 31 March 2025. 6.3.2 - This requirement is a best practice until 31 March 2025. 6.4.2 - This requirement is a best practice until 31 March 2025.

	6.4.3 - This requirement is a best practice until 31 March 2025. 6.5.2 - No significant changes occurred within the assessment year. 7.2.5 - This requirement is a best practice until 31 March 2025. 7.2.5.1 - This requirement is a best practice until 31 March 2025. 8.3.11 - The entity does not use any type of logical access tokens, smart cards, or certificates. 8.4.2 - This requirement is a best practice until 31 March 2025. 8.5.1 - This requirement is a best practice until 31 March 2025. 8.6.1 - This requirement is a best practice until 31 March 2025. 8.6.2 - This requirement is a best practice until 31 March 2025. 8.6.3 - This requirement is a best practice until 31 March 2025. 9.2.1 – 9.3.4 - Equinix Data Center and Microsoft Azure provides hosting for AudienceView CDE and are PCI-compliant service providers. 9.4.1.1 – 9.4.1.2 - There is no offline media backups used in AV environment. 9.4.2-9.4.4 - Media with CHD is not sent outside the facility. 9.4.5-9.4.5.1 - There are no media inventories. 9.4.6 - There is no hard copy materials with CHD. 9.5.1-9.5.1.3 - The responsibility lies with the AV clients and not in scope of this assessment. 10.4.1.1 - This requirement is a best practice until 31 March 2025. 10.4.2 - The system component logs are forwarded to the SIEM (SIEM is monitored by a 3rd party service provider) or have been captured as part of a CCW that includes daily log reviews.

	10.4.2.1 - This requirement is a best practice until 31 March 2025. 10.7.2 - This requirement is a best practice until 31 March 2025. 10.7.3- This requirement is a best practice until 31 March 2025. 11.3.1.1-11.3.1.3 - This requirement is a best practice until 31 March 2025. 11.3.2.1 - No significant changes occurred within the assessment year. 11.4.7 - This requirement is a best practice until 31 March 2025. 11.5.1.1 - This requirement is a best practice until 31 March 2025. 11.6.1 - This requirement is a best practice until 31 March 2025. 12.3.1- 12.3.4 - This requirement is a best practice until 31 March 2025. 12.5.2.1 - This requirement is a best practice until 31 March 2025. 12.5.3 - This requirement is a best practice until 31 March 2025. 12.6.2 - This requirement is a best practice until 31 March 2025. 12.6.3.1 - This requirement is a best practice until 31 March 2025. 12.6.3.2 - This requirement is a best practice until 31 March 2025. 12.10.4.1 - This requirement is a best practice until 31 March 2025. 12.10.7 - This requirement is a best practice until 31 March 2025. A1.1.1 - This requirement is a best practice until 31 March 2025. A1.1.4 - This requirement is a best practice until 31 March 2025. A1.2.3 - This requirement is a best practice until 31 March 2025.

	A2.1.1-A2.1.3 - The entity does not own or manage POS devices. Appendix A3 - The entity is not a Designated Entities Supplemental Validation (DESV).
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	

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.*	May 07, 2024
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	November 21, 2024
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No
Were any testing activities performed remotely?	☒ Yes ☐ No

Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated December 13, 2024.

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 AudienceView Ticketing Corp. 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 AudienceView Ticketing Corp. has not demonstrated compliance with PCI DSS requirements.

Target Date for Compliance:

An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.

□ **Compliant but with Legal exception:** One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby AudienceView Ticketing Corp. has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction.

This option requires additional review from the entity to which this AOC will be submitted.

If selected, complete the following:

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

Part 3. PCI DSS Validation *(continued)*

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:
(Select all that apply)

☒	The ROC was completed according to *PCI DSS*, Version 4.0.1 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
☒	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

Nancy Galaski
Nancy Galaski (Dec 13, 2024 09:38 EST)

Signature of Service Provider Executive Officer ↑	Date: 13/12/24
Service Provider Executive Officer Name: Nancy Galaski	Title: VP, People Operations & Internal Systems

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:

M Dodson

Signature of Lead QSA ↑	Date: 13/12/24
Lead QSA Name: **Melanie Dodson**	

Tom B

Signature of Duly Authorized Officer of QSA Company ↑	Date: 13/12/24
Duly Authorized Officer Name: **Tom Beaupre**	QSA Company: **MNP 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:

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/

PCI DSS AOC - Service Providers

Final Audit Report 2024-12-13

Created:	2024-12-13
By:	Lacey Juk (lacey.juk@audienceview.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAi6aCjcYXRIFb4I5oMz3_hH7ANI18JHIx

"PCI DSS AOC - Service Providers" History

Document created by Lacey Juk (lacey.juk@audienceview.com)
2024-12-13 - 2:30:44 PM GMT

Document emailed to Nancy Galaski (nancy.galaski@audienceview.com) for signature
2024-12-13 - 2:30:49 PM GMT

Email viewed by Nancy Galaski (nancy.galaski@audienceview.com)
2024-12-13 - 2:36:38 PM GMT

Document e-signed by Nancy Galaski (nancy.galaski@audienceview.com)
Signature Date: 2024-12-13 - 2:38:03 PM GMT - Time Source: server

Agreement completed.
2024-12-13 - 2:38:03 PM GMT