Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for
Onsite Assessments – Service Providers

Version 3.2

April 2016

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:	AffiniPay		DBA (doing business as):			
Contact Name:	James Sparrow		Title:	CTO		
Telephone:	512-716-8570		E-mail:	james@affinipay.com		
Business Address:	3700 N Capital of Texas Hwy, Suite 420		City:	Austin		
State/Province:	TX	Country:	USA		Zip:	78746
URL:	www.affinipay.com					

Part 1b. Qualified Security Assessor Company Information (if applicable)						
Company Name:	ControlScan, Inc.					
Lead QSA Contact Name:	Timothy Cunningham		Title:	Senior Security Consultant		
Telephone:	404-844-2181		E-mail:	tcunningham@controlscan.com		
Business Address:	11475 Great Oaks Way, #300		City:	Alpharetta		
State/Province:	GA	Country:	USA		Zip:	30022
URL:	www.controlscan.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:	AffiniPay Payment Gateway

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): Tokenization Services

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:	All other AffiniPay Services.

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): All AffiniPay Services other than the Payment Gateway

Provide a brief explanation why any checked services were not included in the assessment:	This is a separate service unrelated to CHD processing. Infrastructure and operations are effectively segmented.

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	AffiniPay is a Service Provider that provides a p payment gateway to integrated merchants. Through this service, AffiniPay processes card-not-present payment transactions for E-commerce organizations and card-present transactions originating in client POI applications. The AffiniPay Payment Gateway allows merchant clients to offer one-time or recurring payments to their end-users. Storage: AffiniPay stores PAN (no SAD) protected by AES 256 encryption for both one-time and/or recurring transactions within a SQL database. One-time transactions are stored for 180 days to support refunds; recurring transactions are stored for the life of the account (indefinitely). One-time tokens are provided for one-time transactions, and reusable tokens are provided for recurring transactions. Processing: AffiniPay connects to TSYS and First Data, both PCI-compliant payment gateway services, for payment authorization. Transmittal: CHD is transmitted to the AffiniPay Gateway hosted at Amazon Web Services (AWS) from the e-commerce clients over HTTPS/TLS 1.0, 1.1 or 1.2, and then from AWS to TSYS Issuing Processing for processing over HTTPS/TLS1.2. AWS and TSYS provide CHD security within their systems. Both entities provide PCI-compliant services, attested to in Attestations of Compliance provided by third-party QSAs.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	AffiniPay is acting as a Service Provider in such that it owns and maintains the entire Payment Gateway infrastructure and software processes, including all application development/maintenance controls in scope for PCI-DSS.

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):
Corporate Office	1	Austin, TX
Production Data Center -- AWS	2	Eastern Region Western Region (backup)

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)
None	----------	----------	☐ 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.*

Connections into and out of the cardholder data environment (CDE) using the Internet such as remote access, AWS administrative interface or through the public facing web application.

Development, maintenance and operation of the AffiniPay Payment Gateway application.

Application logic, mechanisms and processes for protection of stored PAN data.

Application logic, mechanisms and processes for tokenization of PAN data.

Mechanisms and processes for protection of PAN data in transmission between end-user entry and the payment gateway.

The components which perform segmentation, including the public facing web stack, AWS ELB, AWS Security Groups, AWS RDS Databases, AWS S3, and other AWS supporting services.

Human Resources and associated training.

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:
Amazon Web Services	Cloud services including infrastructure and platform-as-a-service, storage services, and integrated security services.
TSYS	Payment processing services.
First Data	Payment processing 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:	AffiniPay Payment Gateway			
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:	☐	☒	☐	1.1.6.b: N/A - No insecure services, protocols or ports are allowed.
Requirement 2:	☐	☒	☐	2.1.1: N/A - There is no wireless within scope. 2.2.3: N/A - There are no insecure service in the CDE. 2.6: N/A - The entity is not assessed as a shared hosting provider.
Requirement 3:	☐	☒	☐	3.4.1: N/A – No disk encryption.
Requirement 4:	☐	☒	☐	4.1.h: N/A – No POS terminals in scope. 4.1.1: N/A - There is no wireless within scope.
Requirement 5:	☒	☐	☐	
Requirement 6:	☒	☐	☐	
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	8.5.1: N/A – AffiniPay is not a Service Provider with remote access to clients.
Requirement 9:	☐	☒	☐	9.5.1 – 9.7.1: N/A – No movement of CHD to removeable media. 9.9: N/A – No physical card interaction devices in scope.

Requirement 10:	☐	☒	☐	10.8: N/A -- This requirement is not currently implemented and is categorized as a best practice recommendation until 1/31/2018.
Requirement 11:	☒	☐	☐	
Requirement 12:	☒	☐	☐	
Appendix A1:	☐	☐	☒	All Appendix A1: N/A – The entity is not assessed as a shared hosting provider.
Appendix A2:	☒	☐	☐	

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:	*5/15/2017*
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 *5/15/2017.*

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 *AffiniPay* 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 --------- 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*, 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, ControlScan.

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	*Date:* 6-1-2017
Service Provider Executive Officer Name: James Sparrow	*Title:* VP of Technology

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

If a QSA was involved or assisted with this assessment, describe the role performed:	*A QSA performed all testing and evidence review. The QSA completed all sections of the Report on Compliance.*

Signature of Duly Authorized Officer of QSA Company ↑	*Date: 6/1/2017*
Duly Authorized Officer Name: Timothy J Cunningham	*QSA Company:* ControlScan, Inc.

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	☒	☐	---------