Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for
Onsite Assessments - Service Providers

Version 3.2.1

Using the PCI Security Standards Council Template dated **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:	Payrix Holdings, LLC	DBA (doing business as):	Payrix, LLC Payrix Solutions, LLC Benchmark Merchant Solutions, LLC Payrix Canada Corp.
Contact Name:	Jack Tsigankov	Title:	Director - IT & Information Security
Telephone:	+1 (215) 500-4263	E-mail:	jack.tsigankov@payrix.com
Business Address:	5605 Glenridge Drive, Suite 375	City:	Atlanta
State/Province:	Georgia	Country:	United States of America	Zip:	30342
URL:	https://www.payrix.com		

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

Company Name:	A-LIGN Compliance and Security, Inc. dba A-LIGN		
Lead QSA Contact Name:	John Bowman	Title:	Senior Consultant
Telephone:	+1 (888) 702-5446	E-mail:	john.bowman@A-LIGN.com
Business Address:	400 N. Ashley Drive, Suite 1325	City:	Tampa
State/Province:	Florida	Country:	United States of America	Zip:	33602
URL:	https://www.A-LIGN.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 Facilitator Platform (PayFac Platform)

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.*

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	☐ 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 Applicable.

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Payrix provides a payment platform, providing authorization and settlement services, as well as transaction analysis services including risk identification and fraud detection. Payrix maintains a database for storing encrypted cardholder data on behalf of their customers to enable scheduled recurring payments to be processed. All credit card information is received by the Payrix API via encrypted connections and stored encryption within a cloud service provider. When processing transactions, Payrix uses encrypted connections to send cardholder data to the processor.
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 Office	1	Atlanta, Georgia, United States of America
Office	1	Toronto, Ontario, Canada
AWS Data Center US East (N. Virginia)	1	Virginia, United States of America

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.	Not Applicable.	Not Applicable.	☐ 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._	The assessed environment consisted of multiple networks hosted within a PCI compliant cloud service provider as well as web application, and database servers used to receive, process, and store cardholder data in the Payrix environment. Each network contained connections into and out of the CDE to support payment gateway connections. The assessment focused on the Also included in the assessment were the firewalls used to segment the CDE from the Internet and other untrusted networks, and

	connections made to the processor to share transaction data for 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 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:**
Amazon Web Services	Colocation datacenter and hosting provider
Millennium Digital Technologies	VPN provider for access to Vantiv Core and host for transaction authorization
Evo Payments, Inc	ISO-Merchant, VISANET processor, and TPS-PIN
Worldpay, Inc.	Merchant servicer, payment facilitator, and third-party servicer
Wells Fargo	Merchant servicer, payment facilitator, and third-party servicer
Fiserv - Electronic Payments	Merchant servicer and third-party servicer
Lexis Nexis	Third-party risk servicer
Sift Science	Third-party risk servicer

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:	Payment Facilitator Platform (PayFac Platform)

	Details of Requirements Assessed			
PCI DSS Requirement	**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:	☐	☒	☐	Not Applicable. - 1.2.3 - The Payrix CDE is hosted within a controlled PCI compliant cloud-based environment where wireless networks are prohibited. Not Applicable. - 1.3.6 - Cardholder data is not stored within the Payrix environment.
Requirement 2:	☐	☒	☐	Not Applicable. - 2.1.1 - There are no wireless environments connected to the Payrix CDE. Not Applicable. - 2.2.3 - There are no insecure services, protocols, or daemons present in the Payrix environment. Not Applicable. - 2.6 - Payrix is not a shared hosting provider.
Requirement 3:	☐	☒	☐	Not Applicable. - 3.6 - Payrix is a service provider but does not share keys. Not Applicable. - 3.6.6 - Payrix does not use manual clear-text cryptographic methods.
Requirement 4:	☐	☒	☐	Not Applicable. - 4.1.1 - There are no wireless networks connected to the Payrix CDE.
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	Not Applicable. - 6.4.6 - There were no significant changes in the last 365 days.
Requirement 7:	☒	☐	☐	

Requirement 8:	☐	☒	☐	Not Applicable. - 8.1.5 - No vendor accounts are granted access to the environment. Not Applicable. - 8.5.1 - Payrix is a service provider but does not have any logical access to any client environment.
Requirement 9:	☐	☒	☐	Not Applicable. - 9.1.2 - Clients have no access to AWS datacenters. AWS does not make any network jacks available in their datacenters. Not Applicable. - 9.5 - Cardholder data was not handled or stored to any media within the Payrix CDE. Not Applicable. - 9.5.1-9.6.1, 9.7-9.8.1.b - Removeable media backups of cardholder data are not maintained within the Payrix CDE. Not Applicable. - 9.6.2 - Removable media was not utilized for storage of cardholder data or shipped offsite to another location. Not Applicable. - 9.6.3 - Removeable media was not utilized for storage of cardholder data or permitted to be moved without proper authorization. Not Applicable. - 9.8.2 - Cardholder data was not stored on any electronic media. Not Applicable. - 9.9-9.9.3 - Payrix does not utilize devices that capture payment card data via direct physical interaction with the card.
Requirement 10:	☒	☐	☐	
Requirement 11:	☐	☒	☐	Not Applicable. - 11.1-11.1.2 - There are no wireless access points, authorized or maintained within the Payrix environment. Not Applicable. - 11.2.3 - There were no significant changes in the last 365 days. Not Applicable. - 11.3.3 - There were no exploitable vulnerabilities found.
Requirement 12:	☒	☐	☐	
Appendix A1:	☐	☐	☒	Not Applicable. - A1 - Payrix is not a shared hosing provider.
Appendix A2:	☐	☐	☒	Not Applicable. - A2 - Payrix does not utilize any POS/POI devices.

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:	27 February 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 27 February 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 **Payrix, 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 - 3728-01-16).

Part 3b. Service Provider Attestation

Evgeniy Tsigankov

Signature of Service Provider Executive Officer ↑	*Date:* 21 March 2023
Service Provider Executive Officer Name: Evgeniy (Jack) Tsigankov	*Title:* Director - IT & Information Security

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

If a QSA was involved or assisted with this assessment, describe the role performed:	The assessor provided PCI DSS advisory and assessment services, which included observation of controls, interviews with key personnel, and review of policies and procedures.
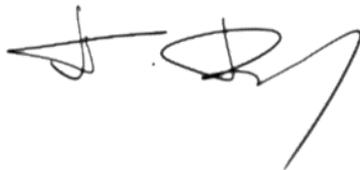
Signature of Duly Authorized Officer of QSA Company ↑	*Date:* 21 March 2023
Duly Authorized Officer Name: Petar Besalev, EVP Cybersecurity and Compliance Services	*QSA Company:* A-LIGN

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.
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☐	☐	Not Applicable.