Payment Card Industry (PCI)

Data Security Standard

5/29/2021

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:	AffiniPay		DBA (doing business as):	----	
Contact Name:	James Sparrow		Title:	VP of Technology	
Telephone:	512-716-8570		E-mail:	james@affinipay.com	
Business Address:	3700 N Capital of Texas Hwy, Suite 420		City:	Austin	
State/Province:	Texas	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:	Brandon Barney		Title:	Principal Security Consultant	
Telephone:	603-440-1055		E-mail:	bbarney@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 Methods Service & AffiniPay Payment Gateway	
Type of service(s) assessed:		
Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☒ Other Hosting (specify): AffiniPay Payment Methods Service	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify): --------	**Payment Processing:** ☐ POS / card present ☒ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (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 services not explicitly outlined in the previous section	
Type of service(s) not assessed:		
Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify): ---	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify): ---	**Payment Processing:** ☐ POS / card present ☐ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (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 Applicable	

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 payment gateway and hosted payment field services for card-not-present transactions to e-commerce organizations and card-present transactions originating in client POI applications. **AffiniPay Payment Gateway** The AffiniPay Payment Gateway (formerly called the ChargeIO Gateway) is a REST-oriented payment gateway hosted within the Amazon Web Services (AWS) PCI-certified infrastructure. Payment requests are initiated via HTTPS requests over TLSv1.2 using HTTP Basic authentication from merchant sites and partner applications. These requests are routed by Amazon's Route 53 DNS to an Amazon Elastic Load Balancer, at which point transport layer security is terminated (all further request processing occurs within Amazon's secured environment). The request is then forwarded to one of multiple Payment Gateway server processes executing on an Amazon EC2 instance.

	When a Payment Gateway server receives a request, the authentication credentials are first checked against the hashed credentials in the Gateway's database (an Amazon RDS instance with automatic failover support). After the credentials are verified, data flow varies depending on the nature of the request, as described below: Card authorizations can be performed by supplying the card details in the request itself, or through the use of a payment token. Payment tokens allow integrating merchant sites and partners to avoid the PCI compliance requirements that come with storing sensitive card details during the interaction between submission of a payment request and the processing of that request by the Payment Gateway. A caller can submit a payment form directly to the Gateway, or through the payment method service to receive a payment token. The Payment Gateway stores the card details and returns the payment token to the payment form. The caller can then proceed with the payment request to the Payment Gateway by passing the token instead of the card details. This tokenization model is used by a number of modern payment gateways. When authorizing payments using a token, the Payment Gateway must securely maintain the payment card details until the caller performs the authorization request, passing the token. The Payment Gateway encrypts all sensitive data prior to storage in the database. Upon receiving the token, the Payment Gateway retrieves the card details from the database, decrypts the contents, and deletes the card details from the database. The authorization request then proceeds as though the card details were provided directly in the request. The Payment Gateway automatically deletes from the database any card details associated with tokens within five minutes of creation. Authorization requests including card details are first stored in the Payment Gateway's database before being sent to a payment processing network (e.g., TSYS). Sensitive card data such as the card number is encrypted prior to storage. Card security code and magnetic stripe data is not stored in the database; this data is maintained in memory until the interaction with the processing network is complete. Following authorization, the card number and payment processing network response is stored encrypted in the Payment Gateway database until the data is archived. All card transaction data is archived after 180 days, at which point all encrypted sensitive data is deleted or replaced with masked versions. Following authorization, card transactions can be retrieved for viewing and modified through the transaction operations: void, capture, and refund. All operations are authenticated and authorized to verify the caller has the rights necessary to perform the operation. Unless performed using administrative access, none of these operations return sensitive card details in the clear; card numbers are always returned in masked form. Administrative access is available only through a local HTTP port on the server machine. Authorized users may also register webhook URLs to receive card transaction events. This mechanism allows

	the caller to be notified as changes occur to transactions for which they have access, such as successful and rejected batch captures. The content of these events is similar to the data returned when retrieving card transactions; no sensitive data is ever returned in the clear, and all card numbers are returned in masked form. The Payment Gateway uses Amazon's Simple Notification Service (SNS) for communication and synchronization between server processes using dedicated SNS topics that require AWS credentials for subscription. The Payment Gateway also communicates with AffiniPay's non-Cardholder Data environment via message-passing over the Kafka message bus; via HTTPS to HashiCorp Consul for configuration and service discovery; and via HTTPS to HashiCorp Vault for secrets and data encryption key acquisition. No card details are sent to or received from Kafka, Consul, or Vault. The Payment Gateway database is replicated within Amazon's RDS environment for failover support. AWS automatically maintains a hot standby replica in a separate availability zone within the same region as the master, as well as a read replica in a separate region. In addition, automatic nightly backups of the database are performed, of which two are always immediately available within the AWS infrastructure. **AffiniPay Payment Methods Service** The AffiniPay Payment Methods Service is a REST-oriented tokenization service hosted within the Amazon Web Services (AWS) PCI-certified infrastructure, providing backend support to a hosted payment fields implementation. Tokenization requests are initiated via HTTPS requests over TLSv1.2 from merchant sites and partner applications. These requests are routed by Amazon's Route 53 DNS to an Amazon Elastic Load Balancer, at which point transport layer security is terminated (all further request processing occurs within Amazon's secure environment). The request is then forwarded to one of multiple Payment Methods Service server instances executing on an Amazon EC2 docker host instance. Card authorizations are performed through the use of a payment method. A caller receives a payment method by using the AffiniPay Hosted Fields solution on their site. The caller's site initializes a payment form containing credit card number and CVV fields inside HTML iframes which serve code hosted in AffiniPay's PCI-certified infrastructure. The hosted fields JavaScript library loaded in the iframe interacts with the Payment Methods Service to tokenize field contents on UI changes. When the payment form is submitted, the hosted field token IDs and accompanying non-sensitive payment form contents are POST'ed to the Payment Methods Service. The tokenized contents are retrieved, and the full payment data is sent to the Payment Gateway over an HTTPS TLSv1.2 connection to obtain a Payment Gateway payment token. The caller then proceeds with the payment request to the Payment Gateway by passing the received token instead of the card details.

