Security Standards Council ®

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 12, 2025

Date Assessment Ended: December 10, 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:	AudienceView Ticketing Corp
DBA (doing business as):	
Company mailing address:	200 Wellington St W, 2nd Floor, Toronto, ON, Canada M5C 3C7
Company main website:	https://www.audienceview.com/
Company contact name:	Daymon Boswell
Company contact title:	Director, Internal Systems
Contact phone number:	416.687.2000
Contact e-mail address:	pci@audienceview.com daymonboswell@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):	Not Applicable
Qualified Security Assessor	
Company name:	Prescient Security LLC
Company mailing address:	1900 Church Street, Suite 300, Nashville, TN 37203
Company website:	https://prescientsecurity.com/
Lead Assessor name:	Kevin Whalen
Assessor phone number:	+1 212-271-0175
Assessor e-mail address:	pci@prescientsecurity.com
Assessor certificate number:	PCI DSS QSA, Certificate Number: 202-230

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were <u>INCLUDED</u> in the scope of the Assessment (select all that apply):

Name of service(s) assessed:	AudienceView Unlimited	
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):	**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): None		

***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:	Not Applicable

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.	Headquartered in Toronto, Canada, AudienceView Ticketing Corporation (aka Audienceview Unlimited), is a fully managed SaaS solution for box office management and ticketing. Client companies operate performance theatres and utilize the platform 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 Unlimited delivers this functionality as a managed service. The solution is deployed, configured, and maintained by AudienceView within the Microsoft Azure public cloud infrastructure-as-a-service.

	AudienceView Unlimited receives transactions via their bespoke applications regardless of the payment channels used by the clients. AudienceView Unlimited is composed of two primary services: • Unlimited: The Unlimited platform represents the core box office management system, including payment services for use in purchasing tickets. The Unlimited platform offers CHD storage as well as direct connection capability to payment gateway services. • Unified Payment Service (UPS): The UPS platform has been designed a general service payment gateway, that eventually all AudienceView platforms can use to isolate cardholder data capture and integrate with payment gateways. The UPS platform utilized TokenEx and payment gateways for storage of CHD. Transmission of CHD Card Not Present (e-Commerce) | AudienceView accepts online e-commerce CNP transactions (PAN, Expiry, CVV) through a checkout page (fully managed by Audienceview). All transmission of cardholder data is secured via HTTPS over TLS 1.2 or greater. Card Present (POS) | Cardholder data is encrypted and transmitted directly from the box office checkout POI to payment processer for and authorization and settlement services. Telephone Order | Integration with a PCI compliant IVR service which then transmits CHD via an API to Audienceview for further transmission and storage. Processing of CHD Card Not Present (e-Commerce) | Inbound transaction PANs, CVVs, and Expiry are received from the checkout page to the payment services application service, and the transaction is forwarded either a payment gateway of the UPS. From UPS, CHD is forwarded to TokenEx. Card Present (POS) | transactions are either forwarded directly to the payment service provider (P2PE) or the swipe is converted to input fields and forwarded to Unlimited where it is processed as if it were card not present. Storage of CHD AudienceView Unlimited stores CHD three different methods: • Stored in Unlimited using custom encryption key generation and management. • Stored in a PCI compliant data vault provider. • Stored with payment gateways.

Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Unlimited offers a ticket purchasing solution for the theatre industry, museums, concerts, festivals, sporting venues, and similar events. Card present transactions are received via a web browser through the application. The scope of this assessment does not include client-owned and managed systems including card swipers and computer systems used to enter cardholder data into the AudienceView Unlimited platform. Card-not-present transactions occur via the AudienceView web application. Consumers and clients can enter cardholder data directly into the web application. Telephone orders can be placed via a third-party IVR which then forwards CHD to AudienceView for processing.
Describe system components that could impact the security of account data.	System Components include: • Cloudflare - Web Application firewall • Azure Firewalls - network security controls. • PaloAlto Virtual Firewall –VPN IPsec tunnels, and egress network security controls from Azure. • Web servers - Virtual machines and Containers • Azure Active Directory and Active Directory on-prem (master) – Authentication and User Management Platform • Microsoft Authenticator App – MFA • Microsoft 365 Defender for endpoint – Malware protection solution and FIM • Sonar Cloud and Zap – SAST • Vanta GRC Platform • MS Defender for Cloud • Rapid7 for Internal vulnerability scanner

