Payment Card Industry (PCI)

Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

Revision 2

September 2022

Document Changes

Date	Version	Description
September 2022	3.2.1 Revision 2	Updated to reflect the inclusion of UnionPay as a Participating Payment Brand.

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS).* Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

Part 1. Service Provider and Qualified Security Assessor Information

Part 1a. Service Provider Organization Information

Company Name:	AudienceView Ticketing Corp.		DBA (doing business as):		
Contact Name:	Daymon Boswell		Title:	Director - Internal Systems and Business Processes	
Telephone:	1-226-980-5957		E-mail:	daymon.boswell@audienceview.com pci@audienceview.com	
Business Address:	200 Wellington St. W., 2nd Floor		City:	Toronto	
State/Province:	ON	Country:	Canada	Zip:	M5C 3C7
URL:	www.audienceview.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:	MNP LLP.				
Lead QSA Contact Name:	Alistair Thompson		Title:	Snr. Manager, Risk and Compliance	
Telephone:	905-607-9777		E-mail:	alistair.thompson@mnp.ca	
Business Address:	255 Longside Dr, Suite 102		City:	Mississauga	
State/Province:	ON	Country:	Canada	Zip:	L5W 0G7
URL:	www.mnpdigital.ca				

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) assessed:	AudienceView Unlimited Ticketing software application and UPS

Type of service(s) assessed:

Hosting Provider:

☒ Applications / software

☒ Hardware

☒ Infrastructure / Network

☒ Physical space (co-location)

☒ Storage

☒ Web

☐ Security services

☐ 3-D Secure Hosting Provider

☐ Shared Hosting Provider

☐ Other Hosting (specify):

Managed Services (specify):

☒ Systems security services

☒ IT support

☒ Physical security

☐ Terminal Management System

☐ Other services (specify):

Payment Processing:

☐ POS / 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 you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.*

Part 2a. Scope Verification (continued)

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

Name of service(s) not assessed:	N/A

Type of service(s) not assessed:

Hosting Provider:

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

Managed Services (specify):

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

Payment Processing:

- ☐ POS / 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:	N/A

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	AudienceView accepts transactions from the public (ticket buyer) or a customer service rep (CSR) of their customer. These transactions occur directly on the hosted AudienceView web application. From the perspective of CHD handling there is no material difference between how a member of the public or a CSR interacts with the AudienceView application. Presently the application is undergoing a transition period to migrate their payment process to a production called UPS.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Legacy (Unlimited) - During the process to authorize a credit card payment, card numbers are stored encrypted within the database using Microsoft TDE and a predefined key using the internal process involving an industry accepted certificate store. UPS – During the process to authorize a credit card, the transaction enters the UPS environment through a hosted payment solution presented to the Unlimited application by means of an iFrame. UPS then sends the card details onward to the clients acquirer for payment processing. The card numbers are never stored except within memory.

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility:	Number of facilities of this type	Location(s) of facility (city, country):
Example: Retail outlets	*3*	*Boston, MA, USA*
Q9 Data Centre	1	Markham, ON, Canada
Vantage Data Centres UK Limited	1	Newport, South Wales, UK
Corporate Head Office	1	Toronto, ON, Canada

Part 2d. Payment Applications				
Does the organization use one or more Payment Applications?			☐ Yes ☐ No	
Provide the following information regarding the Payment Applications your organization uses:				
Payment Application Name	**Version Number**	**Application Vendor**	**Is application PA-DSS Listed?**	**PA-DSS Listing Expiry date (if applicable)**
Eigen Developments/ Miraserv	6.0	Eigen		
Tender Retail Systems/Merchant Multi Connect with Moneris	3.3.1.17	Tender Retail		
Elavon/Protobase suite	6.01.0621	Elavon		

Part 2e. Description of 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 POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	The AudienceView environment is located at 3 data centres as well as in the Microsoft Azure cloud. MNP verified that there is no direct connection between the head office and the data centres. Connections into and out of the CDE is through a VLAN setup specifically to administer the devices and systems.
Does your business use network segmentation to affect the scope of your PCI DSS environment? *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*	☒ Yes ☐ No

Part 2f. Third-Party Service Providers	
Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated?	☐ Yes ☒ No
If Yes:	
Name of QIR Company:	
QIR Individual Name:	
Description of services provided by QIR:	
Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?	☒ Yes ☐ No
If Yes:	

Name of service provider:	**Description of services provided:**
Q9	Data Centre
Vantage Data Centres UK Limited	Data Centre
Commedia / Verifone	Payment Processor
Moneris	Payment Processor
PayPal	Payment Processor
Red Card / Anderson Zaks	Payment Processor
Elavon	Payment Processor
Global Payments	Payment Processor
BlueFin	Payment Processor
ACCEO Tender Retail	Payment Processor
Braintree	Payment Processor
TouchNet	Payment Processor
AlienVault	SIEM
Microsoft Azure	Cloud Services

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

Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as "Not Tested" or "Not Applicable" in the ROC.
- **None** – All sub-requirements of that requirement were marked as "Not Tested" and/or "Not Applicable" in the ROC.

