



Payment Card Industry (PCI) Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

June 2018

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:	Rob Williams	Title:	Chief Product Officer
Telephone:	(416) 687 2000	E-mail:	rob.williams@audienceview.com
Business Address:	200 Wellington St. W., 2 nd Floor	City:	Toronto
State/Province:	Ontario	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, CyberSecurity
Telephone:	(416) 575-7026	E-mail:	alistair.thompson@mnp.ca
Business Address:	255 Longside Dr, Suite 102	City:	Mississauga
State/Province:	Ontario	Country:	Canada
		Zip:	L5W 0G7
URL:	www.mnp.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	
Type of service(s) assessed:		
Hosting Provider: <input checked="" type="checkbox"/> Applications / software <input checked="" type="checkbox"/> Hardware <input checked="" type="checkbox"/> Infrastructure / Network <input checked="" type="checkbox"/> Physical space (co-location) <input checked="" type="checkbox"/> Storage <input checked="" type="checkbox"/> Web <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Shared Hosting Provider <input type="checkbox"/> Other Hosting (specify):	Managed Services (specify): <input checked="" type="checkbox"/> Systems security services <input checked="" type="checkbox"/> IT support <input checked="" type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	Payment Processing: <input type="checkbox"/> POS / card present <input checked="" type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input 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):		

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:	Managed Services (specify):	Payment Processing:
<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 <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Shared Hosting Provider <input type="checkbox"/> Other Hosting (specify):	<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):	<input type="checkbox"/> POS / card present <input type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input 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):		

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
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	AudienceView stores credit card information if the customer opt's in to do so. The credit card information is stored in an unreadable format within a database.

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):
<i>Example: Retail outlets</i>	3	<i>Boston, MA, USA</i>
Equinix Data Center	1	Brampton, ON, Canada
Next Generation Data Center	1	Newport, South Wales, UK
Corporate Head Office	1	Toronto, ON, Canada

Amazon Web Services	1	London, UK
---------------------	---	------------

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)
Tender Retail Systems/Merchant Multi Connect with Moneris	4.2.11 - Global Payments 4.2.13 - Moneris 4.2.16 - Chase Paymentech	Tender Retail	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	

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 2 data centres as well as in the Amazon 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:	Not applicable
QIR Individual Name:	Not applicable
Description of services provided by QIR:	Not applicable

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:
Equinix, Inc.	Data Centre
Vantage Data Centers UK Limited	Data Centre
OnX Managed Services Inc.	Firewall and hardware support
FIS Worldpay, LLC	Payment Processing
Worldwide Payment Gateway (WPG)	
Paypal Inc.	Payment Processing
Anderson Zaks Ltd.	Payment Processing
Braintree, a service of PayPal Inc.	Payment Processing
CyberSource Corporation	Payment Processing
Bluefin Payment Systems LLC	Payment Processing
TouchNet Information Systems Inc.	Payment Processing
Amazon Web Services	Backup hosting
AlienVault	SIEM
Authorize.net/CyberSource	Payment Processing
PayPal (Payflow Pro and PayPal Payments Pro)	Payment Processing
Heartland	Payment Processing
Moneris	Payment Processing
TouchNet	Payment Processing
Optimal Payments/PaySafe	Payment Processing

Stripe	Payment Processing
USAePay	Payment Processing
First Data/Payeezy	Payment Processing
Elavon/Converge	Payment Processing
Chase Paymentech	Payment Processing
BluePay (Clover Network)	Payment Processing
AsiaPay	Payment Processing
Verifone	Payment Processing
Red Card/Anderson Zaks	Payment Processing
PXP/ Servebase	Payment Processing
CardConnect	Payment Processing
Chase Paymentech	Payment Processing
Recurly	Payment Processing
Sagenet	Payment Processing
TokenX	Payment Processing
Magtec	Payment Processing
Alienvault/AT&T Cybersecurity USMA	SIEM
Amazon Web Services AWS	Backup Services
Spectrum	Payment Processing

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:		AudienceView Ticketing software application		
PCI DSS Requirement	Details of Requirements Assessed			Justification for Approach (Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)
	Full	Partial	None	
Requirement 1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1.2.3 No wireless in scope
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2.1.1. No wireless in scope 2.2.3 No insecure services 2.6 Not a shared hosting provider
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3.2 - N/A - SAD data is not stored 3.4.1 No full disk encryption 3.6.a No sharing of keys
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	4.1.1 No wireless in scope
Requirement 5:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	5.1.2 AV on all systems, no systems not commonly affected
Requirement 6:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	8.6.a No other authentication systems
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	9-1 – 9.4 – The entity uses third party physical data centres 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:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 11:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	11.1 N/A – the data centres are PCI compliant 11.2.3 No significant change requiring rescan
Requirement 12:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not a shared hosting provider
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	No use of POS devices which use SSL of 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:	09-Nov-2022	
Have compensating controls been used to meet any requirement in the ROC?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Were any requirements not tested?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated *November 9th 2022*.

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**):

<input checked="" type="checkbox"/>	<p>Compliant: All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby <i>Audience View Ticketing Corp.</i> has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p>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 (<i>Service Provider Company Name</i>) has not demonstrated full compliance with the PCI DSS.</p> <p>Target Date for Compliance:</p> <p>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. <i>Check with the payment brand(s) before completing Part 4.</i></p>						
<input type="checkbox"/>	<p>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.</p> <p><i>If checked, complete the following:</i></p> <table border="1" style="width: 100%;"> <thead> <tr> <th style="width: 35%;">Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met				
Affected Requirement	Details of how legal constraint prevents requirement being met						

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to the <i>PCI DSS Requirements and Security Assessment Procedures</i> , Version 3.2.1, 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 my assessment in all material respects.
<input type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	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)

<input checked="" type="checkbox"/>	No evidence of full track data ¹ , CAV2, CVC2, CID, or CVV2 data ² , or PIN data ³ storage after transaction authorization was found on ANY system reviewed during this assessment.
<input checked="" type="checkbox"/>	ASV scans are being completed by the PCI SSC Approved Scanning Vendor <i>MNP LLP</i> .

Part 3b. Service Provider Attestation

Lawrence Franco

Lawrence Franco (Nov 29, 2022 10:50 EST)

Signature of Service Provider Executive Officer ↑	Date: November 29 2022
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:	<i>Alistair Thompson, QSA, conducted the assessment and completed the Report on Compliance</i>
--	--

Tom Beaupre

Signature of Duly Authorized Officer of QSA Company ↑	Date: November 29 th 2022
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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	<input checked="" 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 checked="" type="checkbox"/>	<input type="checkbox"/>	









AudienceView_AOC_2022

Final Audit Report

2022-11-29

Created:	2022-11-29
By:	Elinor Zantinge (elinor.zantinge@audienceview.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAzNQm8M1ZqxmAUai3rXZimdNrEOtMeA9O

"AudienceView_AOC_2022" History

-  Document created by Elinor Zantinge (elinor.zantinge@audienceview.com)
2022-11-29 - 3:47:44 PM GMT
-  Document emailed to lawrence.franco@audienceview.com for signature
2022-11-29 - 3:50:14 PM GMT
-  Email viewed by lawrence.franco@audienceview.com
2022-11-29 - 3:50:25 PM GMT
-  Signer lawrence.franco@audienceview.com entered name at signing as Lawrence Franco
2022-11-29 - 3:50:40 PM GMT
-  Document e-signed by Lawrence Franco (lawrence.franco@audienceview.com)
Signature Date: 2022-11-29 - 3:50:42 PM GMT - Time Source: server
-  Agreement completed.
2022-11-29 - 3:50:42 PM GMT