Payment Card Industry (PCI)

Data Security Standard

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:	EVO Merchant Services, LLC		DBA (doing business as):	PayFabric	
Contact Name:	Walid Barakat		Title:	Senior Vice President, IT Governance, Risk and Compliance	
Telephone:	+1 (770) 829-8548		E-mail:	Walid.barakat@globalpay.com	
Business Address:	5595 Windward Parkway		City:	Alpharetta	
State/Province:	GA	Country:	USA	Zip:	30005
URL:	https://www.evopayments.com				

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

Company Name:	VikingCloud				
Lead QSA Contact Name:	Dean Massiah		Title:	Senior Security Consultant	
Telephone:	+1 833-903-3469		E-mail:	deanmassiah@vikingcloud.com	
Business Address:	70 West Madison Street, Suite 400		City:	Chicago	
State/Province:	IL	Country:	USA	Zip:	60602
URL:	https://www.vikingcloud.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:	PayFabric	
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):	**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		

***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

Type of service(s) not assessed:

Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
□ Applications / software □ Hardware □ Infrastructure / Network □ Physical space (co-location) □ Storage □ Web □ Security services □ 3-D Secure Hosting Provider □ Shared Hosting Provider □ Other Hosting (specify):	□ Systems security services □ IT support □ Physical security □ Terminal Management System □ Other services (specify):	□ 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.	EVO Merchant Services, LLC (EVO Merchant Services), dba EVO Payments International, LLC, is classified as Level 1 Service Provider. EVO Merchant Services, LLC provides payment processing for merchants throughout the United States. EVO Merchant Services, LLC processes and transmits cardholder data to its payment processors over TLS v1.2 secured connections using AES 256-bit CBC RSA 2048-bit symmetric encryption to facilitate the authorization and settlement of payments for merchants utilizing the following channels: - Card-Present: Retail POS Swipe, Chip transactions - PIN/Debit: Retail POS Swipe, Chip transactions - Card-Not-Present: Retail Manual Entry and Call Center - Phone Support (recorded) Card Holder Data is stored as part of EVO Merchant Services' normal operations as follows: - EVO also processes transactions from merchants over dial (POTS) connections. Recorded calls by EVO Merchant Services from merchant customers to the Help Desk are protected using AES 256-bit encryption. Cardholder data is not stored during calls. - Tokenized by EVO Merchant Services and saved to databases as part of transaction processing, reoccurring transactions, and chargebacks - Encrypted (AES-128, 3DES-168, and RSA-2048, AES 256-bit) by EVO Merchant Services and stored in databases for batch processing for settlement - Encrypted (AES 256-bit) by EVO Merchant Services and stored to disk as part of the settlement process - Tokenized by EVO Merchant Services and stored in databases, for bulk export to 3rd party service providers upon merchant customer request. EVO Merchant Services, LLC, stores, processes and transmits cardholder data to facilitate authorizations, recurring transactions and historical data for reporting along with risk/fraud, chargebacks and Help Desk support.

	The PayFabric application is hosted, developed, and managed by EVO Merchant Services, LLC. It is included among the suite of applications which comprise EVO Merchant Services, LLC's assessment. EVO Merchant Services, LLC, stores, processes and transmits cardholder data to facilitate authorizations, recurring transactions and historical data for reporting along with risk/fraud, chargebacks and Help Desk support.
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):
Corporate Data Centers	2	Portland, ME USA
		Moorestown, NJ USA
US Headquarters / Chargeback Center	1	Melville, NY USA
Call Centers	2	Tampa, FL USA
		Farmers Branch, TX 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)
NGTrans	Proprietary	EVO Merchant Services LLC	☐ Yes ☒ No	Not Applicable
SNAP*	Proprietary	EVO Merchant Services LLC	☐ Yes ☒ No	Not Applicable
Sterling Gateway	6.9	EVO Merchant Services LLC	☐ Yes ☒ No	Not Applicable
Payfabric	Proprietary	EVO Merchant Services LLC	☐ Yes ☒ No	Not Applicable
A360	Proprietary	EVO Merchant Services LLC	☐ Yes ☒ No	Not Applicable
E360	Proprietary	EVO Merchant Services LLC	☐ Yes ☒ No	Not Applicable
Onboard	Proprietary	EVO Merchant Services LLC	☐ Yes ☒ No	Not Applicable

eSafe	Proprietary	EVO Merchant Services LLC	☐ Yes ☒ No	Not Applicable
Spoon	Proprietary	EVO Merchant Services LLC	☐ Yes ☒ No	Not Applicable
Sterling Tokenizer	2.5	EVO Merchant Services LLC	☐ Yes ☒ No	Not Applicable
TRR	Proprietary	EVO Merchant Services LLC	☐ Yes ☒ No	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.*