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.*	All in-bound traffic passes securely (HTTPS TLS v1.2) first through Cloudflare Web Application Firewall services which are configured with security blocking rules and alerts. Cloudflare provides HTTPS connectivity to the web application virtual services within Azure, that are protected with Azure Firewalls. Web sites are presented to consumers and customers to purchase tickets. Purchasing CHD can be routed to the AudienceView for storage, forwarding to data vault tokenization provider, and payment gateways for transaction authorization and settlement. Card present transactions are managed by clients and payment service providers to support the transmission of encrypted transactions directly from the POI to the payment service provider for decryption, authorization and settlement. Card present transactions can also support card readers for capture and translation of card data to the web browser input fields. Azure application and infrastructure services are accessed by Administrators via a VPN Tunnel between the Azure hosted Palo Alto virtual firewall and an on-premises Cisco ASA VPN firewall. Web application services and administrator workstations are protected by MS Defender end point security, which includes IDS and FIM for the cloud hosted services. All security event logs are forwarded to a 24/7 security operations center that utilizes AlienVault SEIM.
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)
Azure – Public Cloud IaaS	3	europe-north | Ireland ca-central | Ontario, CA us-west | Virginia, USA
Corporate Office (no CHD, only connectivity to the Azure Cloud)	1	Toronto, ON, 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
Tender Retail, Merchant Connect Multi	4.2	Secure Software Standard, v1.2.1	#25-45.00143.003	2-Jun-2028
Tender Retail, Merchant Connect Multi	5.0	Secure Software Standard, v1.2.1	#25-45.00143.004	28-May-2028

* 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:
Microsoft Corporation – Microsoft Azure	Public Cloud Infrastructure as a Service
Cloudflare	DNS, WAF, SSL, and Page Sheild
Ixopay, Inc	CHD tokenization
Adyen	Payment processor
Bluefin Payment Systems	Payment processor
PayPal, Inc.'s Braintree Payment Processing System	Payment processor
CyberSource	Payment processor
Eckoh	Payment processor
PayPal	Payment processor
TouchNet	Payment processor
WorldPay	Payment processor
LevelBlue Unified Security Management (AlienVault)	SIEM and SOC
Audienceview Inc	Corporate Shared 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: AudienceView - Unlimited

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 - AudienceView did not support the use of insecure services, protocols, or ports. 1.3.3 - AudienceView did not support wireless environments that connected to the CDE. 2.2.5 – AudienceView did not support insecure services, daemons, or protocols were enabled. 2.3.1, 2.3.2 - AudienceView did not support wireless environments that connect to the CDE. 3.3.2 - SAD was never stored electronically in the AudienceView database. 3.3.3 - AudienceView was not an issuer and did not support issuing services. 3.4.1 - AudienceView does not provide display of encrypted full PAN and only displays the last four. 3.5.1.2, 3.5.1.3 - AudienceView does not rely on disk-level encryption for securing stored PAN. 3.7.9 - AudienceView does not share cryptographic keys with customers. 4.2.1.2 - There were no wireless networks permitted for transmitting cardholder data. 4.2.2 - AudienceView did not use end-user messaging technologies to send cardholder data. 5.2.3, 5.2.3.1 - All systems in the CDE are protected by anti-virus software. 5.3.2.1 – AudienceView endpoint security performs continuous malware scans. 6.4.1 – This requirement was superseded by Requirement 6.4.2 after 31-March-2025. 8.2.2 - AudienceView did not use shared authentication credentials. 8.2.3 - AudienceView did not have remote access to customer premises. 8.2.7 - Vendors were not provided with access (local or remote) to the payment card environment. 8.3.10, 8.3.10.1 - Customer didn't have access to stored account data and could not impact the security of the dataflows. 9.4.1, 9.4.1.1, 9.4.1.2, 9.4.2, 9.4.3, 9.4.4, 9.4.5, 9.4.5.1, 9.4.6, 9.4.7 - AudienceView did not store CHD in physical media. 9.5.1, 9.5.1.1, 9.5.1.2, 9.5.1.2.1, 9.5.1.3 - AudienceView was not responsible for the management of card reading devices. 10.7.1 - This requirement was superseded by Requirement 10.7.2 after 31-March-2025. 11.2.2 - AudienceView did not support wireless access points within the cardholder data environment. 11.4.7 - AudienceView clients were not required to perform external pentation testing of the services they use from AudienceView. 12.3.2 - There was no PCI DSS requirement that the AudienceView met with the customized approach. Appendix A1 – AudienceView was not considered a multi-tenant service provider as customers had no access to CHD and did not have access to the configuration of secure cardholder data flows. Appendix A2 – AudienceView did not support SSL or early TLS.
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: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*	10/02/2025
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	12/10/2025
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 12, 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 ***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 *Not Applicable* has not demonstrated compliance with PCI DSS requirements.

Target Date for Compliance: *Not Applicable*

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 *Not Applicable* 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
Not Applicable.	Not Applicable.

Part 3. PCI DSS Validation *(continued)*

Part 3a. Service Provider Acknowledgement

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

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

Part 3b. Service Provider Attestation

DocuSigned by:
Nancy Galaski
D7D89A10E36C41C...

Signature of Service Provider Executive Officer ↑	Date: 12/16/2025
Service Provider Executive Officer Name: **Nancy Galaski**	Title: **VP, People & 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:

DocuSigned by:
Kevin Whalen
0B32514137D7445...

Signature of Lead QSA ↑	Date: 12/16/2025
Lead QSA Name: **Kevin Whalen**	

DocuSigned by:
Kevin Whalen
0B32514137D7445...

Signature of Duly Authorized Officer of QSA Company ↑	Date: 12/16/2025
Duly Authorized Officer Name: **Kevin Whalen**	QSA Company: **Prescient Security LLC**

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/