Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for
Onsite Assessments – Service Providers

Version 3.0

February 2014

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:	Cayan LLC		DBA (doing business as):		
Contact Name:	Chris McGill		Title:	Security Architect	
ISA Name(s) (if applicable):	Not Applicable		Title:		
Telephone:	(800) 941-6557 x2801		E-mail:	cmcgill@cayan.com	
Business Address:	One Federal Street, 2nd Floor		City:	Boston	
State/Province:	MA	Country:	USA	Zip:	02110
URL:	www.cayan.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	Trustwave				
Lead QSA Contact Name:	James Kist		Title:	Principal Security Consultant	
Telephone:	(312) 873 7500		E-mail:	jkist@trustwave.com	
Business Address:	70 West Madison St, Suite 1050		City:	Chicago	
State/Province:	IL	Country:	USA	Zip:	60602
URL:	www.trustwave.com				

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:	Payment gateway services

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):		
☐ 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.

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

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:	

Part 2b. Description of Payment Card Business

| Describe how and in what capacity your business stores, processes, and/or transmits cardholder data. | Cayan LLC (Cayan) is a Level 1 Service Provider that provides credit card processing services (as a payment gateway) to merchants. Cayan processes card-not-present transactions through e-commerce web sites, and card-present transactions and PIN/debit transactions through integration with POS software. For card-not-present transactions, PAN, expiration date, and card security code are collected. For card-present transactions, full track data is collected. For PIN/debit transactions, full track data and encrypted PIN block is collected. All transactions use TLS to transmit cardholder data to Cayan's servers.

Cayan accepts Visa, MasterCard, American Express, Discover, and JCB.

Cayan stores name on card, expiration date, and encrypted PAN (using 192-bit three-key Triple DES) in a single data repository hosted at a CenturyLink data center in Waltham, MA USA. All transactions are sent over TLS to one of seven processors: First Data Omaha, First Data Nashville, First Data North, First Data Buypass, Global East, BridgePay or TSYS. |
|---|---|
| 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 and a summary of locations included in PCI DSS review (for example, retail outlets, corporate offices, data centers, call centers, etc.):

Type of facility:	Location(s) of facility (city, country):
Corporate Offices	Boston, MA USA
Data Center	Waltham, MA 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)
MerchantWARE	N/A	Cayan	☐ Yes ☒ No	N/A
			☐ Yes ☐ No	
			☐ Yes ☐ 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.*	Systems and networks in Cayan's CDE (payment gateway web servers, payment gateway application services, cardholder database servers) and the IT management networks and systems that provide security and support services to the CDE were included in the scope of this assessment. IT administrator laptops that are used to manage the in-scope systems were also included in the scope of this assessment. Cayan has a direct connection to First Data for the purposes of payment processing. Cayan sends encrypted track data to Magtek for the purposes of decryption, prior to authorization. Cayan sends cardholder data to First Data Merchant Services, First Data Omaha, First Data Buypass, First Data Nashville, First Data North, BridgePay, Global East, and TSYS for the purposes of payment processing.

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 one or more third-party service providers (for example, 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:

Type of service provider:	Description of services provided:
Magtek	Decrypt of full track data
First Data Merchant Services, payment processor	Payment processing
TSYS, payment processor	Payment processing

BridgePay, payment processor	Payment processing
Global East, payment processor	Paymnet processing
First Data Omaha, payment processor	Payment processing
First Data Nashville, payment processor	Payment processing
First Data North, payment processor	Payment processing
First Data Buypass, payment processor	Payment processing
CenturyLink	Co-location 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:	Prepaid Services		

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.)

PCI DSS Requirement	Full	Partial	None	Justification for Approach
Requirement 1:	☒	☐	☐	
Requirement 2:	☐	☒	☐	**PCI-DSS requirement 2.1.1 is not applicable because Cayan does not have wireless networks in the cardholder data environment. PCI-DSS requirement 2.6 is not applicable because Cayan is not a shared hosting provider.**
Requirement 3:	☐	☒	☐	**PCI-DSS requirement 3.4.c is not applicable because cardholder data is never written to removable media.** **PCI-DSS requirement 3.4.1 is not applicable because disk encryption is not used.** **PCI-DSS requirement 3.6.6 is not applicable because clear-text key operations are not in use.**
Requirement 4:	☐	☒	☐	**PCI-DSS requirement 4.1.1 is not applicable because Cayan does not have wireless networks in the cardholder data environment.**
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	**PCI-DSS requirement 6.5.10 is not applicable because this ROC is being completed before June 30, 2015**
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	**PCI-DSS requirement 8.1.5 is not applicable because there are no vendor accounts in the in-scope environment.**

Requirement 9:	☐	☒	☐	**PCI-DSS requirements 9.9.x are not applicable because Cayan does not maintain any POS systems.**
Requirement 10:	☒	☐	☐	
Requirement 11:	☐	☒	☐	**PCI-DSS requirement 11.1.1 is not applicable because there are no wireless access points in use in the cardholder data environment.**
Requirement 12:	☐	☒	☐	**PCI-DSS requirement 12.9 is not applicable because this ROC is being completed before June 30, 2015. PCI-DSS requirement 12.3.9 is not applicable because there are no vendor accounts in the in-scope environment.**
Appendix A:	☐	☐	☒	**PCI-DSS requirements A.1.1 through A.1.4 are not applicable because Cayan is not a shared hosting provider.**

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:	*22 June 2015*
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

Based on the results noted in the ROC dated *22 June 2015*, 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 as of *22 June 2015*: (*check one):*

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *Cayan LLC* 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 *(Service Provider Company Name)* 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 *3.0*, 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, CID, or CVV2 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 *Trustwave*

---

[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.
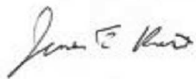
Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	Date: 6/22/2015
Service Provider Executive Officer Name: Paul Vienneau	Title: CTO

Part 3c. QSA Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	QSA performed the assessment.

Signature of QSA ↑	Date: 22 June 2015
QSA Name: James Kist	QSA Company: Trustwave

Part 3d. ISA Acknowledgement (if applicable)

If an ISA was involved or assisted with this assessment, describe the role performed:	Not applicable.

Signature of ISA ↑	Date:
ISA Name:	Title:

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	☒	☐	