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:	Fullsteam Operations LLC		DBA (doing business as):	N/A	
Contact Name:	Fred Byrd		Title:	Chief Technology Officer	
Telephone:	+1 334-750-0903		E-mail:	fred.byrd@fullsteam.com	
Business Address:	540 Devall Dr, Suite 301		City:	Auburn	
State/Province:	AL	Country:	USA	Zip:	36832
URL:	https://www.fullsteam.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	VikingCloud				
Lead QSA Contact Name:	Jeremy Dart		Title:	Sr. Security Consultant	
Telephone:	+1 (833) 970-3100		E-mail:	jeremydart@vikingcloud.com	
Business Address:	405 West Superior Street, 7th Floor		City:	Chicago	
State/Province:	IL	Country:	USA	Zip:	60654
URL:	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:	Hosted Software Solutions: Tapestry, Official Records Online and AVA.	
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 and Forwarding		

***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:	Not Applicable	

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	**Storage:** PAN, cardholder name, and expiry is stored with the Microsoft Azure Platform as a Service (PaaS), within a hosted SQL database. This data is stored using AES 256 for the name and expiry and RSA-OAEP-256 (2048) for the token and PAN, employing the Microsoft Key Vault. PAN, name, and expiry, and CAV2/CVV2/CVC2/CID are held in memory temporarily to support the immediate transaction. Once the transaction is complete, a token is stored in the SQL database alongside the encrypted PAN (RSA-OAEP-256), expiry, and cardholder name (AES-256). CAV2/CVV2/CVC2/CID is garbage collected by the application. Merchants or ISVs (subsidiary, wholly owned organizations) who choose to may process future and reoccurring transactions against that stored token. **Processing:** Cardholder data (PAN, expiry, cardholder name, CAV2/CVV2/CVC2/CID, and full track data) is transmitted to WorldPay/Vantiv over HTTPS/TLS 1.2 for processing and authorization. **Transmission:** All cardholder data is received over port 443 using TLS 1.2. Cardholder data (PAN, cardholder name, expiry, CAV2/CVV2/CVC2/CID, and full track data) once received is formatted and transmitted securely (HTTPS/TLS 1.2) to WorldPay/Vantiv for authorization. Fullsteam's payments gateway and services supporting it are collectively called "FullsteamPay". "FullsteamPay" consists of four primary services which are hosted in the Microsoft Azure CDE: • "FullsteamPay Gateway" - a RESTful payments API where Integrated Software Vendors (ISVs) can submit transaction requests (PAN, expiry, cardholder name, CAV2/CVV2/CVC2/CID) over HTTPS/TLS 1.2. ISVs can also request transaction and historical data for reporting, collect signatures from terminals, gateway status, token creation requests, and other management services. • "MerchantTrack" - a merchant reporting tool. ISVs which do not provide their own payments reporting can provide their client merchants access to the MerchantTrack tool which provides transaction reporting over TLS 1.2. This mechanism only provides transaction data, not CHD.

	• "Admin App" - an internal administrative tool for configuring and maintaining FullsteamPay configuration data and ISV API provisioning. Only Fullsteam personnel can access the Admin App. • "Hosted Payments" - a web site utilized by a FullsteamPay JavaScript SDK for browser-based tokenization to minimize PCI scope for ISVs by use of iFrames. Payment is accepted through the FullsteamPay Gateway for eCommerce and point of sale (POS) transactions. This API facilitates the following payment scenarios: 1) Consumer Card-Not-Present "Hosted" web payments 2) Card-Present POS Internet connected Encrypted PIN Pad payments 3) Card-Present POS USB connected Encrypted Device payments 4) Tokenized Payments Requests 5) Unencrypted PAN payments 6) MerchantTrack Virtual Terminal Payments
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	Auburn, AL, 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)
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).*	• Microsoft Azure PaaS • Processor Connections • Security Infrastructure • Change management systems and protocols

• *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	• Identity and access management systems • Log correlation and security/event management systems • Fullsteam Application • Payment processing • SQL Database • Anti-Malware • Operating Systems • Key Vaults • Connections/communications between Fullsteam and its ISVs and its processor, WorldPay/Vantiv WAFs
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:**
Microsoft Azure	Cloud Hosting Services
WorldPay/Vantiv	Payment Processing
VeryGoodSecurity	Token imports

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:	Hosted Software Solutions: Tapestry, Official Records Online and AVA.

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: N/A – There are no wireless networks in scope. 2.2.3: N/A – No insecure protocols permitted. 2.6: N/A – Fullsteam Operations LLC is not a shared hosting provider.
Requirement 3:	☐	☒	☐	3.4.1: N/A – Disk Encryption not utilized 3.6: N/A – Keys are not shared with customers. 3.6.6: N/A - Manual clear-text cryptographic key-management operations are not used.
Requirement 4:	☐	☒	☐	4.1.1: N/A – There are no wireless networks in use.
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	6.4.6: N/A – There were no significant changes.
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	8.1.3: N/A - No users with access to the CDE have been terminated within the past 6 months. 8.1.5: N/A – No non-consumer customer accounts with access to CDE components exist. 8.5.1: N/A – Fullsteam Operations LLC is not a

				Service Provider with remote access to its clients' environment.
Requirement 9:	☐	☒	☐	9.5, 9.5.1,, 9.6, 9.6.1, 9.6.2, 9.6.3, 9.7, 9.7.1, 9.8, 9.8.1, 9.8.2: N/A – Fullsteam does not maintain any media as part of the CDE. 9.9, 9.9.1, 9.9.2, 9.9.3: N/A - There are no POS devices in scope managed by Fullsteam Operations LLC.
Requirement 10:	☒	☐	☐	
Requirement 11:	☐	☒	☐	11.2.3: N/A – No significant changes requiring rescan 11.3.3: N/A – There were no exploitable vulnerabilities which required retesting.
Requirement 12:	☒	☐	☐	
Appendix A1:	☐	☐	☒	All Appendix A1: N/A – Fullsteam Operations LLC is not a shared hostingprovider.
Appendix A2:	☐	☐	☒	All Appendix A2: N/A – There are no POS devices in scope managed by Fullsteam Operations LLC.

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:	June 10, 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 June 10, 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 *Fullsteam Operations 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 *Control Scan.*

[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 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	*Date:* June 10, 2022
Service Provider Executive Officer Name: Fred Byrd	*Title:* CTO

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

If a QSA was involved or assisted with this assessment, describe the role performed:	VikingCloud QSA Jeremy Dart performed all testing and evidence review. VikingCloud QSA Jeremy Dart completed all sections of the Report on Compliance.

Signature of Duly Authorized Officer of QSA Company ↑	*Date*: June 10, 2022
Duly Authorized Officer Name: Jeremy Dart	*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 - No ISA was involved with the assessment.

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	☒	☐