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:	eSentire	DBA (doing business as):			
Contact Name:	Greg Crowley	Title:	CISO		
Telephone:	519.651.2200	E-mail:	Greg.crowley@esentire.com		
Business Address:	451 Phillip Street	City:	Waterloo		
State/Province:	Ontario	Country:	Canada	Zip:	N2L 3X2
URL:	www.esentire.com				

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

Company Name:	MNP LLP				
Lead QSA Contact Name:	Melanie Dodson	Title:	Senior Manager Cyber Security		
Telephone:	905-607-9777	E-mail:	melanie.dodson@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:	Network, Endpoint, Log, Cloud
Type of service(s) assessed:	

Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
☐ Applications / software	☒ Systems security services	☐ POS / 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		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Shared Hosting Provider		
☐ Other Hosting (specify): Not applicable - eSentire is not a Hosting Service Provider		
☐ 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:	Cyber forensics and response investigation

Type of service(s) not assessed:

Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
□ Applications / software	□ Systems security services	□ POS / 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		
□ Security services		
□ 3-D Secure Hosting Provider		
□ Shared Hosting 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:	Not currently in scope of assessment

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	eSentire, as a managed service provider, does not store, process, or transmit cardholder data as part of its business. eSentire sensors (Network, Log, Endpoint and Cloud) can be used to help a customer achieve compliance with specific PCI controls. eSentire may transmit and temporarily store incidental cardholder data if it is present in a packet capture file (PCAP) pulled for investigative purposes. The transmission and subsequent temporary storage are limited to the transmission of the PCAP from the eSentire sensor to the eSentire CloudShark secure environment.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	eSentire sensors (Network, Log, Endpoint and Cloud) can be used to help a customer achieve compliance for specific PCI controls by offering system security services.

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*
Corporate Office	1	Waterloo, ON, Canada
Satellite Office/SOC	1	Cork, Ireland
Data Center	1	London, 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)
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.*	eSentire products and services included as part of this assessment provide customers with monitoring, detection and response by ingesting multiple signals and correlating data across the custom-designed, endpoints, logs, and cloud sources. eSentire sensors can be implemented as a virtual system or a physical server. eSentire has no integration with payment processors and does not intentionally collect cardholder data from its customer's infrastructure as part of its services. However, cardholder data may be present in packet capture files pulled by eSentire for investigative purposes. eSentire can also potentially impact the security of the customer's environment through the services they offer and the management of such services.
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:**
AWS	Web hosting and security services
Rogers Communications Inc.	Physical hosting space and security
SumoLogic	SaaS provider SIEM solution
Carbon Black	SaaS provider SIEM solution
Defender	SaaS provider SIEM solution

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:	Network, Endpoint, Log, Cloud

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:	□	☒	□	1.1.3, No CHD flow in eSentire environment 1.2.3 No wireless networks in scope
Requirement 2:	□	☒	□	2.1.1 No wireless networks in scope 2.6 Not a shared hosting provider
Requirement 3:	□	☒	□	3.2 SAD is not collected or stored in the eSentire network 3.4, 3.4.1, 3.5, 3.5.x, 3.6.x, 3.7 The eSentire services assessed do not process, transmit or intentionally store cardholder information.
Requirement 4:	□	☒	□	4.1.1 There are no wireless networks in scope. 4.2 PAN is not sent using end-user messaging.
Requirement 5:	☒	□	□	
Requirement 6:	□	☒	□	6.4.3 No production or test cards 6.4.4 Software development for the sensors does not include test accounts or data. 6.4.6 eSentire confirmed there were no significant changes to the environment during the assessment year. 6.5-6.5.5, 6.5.7-6.5.10, 6.6 eSentire does not provide public-facing application services
Requirement 7:	☒	□	□	

Requirement 8:	☐	☒	☐	8.1.5 – There are no 3rd party accounts permitted to the environment. 8.6 - There are no physical tokens included in scope of this assessment. 8.7 There are no databases storing CHD in scope for eSentire.
Requirement 9:	☐	☒	☐	9.1-9.8.2 Physical security covered by 3rd party hosting providers AWS and Rogers. 9.9. 9.9.1-9.9.3 There are no POS devices in scope 9.10 – Policies are needed as the whole requirement is not applicable.
Requirement 10:	☐	☒	☐	10.5.5 This responsibility is with the SIEM vendor, SumoLogic.
Requirement 11:	☐	☒	☐	11.1.x No wireless in scope, AWS, and Rogers responsible for scanning the data centers. 11.2.3 there were no significant changes to the environment during the assessment year. 11.3.4.1 eSentire does not have a CDE
Requirement 12:	☐	☒	☐	12.3.10 CHD handling is not part of the eSentire scope. 12.8, 12.8.2 Cardholder data is not shared with service providers.
Appendix A1:	☐	☐	☒	Not a shared hosting provider
Appendix A2:	☐	☐	☒	No POS POI and no use of SSL / 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:	May 5, 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 May 5, 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 eSentire 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 eSentire has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: Not applicable 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 Tenable.io

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	*Date:* 05/05/2023
Service Provider Executive Officer Name: Greg Crowley	*Title:* CISO

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.

Tom

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* May 5, 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:	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	☒	☐	
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	☐	☒	Not applicable - the entity is not a Shared Hosting Provider
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☐	☒	Not applicable - the entity does not own, manage nor deploy POS terminals.