



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 Campus		DBA (doing business as):		
Contact Name:	Daymon Boswell		Title:	Director, Internal Systems	
Telephone:	(416) 687 2000		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:	Melanie Dodson		Title:	Senior Manager, Cyber Risk	
Telephone:	(905) 607-9777		E-mail:	Melanie.Dodson@mnp.ca	
Business Address:	255 Longside Drive Suite 102		City:	Mississauga	
State/Province:	ON	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 Campus	
Type of service(s) assessed:			
Hosting Provider: <input checked="" type="checkbox"/> Applications/software <input type="checkbox"/> Hardware <input checked="" type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input checked="" type="checkbox"/> Web <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input checked="" type="checkbox"/> Shared Hosting Provider <input type="checkbox"/> Other Hosting (specify):		Managed Services (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):	
		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"/> Back-Office Services <input type="checkbox"/> Billing Management <input type="checkbox"/> Clearing and Settlement <input type="checkbox"/> Network Provider <input type="checkbox"/> Others (specify):		<input type="checkbox"/> Fraud and Chargeback <input type="checkbox"/> Issuer Processing <input type="checkbox"/> Loyalty Programs <input type="checkbox"/> Merchant Services	
		<input type="checkbox"/> Payment Gateway/Switch <input type="checkbox"/> Prepaid Services <input type="checkbox"/> Records Management <input type="checkbox"/> Tax/Government Payments	

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: Not applicable. The AudienceView Campus solution was assessed.

Type of service(s) not assessed:

Hosting Provider:	Managed Services (specify):	Payment Processing:
<input type="checkbox"/> Applications / software	<input type="checkbox"/> Systems security services	<input type="checkbox"/> POS / card present
<input type="checkbox"/> Hardware	<input type="checkbox"/> IT support	<input type="checkbox"/> Internet / e-commerce
<input type="checkbox"/> Infrastructure / Network	<input type="checkbox"/> Physical security	<input type="checkbox"/> MOTO / Call Center
<input type="checkbox"/> Physical space (co-location)	<input type="checkbox"/> Terminal Management System	<input type="checkbox"/> ATM
<input type="checkbox"/> Storage	<input type="checkbox"/> Other services (specify):	<input type="checkbox"/> Other processing (specify):
<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"/> 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:

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.

AudienceView Campus facilitates the transmission of cardholder data by integrating numerous supported payment gateways. E-commerce transactions leverage both hosted payment page (iFrame, hosted fields and full URL redirect) and/or an API call to the payment gateway. Cardholder data is not stored.

Additionally, AudienceView Campus receives transactional data (limited to the last 4 digits of the credit card) from point-of-sale device transactions via the payment gateway. For clarity, the POS devices connect directly to the payment gateways for authorization and the transaction details are sent to AudienceView for reconciliation purposes. AudienceView are considered a reseller for these POS devices but is not involved in the shipping, installation or maintenance of the devices. PCI compliance related to the POS devices is the responsibility of the merchants and therefore considered out of scope for this assessment.

Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.

Not applicable.

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	Boston, MA, USA
Corporate Office	1	Toronto, ON, Canada
Azure	1	Virginia, USA



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)
Not applicable.				

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 Campus environment is hosted in Azure. All web connections/transmissions that contain cardholder data are transmitted through Cloudflare.

The critical systems examined in this assessment include:

- Web servers
- Database servers
- Cisco AnyConnect - Secure VPN connector
- Cloudflare - Web Application firewall
- Microsoft Authenticator App – MFA
- Azure Active Directory and Active Directory on-prem (master) – Authentication and User Management Platform
- Microsoft 365 Defender for endpoint – Malware protection solution and FIM
- Microsoft Intune – MDM solution
- Azure network security groups - Virtual firewall
- KnowBe4 - Security Awareness Platform
- ZAP - Web application security scanner
- Azure Bastion - Virtual Machine connector



	<ul style="list-style-type: none">• Azure DevOps - cloud-based DevOps services• Azure Recovery services vault - Backup solution• Datadog - Cloud Monitoring• Microsoft SQL Server Management Studio - Database Management solution (SQL infrastructure)• Jira and Azure Boards - SDLC management solution and change management system
--	--