	When a Payment Methods Service server receives a field tokenization request with either a credit card number or a card verification value, the data is encrypted using a 256-bit AES cipher (AES/CBC/PKCS5Padding) using a Base-64 encoded key and sent to a Redis cluster hosted by Amazon Web Services (AWS) along with a generated Base-62 UUID identifier. This data is stored with a 5 minute time-to-live and is automatically deleted from Redis if not used within that 5-minute window. The Base-62 UUID identifier is returned as the field token ID to the requesting iframe embedded in the payment form. When a Payment Methods Service server receives a payment method request with credit card number and CVV token IDs and cardholder details, it retrieves encrypted package envelopes from the Redis cluster, decrypts the package payloads and combines the resulting raw credit card and CVV values with cardholder details sent by the payment form to create a payment token on the AffiniPay Payment Gateway. This payment token is passed on to the payment form and is not persisted by the Payment Methods Service.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	AffiniPay acts as a Service Provider and owns/maintains the entire AffiniPay Payment Gateway and Payment Methods infrastructure and software processes, including application development and maintenance controls in scope for PCI.

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, Texas, USA
Production Data Center – Amazon Web Services (AWS)	2	Eastern and Western AWS Regions

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.	Connections into and out of the cardholder data environment (CDE) using the Internet such as

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.*	remote access, AWS administrative interface or through the public facing web application. Development, maintenance and operation of the AffiniPay Payment Gateway application and Payment Methods Service. 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.
First Data	Payment processing services.
TSYS	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 Methods Service and 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:	☐	☒	☐	1.2.3: Not Applicable – Wireless is not used in the AffiniPay cardholder data environment.
Requirement 2:	☐	☒	☐	2.1.1 (all): Not Applicable – Wireless is not used in the AffiniPay cardholder data environment. 2.2.3: Not Applicable – There are no insecure services, protocols, or daemons in the AffiniPay cardholder data environment. 2.6: Not Applicable – AffiniPay is not a shared hosting provider
Requirement 3:	☐	☒	☐	3.2.a, b: Not Applicable – AffiniPay does not support issuing services. 3.4.1 (all): Not Applicable – Disk encryption is not used in the AffiniPay cardholder data environment. 3.6.6 – Not Applicable – Manual clear-text cryptography is not used.
Requirement 4:	☐	☒	☐	4.1.1: Not Applicable – Wireless is not used in the AffiniPay cardholder data environment.
Requirement 5:	☒	☐	☐	----------
Requirement 6:	☒	☐	☐	----------
Requirement 7:	☒	☐	☐	----------

Requirement 8:	☐	☒	☐	8.1.5: Not Applicable – There are no vendor or third party accounts in the AffiniPay environment. 8.5.1: Not Applicable – AffiniPay does not have remote access to any client environment.
Requirement 9:	☐	☒	☐	9.5.1 – 9.7.1: Not Applicable – Backup media is not created in the AffiniPay environment. 9.8, 9.8.1: Not Applicable – No hard-copy material or media containing cardholder data is created in the AffiniPay environment. 9.8.2: Not Applicable – No electronic media containing cardholder data is created in the AffiniPay environment. 9.9 (all): Not Applicable – AffiniPay does not use physical devices to interact with payments in the cardholder data environment.
Requirement 10:	☒	☐	☐	----------
Requirement 11:	☒	☐	☐	----------
Requirement 12:	☒	☐	☐	----------
Appendix A1:	☐	☐	☒	Requirement A1: Not Applicable – AffiniPay is not a shared hosting provider
Appendix A2:	☐	☐	☒	Requirement A2: Not Applicable – AffiniPay does not have any POS POI devices in use in the cardholder data environment.

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:	5/29/2021	
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 *5/29/2021.*

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 *3.2.1*, 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, Inc.*

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	Date: 5/29/2021
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:	The QSA performed testing, observations, interviews, evidence collection, and reporting as required to complete the PCI DSS Assessment.

Signature of Duly Authorized Officer of QSA Company ↑	Date: 5/29/2021
Duly Authorized Officer Name: Brandon Barney	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 for Card-Present POS POI Terminal Connections	☒	☐	----------