EVO Merchant Services LLC systems included in this assessment are:

- Internally Developed Applications:
  - NGTrans
  - Onboard
  - Spoon
  - Payfabric
  - SNAP
  - Sterling Gateway
  - Sterling Tokenizer
  - eSafe
  - A360
  - E360
  - TRR
- Firewalls
- Router
- Switches
- Load Blanacers
- WAFs
- SANs
- VOIP Systems
- Administration Workstations
- Remote authentication systems
- Windows Operating systems
- Linux Operating Systems
- Database servers
- Web servers
- Multifactor Authentication
- Active Directory Services
- Anti-Virus
- SIEM
- FIM/HSM
- IDS/IPS

	- Network Segements: ○ Portland, ME USA Data Center ○ Moorestown, NJ USA Data Center - Network connections to processors: ○ Chase Paymentech ○ TSYS ○ Discover ○ American Express ○ MasterCard ○ Visa ○ Global Payments ○ FIS (Fidelity Information Services) ○ eGlobal ○ Paytrace ○ NMI ○ First Data ○ PayPal ○ USA ePay ○ WorldPay ○ Forte ○ FundPaising ○ CyberSource ○ Authorize.net
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:**
Global Payments	Transaction processing
Chase Paymentech	Transaction processing
Total Systems (Tsys Acquiring Solutions)	Transaction processing
FIS	Debit Payment Processing
PayTrace	Transaction processing
eGlobal	Transaction processing
Fiserv	Debit Payment Processing
NMI	Transaction processing

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:	Payfabric			
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:	☒	□	□	
Requirement 2:	□	☒	□	2.1.1 – CDE wireless is not present 2.2.3 – No insecure services, daemons, or protocols in use 2.6 – EVO Merchant Services is not a shared hosting provider
Requirement 3:	□	☒	□	3.6 - Keys are not shared. 3.6.6 – Clear-Text Key-Management is not utilized.
Requirement 4:	□	☒	□	4.1.1 – CDE wireless is not present.
Requirement 5:	☒	□	□	
Requirement 6:	□	☒	□	6.4.6 – No significant changes
Requirement 7:	☒	□	□	
Requirement 8:	□	☒	□	8.1.5 - No vendor accounts exist. 8.5.1 – No remote access into any customer's environment.
Requirement 9:	□	☒	□	9.6.2, 9.6.3, 9.7.1 - Removable media is not utilized

				9.9, 9.9.1, 9.9.2, 9.9.3 – EVO Merchant Services does not maintain any physical POS devices.
Requirement 10:	☒	☐	☐	
Requirement 11:	☐	☒	☐	11.1.1 - CDE wireless is not present
Requirement 12:	☒	☐	☐	
Appendix A1:	☐	☐	☒	EVO Merchant Services is not shared hosted provider
Appendix A2:	☐	☐	☒	Early TLS Is not utilized

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:	*October 26, 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 *October 26, 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 *EVO Merchant Services, 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 *3.2.1*, 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 *Qualys*

Part 3b. Service Provider Attestation	
Signature of Service Provider Executive Officer ↑	*Date:* **October 26, 2023**
Service Provider Executive Officer Name: **Guido Sacchi**	*Title:* **Senior EVP & CIO**

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)	
If a QSA was involved or assisted with this assessment, describe the role performed:	Dean Massiah was the QSA who was responsible for the assessment, on-site assessment, remote evidence and generation and completion of the Report on Compliance.
Signature of Duly Authorized Officer of QSA Company ↑	*Date: October 26, 2023*
Duly Authorized Officer Name: Dean Massiah	*QSA Company:* VikingCloud

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	☒	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☒	☐	