For all requirements identified as either "Partial" or "None," provide details in the "Justification for Approach" column, including:

- Details of specific sub-requirements that were marked as either "Not Tested" and/or "Not Applicable" in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

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:	

PCI DSS Requirement	**Details of Requirements Assessed**			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	☐	☒	☐	1.2.3 – N/A Wireless not in scope
Requirement 2:	☐	☒	☐	2.1.1 – N/A Wireless not in scope 2.6 – N/A Managed Services not in scope
Requirement 3:	☐	☒	☐	3.2 - N/A - SAD data is not stored 3.4.1 – N/A – Disk encryption not used 3.8 - N/A - keys are not shared with customers
Requirement 4:	☐	☒	☐	4.1.1 – N/A – Wireless not in scope
Requirement 5:	☐	☒	☐	5.1.2 – N/A – All systems are commonly affected by Malware
Requirement 6:	☒	☐	☐	
Requirement 7:	☒	☐	☐	
Requirement 8:	☒	☐	☐	

Requirement 9:	☐	☒	☐	9.5 - N/A - Entity does not store CHD on physical media 9.6 - N/A - Entity does not store CHD on physical media 9.7 - N/A - Entity does not store CHD on physical media 9.8 - N/A - Entity does not store CHD on physical media 9.9 - N/A - Entity does not collect CHD with any physical devices
Requirement 10:	☒	☐	☐	
Requirement 11:	☒	☐	☐	
Requirement 12:	☒	☐	☐	
Appendix A1:	☐	☐	☒	Not A Shared hosting provider
Appendix A2:	☐	☐	☒	POS devices do not user SSL or early TLS

Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	August 1st 2023
Have compensating controls been used to meet any requirement in the ROC?	☒ Yes ☐ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes ☐ No
Were any requirements not tested?	☐ Yes ☒ No
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated July 31st 2023.

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

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby AudienceView Ticketing Corp. has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby AudienceView Ticketing Corp. has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with the payment brand(s) before completing Part 4.*
☐	**Compliant but with Legal exception:** One or more requirements are marked “Not in Place” due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version 3.2.1 Revision 2, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
☐	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☒	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☒	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

Part 3a. Acknowledgement of Status (continued)	
☒	No evidence of full track data[1], CAV2, CVC2, CVN2, CVV2, or CID data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor MNP LLP.

Part 3b. Service Provider Attestation

lawrence Franco

lawrence Franco (Aug 9, 2023 12:01 EDT)

Signature of Service Provider Executive Officer ↑	*Date: August 9th 2023*
Service Provider Executive Officer Name: Lawrence Franco	*Title: Chief Operating Officer*

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)	
If a QSA was involved or assisted with this assessment, describe the role performed:	Alistair Thompson, QSA, conducted the assessment and completed the Report on Compliance

Tom Ba

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* August 8th 2023
Duly Authorized Officer Name: Tom Beaupre	*QSA Company:* MNP LLP.

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)	
If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	

[1] Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

[2] The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

[3] Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement. If you answer “No” to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with the applicable payment brand(s) before completing Part 4.

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 a firewall configuration to protect cardholder data	□	□	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	□	□	
3	Protect stored cardholder data	□	□	
4	Encrypt transmission of cardholder data across open, public networks	□	□	
5	Protect all systems against malware and regularly update anti-virus software or programs	□	□	
6	Develop and maintain secure systems and applications	□	□	
7	Restrict access to cardholder data by business need to know	□	□	
8	Identify and authenticate access to system components	□	□	
9	Restrict physical access to cardholder data	□	□	
10	Track and monitor all access to network resources and cardholder data	□	□	
11	Regularly test security systems and processes	□	□	
12	Maintain a policy that addresses information security for all personnel	□	□	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	□	□	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	□	□	

AudienceView Unlimited and UPS 2023 AOC

Final Audit Report 2023-08-09

Created:	2023-08-09
By:	Lacey Juk (lacey.juk@audienceview.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAACj9nWGY6GtWpAWUUibVq-0C1AfVHSrpm

"AudienceView Unlimited and UPS 2023 AOC" History

Document created by Lacey Juk (lacey.juk@audienceview.com)
2023-08-09 - 2:48:49 PM GMT

Document emailed to lawrence.franco@audienceview.com for signature
2023-08-09 - 2:49:48 PM GMT

Email viewed by lawrence.franco@audienceview.com
2023-08-09 - 4:00:50 PM GMT

Signer lawrence.franco@audienceview.com entered name at signing as lawrence Franco
2023-08-09 - 4:01:07 PM GMT

Document e-signed by lawrence Franco (lawrence.franco@audienceview.com)
Signature Date: 2023-08-09 - 4:01:09 PM GMT - Time Source: server

Agreement completed.
2023-08-09 - 4:01:09 PM GMT