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:	Shift4 Payments LLC		DBA (doing business as):		
Contact Name:	Andrew Soriano		Title:	Sr. Compliance Program Manager	
Telephone:	949.307.7912		E-mail:	asoriano@shift4.com	
Business Address:	2202 N. Irving Street		City:	Allentown	
State/Province:	PA	Country:	USA	Zip:	18109
URL:	www.shift4.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	Dara Security				
Lead QSA Contact Name:	Barry Johnson		Title:	President/CEO	
Telephone:	775.622.5386		E-mail:	barryj@darasecurity.com	
Business Address:	10580 N. McCarran Blvd #115-337		City:	Reno	
State/Province:	NV	Country:	USA	Zip:	89503
URL:	www.darasecurity.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 and Merchant Services	
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): Risk Management, Non-Transactional Call Center		

***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: ☐ 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:		

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	The Shift4 solution is sold to merchants as a Software-as-a-Service (SaaS) offering. Shift4 supplies payment card authorization, accounting, fraud detection, and settlement services to a large, worldwide merchant client base. Shift4 provides a standard Application Service Provider (ASP) model and facilitates secure connections with merchant clients using proprietary, PA-DSS v.3.2 validated, Application Program Interface (API) applications. These Shift4 APIs are capable of securely connecting merchant client Point-of-Sale (POS) systems to credit, debit and private label transaction processors and acquirers and are also able to provide a complete tokenization solution allowing merchant clients to never deal with CHD in any of their systems. Shift4 provides for a web-based virtual terminal interface allowing merchants to manual enter CHD for payment purposes. Transactions are sent to the payment gateway over the Internet via a TLS 1.2 connection or, for specified merchants, over a dedicated MPLS connection from the merchant via a TLS 1.2 connection. Based on the merchant's acceptance method, transaction may contain full PAN, Expiration Date, cardholder identification data (name & address), Full Track, and card validation code (CVV/CVC). Once authorization occurs, sensitive authentication data (SAD) is securely wiped. The PAN and expiry date are retained with the PAN encrypted. Shift4 returns a unique token to the merchant for their future use. Shift4 also supports a call center to provide non-transactional support to merchants that need to make payment adjustments, confirm a transaction occurred, or perform a refund. A call center technician will receive the call and if needed for support, will use an in-house application to retrieve the full PAN from storage and provide the PAN to the merchant over the phone. The call center technician does not initiate any form of transaction. These calls are recorded by the Calabrio call center VoIP platform and said recordings are encrypted and stored. Shift4 has a risk management group that uses an acquirer provided portal to assist merchants with risk management due to chargebacks.
Describe how and in what capacity your business is	Shift4 accepts Cardholder Data (CHD) into their

otherwise involved in or has the ability to impact the security of cardholder data.	environment for both “Card-Present” and “Card-Not-Present” credit transactions. Shift4 acts as a value-added transaction payment gateway and provides a secure connection between merchant clients and their acquirer of record. For the merchant, Shift4 provides PA-DSS validated API payment components to facilitate transactions to interact with the Shift4 payment gateway solution. These solutions utilize encrypted connectivity over the Internet to connect to the Shift4 environment. Shift4’s transmission technologies, client tokenization solutions, and secure transaction processing environment ensure that CHD is secured and protected throughout the entire transaction process. All storage of merchant CHD is housed securely in separate merchant databases residing in MS-SQL servers on internal network segments. All the tokenized and/or transactional data in each merchant database is fully encrypted using Blowfish (cipher-block chaining using a 256-bit key). Backups of all merchant data are also fully encrypted and remain under the control of Shift4 personnel. Shift4 also provides a call center to support merchants needing to confirm transactions occurred, to perform refunds, or to perform payment adjustments.

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):
Example: Retail outlets	*3*	*Boston, MA, USA*
Corporate Office	1	Allentown PA USA
Office	2	Las Vegas NV USA Silver Spring MD USA
Data Center	1	Las Vegas NV USA
Data Center	1	Austin TX USA
Data Center	1	Tampa FL USA
Data Center	1	Sterling VA 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)
In-House		Shift4 Payments	☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ 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.*	Assessment addressed all system components within the CDE to include database servers, application servers, and web servers. Assessment covered connection to payment processors and development of the software used by entity in delivery of their services. Assessment also assessed implemented policies and procedures governing security and PCI DSS compliance
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:**
Switch	Data Center Provider
CyrusOne	
Cyxtera	
Alliance Data Systems	Processor
American Express	
Anvil	
BlueFin	
Capital One	
Ceridan	
Chase Paymentech	
Citcon	
DHISCO	
Discover	
Elavon USA	
FCIB	
First Data	
GE Capital	
Givex	
Global Payment Systems	
GPS	
Hammer	

Heartland Payment Systems L Brands Lighthouse Mastercard Mercury Payments Moneris Nexcom Pegasus Padial Seven Springs Spacenet Spinner Stored Value Switch TCC Total Solutions (TSYS) Up Vantiv Visa Direct	
Assured Document Destruction	Media Destruction

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 Gateway and Merchant 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.)
Requirement 1:	☐	☒	☐	1.2.2 - N/A - No routers within CDE 1.2.3 - N/A - No wireless within CDE
Requirement 2:	☐	☒	☐	2.1.1 - N/A - No wireless within CDE 2.2.3 - N/A - No insecure service deployed. 2.6 - N/A - Entity not a shared hosting provider
Requirement 3:	☐	☒	☐	3.4.1 - N/A - Disk encryption not used within CDE 3.6.a - N/A - Cryptographic keys not shared with customers 3.6.6 - N/A - Manual-text cryptographic process not utilized
Requirement 4:	☐	☒	☐	4.1.1 - N/A - No wireless deployed
Requirement 5:	☒	☐	☐	
Requirement 6:	☒	☐	☐	
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	8.5.1 - N/A - No access to customer premises
Requirement 9:	☐	☒	☐	9.5 - 9.7.1 - N/A - Removable media not utlized by entity

				9.8.1 - N/A - Hardcopies of card data not maintained or generated 9.9 - 9.9.3 - N/A - Entity does not manage POI device
Requirement 10:	☒	☐	☐	
Requirement 11:	☒	☐	☐	
Requirement 12:	☒	☐	☐	
Appendix A1:	☐	☐	☒	N/A - Not a Shared Hosting Provider
Appendix A2:	☐	☒	☐	N/A - early TLS and SSL not supported

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:	06-May-2022	
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 06-May-2022.

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 Shift4 Payments 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 AppSec Consulting & Qualys

Part 3b. Service Provider Attestation

Mike Russo Digitally signed by Mike Russo
Date: 2022.05.06 09:23:09 -07'00'

Signature of Service Provider Executive Officer ↑	*Date:* 6-May-2022
Service Provider Executive Officer Name: Mike Russo	*Title:* Chief Technology Officer

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

If a QSA was involved or assisted with this assessment, describe the role performed:	Level 1 PCI DSS Audit and Review

Barry Johnson

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* 06-May-2022
Duly Authorized Officer Name: Barry Johnson	*QSA Company:* Dara Security

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	☒	☐