<p>Does your business use network segmentation to affect the scope of your PCI DSS environment? <i>(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)</i></p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p>
--	--



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:
AlienVault	SaaS
Cloudflare	SaaS
CyberSource	Payment processing (Non-Hosted)
CyberSource	Payment processing (Hosted)
Transact Campus Payments Inc.(Cashnet HPP)	Payment processing(Hosted)
Transact Campus Payments Inc.(Cashnet)	Payment processing (Non-Hosted)
Moneris	Payment processing (Non-Hosted)
Moneris (MonerisCheckout)	Payment processing(Hosted)
Bluefin Payment Systems	Payment processing (Non-Hosted)
Paypal	Payment processing (Non-Hosted)
Stripe Inc.	Payment processing (Hosted)
TouchNet Information Systems	Payment processing (Hosted)
Paymenttech LLC.	Payment processing (Non-Hosted)
Nelnet Business solutions Inc.	Payment processing (Hosted)
FreedomPay Inc.	Payment processing (Non-Hosted)
Global Payments Direct Inc.	Payment processing (Hosted)



ACI Payments Inc.	Payment processing (Non-Hosted)
Govolution LLC.	Payment processing (Non-Hosted)
Elavon North America	Payment processing (Non-Hosted)

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 Campus		
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"/>	1.2.2 - No routers in scope. 1.2.3 - No wireless networks in scope. 1.3.1, 1.3.2 - DMZ not required in this architecture. 1.3.3, 1.3.5 - Azure responsibility. 1.3.6 - Cardholder data is not stored.
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2.1.1 - No wireless networks in scope. 2.2.3 - No insecure protocols in use.
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3.1, 3.4 (all), 3.5 (all), 3.6 (all) - Cardholder data is not stored.
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	4.1.1 - No wireless networks in scope. 4.2 - PAN is not sent via end-user messaging.
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Not applicable.
Requirement 6:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	6.4.4 - Test data is not propagated to production. 6.4.6 - No significant changes within the assessment period.
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Not applicable.
Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	8.6 - No physical tokens in use.
Requirement 9:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Physical security is Azure's responsibility and there are no POI devices in scope of this assessment.



Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Not applicable.
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	11.1 (all) - Azure's responsibility. 11.2.3 - Rescans were not required in this assessment.
Requirement 12:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Not applicable.
Appendix A1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	A1.1, A1.3, A1.4 - The Campus SaaS solution restricts merchant access to basic configurations.
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	There are no early versions of SSL/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:	March 8, 2024
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 March 8, 2024.

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 AudienceView Campus 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 AudienceView Campus 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: 30%;">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 Revision 2, 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, CVN2, CVV2, or CID 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 MNP LLP |

Part 3b. Service Provider Attestation

Eric White

Eric White (Mar 18, 2024 16:53 MDT)

Signature of Service Provider Executive Officer ↑	Date: 18/03/2024
Service Provider Executive Officer Name: Eric White	Title: Chief Executive Officer

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	Confirmation of scope, documentation and evidence review, interviews with subject matter experts, review of changes and updates.
--	--

DocuSigned by:

Tom Beaupre

F76260A5D7374C2...

Signature of Duly Authorized Officer of QSA Company ↑	Date: 3/19/2024
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:	Not applicable.
---	-----------------

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



DISCOVER
Global Network



VISA






MNP_AudienceView - ROC_AOC_March 14_2024_r1 (002)

Final Audit Report

2024-03-18

Created:	2024-03-18
By:	Lacey Juk (lacey.juk@audienceview.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAADFNMidE-GBQgA8Ezo8tHaWBfFcvZmki

"MNP_AudienceView - ROC_AOC_March 14_2024_r1 (002)" History

-  Document created by Lacey Juk (lacey.juk@audienceview.com)
2024-03-18 - 2:24:12 PM GMT
-  Document emailed to Eric White (eric.white@audienceview.com) for signature
2024-03-18 - 2:24:17 PM GMT
-  Email viewed by Eric White (eric.white@audienceview.com)
2024-03-18 - 10:52:23 PM GMT
-  Document e-signed by Eric White (eric.white@audienceview.com)
Signature Date: 2024-03-18 - 10:53:13 PM GMT - Time Source: server
-  Agreement completed.
2024-03-18 - 10:53:13 PM GMT