Payment Card Industry (PCI)
Payment Application
Data Security Standard (PA-DSS)

Attestation of Validation

Version 3.2

May 2016

PA-DSS Attestation of Validation

Instructions for Submission

The Payment Application Qualified Security Assessor (PA-QSA) must complete this document as a declaration of the payment application's validation status with the Payment Application Data Security Standard (PA-DSS).

The PA-QSA and Payment Application Software Vendor should complete all applicable sections and submit this document along with copies of all required validation documentation to PCI SSC, per PCI SSC's instructions for report submission as described in the *PA-DSS Program Guide*.

Part 1. Payment Application Vendor and Qualified Security Assessor Information

Part 1a. Payment Application Vendor Information

Company Name:	Shift4®				
Contact Name:	Stephen Ames		Title:	Sr. Director Information Security	
Telephone:	702.597.2480		E-mail:	sames@shift4.com	
Business Address:	1481 Center Crossing Road		City:	Las Vegas	
State/Province:	NV	Country: USA		Postal Code:	89128
URL:	www.shift4.com				

Part 1b. Payment Application Qualified Security Assessor (PA-QSA) Company Information

PA-QSA Company Name:	Dara Security				
Lead PA-QSA Name:	Barry Johnson		Title:	President/CEO	
Telephone:	775.600.2470		E-mail:	barryj@darasecurity.com	
Business Address:	10580 N. McCarran Blvd #115-337		City:	Reno	
State/Province:	NV	Country: USA		Postal Code:	89503
URL:	www.darasecurity.com				

Part 2. Submission Type

Identify the type of submission and complete the indicated sections of this Attestation of Validation associated with the chosen submission type (check only one).

☒	**Full Validation**	Complete Parts 3a, 3c, 4a, 4d, 5a, & 5c
☐	**Annual Revalidation**	Complete Parts 3b, 3c, 4b, & 4d
☐	**Administrative Change**	Complete Parts 3a, 3b, 3c, 4c, 4d, 5b, & 5c
☐	**No Impact Change**	Complete Parts 3a, 3b, 3c, 4c, 4d, 5b, & 5c
☐	**Low Impact Change**	Complete Parts 3a, 3b, 3c, 4c, 4d, 5b, & 5c
☐	**High-Impact Change**	Complete Parts 3a, 3c, 4a, 4d, 5a, & 5c

PCI Security Standards Council

Part 3. Payment Application Information

Part 3a. Payment Application Identification

Payment Application name(s) and version number(s) included in this PA-DSS review:

Application Name: Secure Suite 4 MICROS 3700	Version Number: 1.8
Required Dependencies: Shift4 Universal Transactoin Gateway 4.7 and MICROS 3700 Hardware	
☐ The Payment Application was assessed and is validated to use wildcards as part of its versioning methodology.	
☒ The Payment Application does not use wildcards as part of its versioning methodology.	

Part 3b. Payment Application References

Reference Payment Application name and version number currently on the PCI SSC List of Validated Payment Applications:

Application Name:	Existing Version Number:
PCI SSC Reference Number:	Required Dependencies:
Description of change, if applicable:	

Part 3c. Payment Application Functionality & Target Market

Payment Application Functionality (check only one):

☐ Automated Fuel Dispenser	☐ POS Kiosk	☐ Payment Gateway/Switch
☐ Card-Not-Present	☒ POS Specialized	☐ Payment Middleware
☐ POS Admin	☐ POS Suite/General	☐ Payment Module
☐ POS Face-to-Face/POI	☐ Payment Back Office	☐ Shopping Cart & Store Front

Target Market for Payment Application (check all that apply):

☒ Retail	☐ Processors	☐ Gas/Oil
☐ e-Commerce	☒ Small/medium merchants	
☐ Others (please specify):		

Part 4. Payment Application Vendor Attestation

Company asserts the following status for the application(s) and version(s) identified in Part 3 of this document as of the date noted in Part 4d *(Complete one of Parts 4a, 4b, or 4c; and Part 4d)*:

Part 4a. Confirmation of Validated Status: (each item to be confirmed)

☒	The PA-QSA has been provided with all documentation and resources necessary to reach an accurate assessment of the PA-DSS compliance status of the Payment Application and version noted in part 3a.
☒	No track data (magnetic-stripe data or equivalent data on the chip), CAV2, CVC2, CID, or CVV2 data, or PIN data is stored subsequent to transaction authorization on ANY files or functionalities generated by the application.
☒	We acknowledge our obligation to provide end-users of the Payment Application and version noted in part 3a (either directly or indirectly through their resellers and integrators) with a current copy of the validated payment application's *PA-DSS Implementation Guide.*
☒	We have adopted and implemented documented Vulnerability Handling Procedures in accordance with Section 2(a)(i)(C) of the *Vendor Release Agreement* dated *07/06/2016*, and confirm we are and will remain in compliance with our Vulnerability Handling Procedures.

Part 4b. Annual Re-Validation Confirmation:

Based on the results noted in the PA-DSS ROV dated *(date of ROV)*, Company asserts the following as of the date noted in Part 4d:

***Note**: Part 4b is for the required Annual Attestation for listed payment applications, and should ONLY be completed if:*

- *No modifications have been made to the Payment Application covered by this AOV; OR*
- *A validated wildcard versioning methodology is being used and **only No Impact changes** have been made to the Payment Application covered by this AOV.*

☐	No modifications have been made to the Payment Application and version noted in part 3b
☐	Payment Application and version noted in part 3b uses a validated wildcard versioning methodology and only No Impact changes have been made.
☐	Vendor confirms that all tested platforms, operating systems, and dependencies upon which the application relies remain supported.
☐	Vendor confirms that all methods of cryptography provided or used by the payment application meet PCI SSC's current definition of "strong cryptography."

Part 4c. Change Analysis for No Impact/Low Impact Changes

Based on internal change analysis and the Vendor Change Analysis documentation, Company asserts the following status for the application(s) and version(s) identified in Part 3 of this document as of the date noted in Part 4d (check applicable fields):

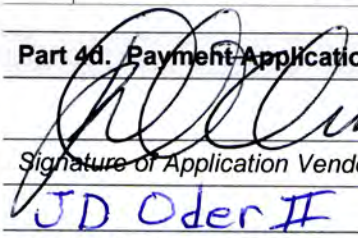
☐	**Only changes** resulting in **No Impact** or **Low Impact** to the PA-DSS requirements have been made to the "Parent" application noted above to create the new application also noted above.
☐	All changes have been applied in a way that is consistent with our documented software-versioning methodology for this application in accordance with the *PA-DSS Program Guide,* and are accurately recorded in the Vendor Change Analysis provided to the PA-QSA noted in Part 1b.

☐	All information contained within this attestation represents the results of the Vendor Change Analysis fairly in all material respects.

Part 4c. Change Analysis for No Impact/Low Impact Changes (continued)

☐	No track data (magnetic-stripe data or equivalent data on the chip), CAV2, CVC2, CID, or CVV2 data, or PIN data is stored subsequent to transaction authorization on ANY files or functionalities generated by the application.
☐	All methods of cryptography provided or used by the payment application meet PCI SSC's current definition of "strong cryptography."
☐	We acknowledge our obligation to provide end-users of the Payment Application and version noted in part 3b (either directly or indirectly through their resellers and integrators) with the updated copy of the validated payment application's *PA-DSS Implementation Guide.*

Part 4d. Payment Application Vendor Acknowledgment

	2016-10-05
Signature of Application Vendor Executive Officer ↑	*Date* ↑
JD Oder II	CTO / Co-Founder
Application Vendor Executive Officer Name ↑	*Title* ↑
Shift4®	
Application Vendor Company Represented ↑	

Part 5. PA-QSA Attestation of PA-DSS Validation

Based on the results noted in the PA-DSS ROV dated *10/3/2016*, PA-QSA Company asserts the following validation status for the application(s) and version(s) identified in Part 3 of this document as of the date noted in Part 5c *(Complete one of Parts 5a or 5b; and Part 5c)*:

Part 5a. Confirmation of Validated Status: (each item to be confirmed)

☒	**Fully Validated:** All requirements in the ROV are marked "in place," thereby the Payment application and version noted in part 3a has achieved full validation with the Payment Application Data Security Standard.
☒	The ROV was completed according to the PA-DSS, version *3.2*, in adherence with the instructions therein.
☒	All information within the above-referenced ROV and in this attestation represents the results of the assessment fairly in all material respects.
☒	No evidence of track data (magnetic-stripe data or equivalent data on the chip), CAV2, CVC2, CID, or CVV2 data, or PIN data storage exists after transaction authorization on ANY files or functionalities generated by the application during this PA-DSS Assessment.

Part 5b. Low/No Impact Change – PA-QSA Impact Assessment

Based on the Vendor Change Analysis documentation provided by the Payment Application Vendor noted in Part 1a, *(Lead PA-QSA Name)* asserts the following status for the application(s) and version(s) identified in Part 3 of this document as of the date noted in Part 5c (check applicable fields). Based on our review of the Vendor Change Analysis documentation, we agree that the documentation supports the vendor's assertion that **only Low Impact or No Impact changes** have been made to the application noted above, resulting in:

☐	**No Impact** to the PA-DSS Requirements and security-related functions
☐	**Low Impact** to the PA-DSS Requirements and security-related functions

Part 5c. PA-QSA Acknowledgment

Barry Johnson	10/4/2016
Signature of Lead PA-QSA ↑	*Date ↑*
Barry Johnson	President/CEO
Lead PA-QSA Name ↑	*Title ↑*
Dara Security	
PA-QSA Company Represented ↑	

Part 6. PCI SSC Acceptance

PCI SSC does not assess or validate payment applications for PA-DSS compliance. The signature below and subsequent listing of a payment application on the List of Validated Payment Applications signifies that the applicable PA-QSA has determined that the application complies with the PA-DSS, that the PA-QSA has submitted a corresponding ROV to PCI SSC, and that the ROV, as submitted to PCI SSC, has satisfied all applicable quality assurance review requirements as of the time of PCI SSC's review.

PCI Security Standards Council LLC

Digitally signed by PCI Security Standards Council LLC
DN: cn=PCI Security Standards Council LLC, o, ou, email=PA-DSS@pcisecuritystandards.org, c=US
Date: 2016.11.15 12:51:29 -05'00'

Signature of PCI Security Standards Council ↑ *Date ↑*