SAQ A — AOC v3.2 — Faria Systems LLC

Self-Assessment Questionnaire A and Attestation of Compliance

Version 3.2

Section 1: Assessment Information

Part 1. Merchant and Qualified Security Assessor Information

Part 1a. Merchant Organization Information

Company Name: **Faria Systems LLC**

DBA(s): **MANAGEBAC.COM**

Contact Name: **Theodore King**

Title: **Company Representative**

Telephone: **415-670-9038**

Email: **theo@faria.co**

Business Address: **548 Market St. #40438**

City: **San Francisco**

State: **CA**

Zip: **94104**

Country: **USA**

URL: **managebac.com**

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

Company Name: **N/A**

Part 2. Executive Summary

Part 2a. Type of Merchant Business (check all that apply)

[ ] Retailer

[ ] Telecommunication

[ ] Grocery and Supermarkets

[ ] Petroleum

[**x**] E-Commerce

[ ] Mail order/telephone order (MOTO)

[ ] Others

What types of payment channels does your business serve?

[ ] Mail order/telephone order (MOTO)

[x] E-Commerce

[ ] Card-present (face-to-face)

Which payment channels are covered by this SAQ?

[ ] Mail order/telephone order (MOTO)

[**x**] E-Commerce

[ ] Card-present (face-to-face)

Part 2b. Description of Payment Card Business

*How and in what capacity does your business store, process and/or transmit cardholder data?***We do not store, process and/or transmit cardholder data.**

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. **N/A**

Part 2d. Payment Application

Does the organization use one or more Payment Applications? **NO**

Provide the following information regarding the Payment Applications your organization uses: **N/A**

Part 2e. Description of Environment

Provide a high-level description of the environment covered by this assessment:

E-commerce: Our customers dispatch all cardholder data securely to Stripe, our payments processor, via an iframe. Our company's servers receive an opaque token object, from which the original cardholder data cannot be derived.

Does your business use network segmentation to affect the scope of your PCI DSS environment? **YES**

Part 2f. Third-Party Service Providers

Does your company use a Qualified Integrator & Reseller (QIR)? **NO**

Does your company share cardholder data with any 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.)? **YES**

Name of service provider: **Stripe, Inc.**

Description of services provided: *Collection, storage and processing of all cardholder data.*

Part 2g. Eligibility to Complete SAQ A

Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because, for this payment channel:

[**x**] Merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions);

[**x**] All processing of cardholder data is entirely outsourced to PCI DSS validated third-party service providers;

[**x**] Merchant does not electronically store, process, or transmit any cardholder data on merchant systems or premises, but relies entirely on a third party(s) to handle all these functions;

[**x**] Merchant has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; and

[**x**] Any cardholder data the merchant retains is on paper (for example, printed reports or receipts), and these documents are not received electronically..

[**x**] Additionally, for e-commerce channels: All elements of the payment page(s) delivered to the consumer's browser originate only and directly from a PCI DSS validated third-party service provider(s)

Section 2: Self-Assessment Questionnaire A

Completion of a Self-Assessment Questionnaire

The assessment documented in this attestation and in the SAQ was completed on: **December 6, 2016**

Have compensating controls been used to meet any requirement in the SAQ? **No**

Were any requirements in the SAQ identified as being not applicable (N/A)? **Yes**

Were any requirements in the SAQ unable to be met due to a legal constraint? **No**

Requirement 2: Build and Maintain a Secure Network and Systems

2.1: (a) Are vendor-supplied defaults always changed before installing a system on the network? **N/A**

2.1(b) Are unnecessary default accounts removed or disabled before installing a system on the network? **N/A**

Requirement 8: Identify and authenticate access to system components

8.1.1: Are all users assigned a unique ID before allowing them to access system components or cardholder data? **N/A**

8.1.3 Is access for any terminated users immediately deactivated or removed? **N/A**

8.2: In addition to assigning a unique ID, is one or more of the following methods employed to authenticate all users? **N/A**

8.2.3(a) Are user password parameters configured to require passwords/passphrases meet the following? **N/A**

8.5: Are group, shared, or generic accounts, passwords, or other authentication methods prohibited as follows: **N/A**

Requirement 9: Restrict physical access to cardholder data

9.5: Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)? **N/A**

9.6(a): Is strict control maintained over the internal or external distribution of any kind of media? **N/A**

9.6.1: Is media classified so the sensitivity of the data can be determined? **N/A**

9.6.2: Is media sent by secured courier or other delivery method that can be accurately tracked? **N/A**

9.6.3 Is management approval obtained prior to moving the media (especially when media is distributed to individuals)? **N/A**

9.7: Is strict control maintained over the storage and accessibility of media? **N/A**

9.8(a): Is all media destroyed when it is no longer needed for business or legal reasons? **N/A**

9.8.1(a): Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed? **N/A**

9.8.1(b): Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents? **N/A**

Requirement 12: Maintain a policy that addresses information security for all personnel

12.8.1: Is a list of service providers maintained, including a description of the service(s) provided? **YES**

12.8.2: Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment? **YES**

12.8.3: Is there an established process for engaging service providers, including proper due diligence prior to engagement? **YES**

12.8.4: Is a program maintained to monitor service providers' PCI DSS compliance status at least annually? **YES**

12.8.5: Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity? **YES**

12.10.1(a): Has an incident response plan been created to be implemented in the event of system breach? **YES**

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

Based on the results documented in the SAQ A dated **December 6, 2016**, 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 as of **December 6, 2016**: (check one):

[**x**] Compliant: All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby **Faria Systems LLC** has demonstrated full compliance with the PCI DSS.

[ ] Non-Compliant: Not all sections of the PCI DSS SAQ are complete, or not all questions are answered affirmatively, resulting in an overall NON-COMPLIANT rating, thereby **Faria Systems LLC** has not demonstrated full compliance with the PCI DSS.

Target Date for Compliance: N/A

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 your acquirer or the payment brand(s) before completing Part 4.

[ ] Compliant but with Legal exception: One or more requirements are marked “No” due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.

Part 3a. Acknowledgement of Status

[**x**] PCI DSS Self-Assessment Questionnaire A, Version 3.2, was completed according to the instructions therein.

[**x**] All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.

[**x**] I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.

[**x**] I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.

[**x**] If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

[**x**] No evidence of full track data , CAV2, CVC2, CID, or CVV2 data , or PIN data 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

Part 3b. Merchant Attestation

Signature of Merchant Executive Officer: **Theodore King**

Date: _____

Merchant Executive Officer Name: _____

Title: Company Representative

_____

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

If a QSA was involved or assisted with this assessment, describe the role performed: **N/A**

Part 3d. Internal Security Assessor (ISA) Acknowledgement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed: **N/A**

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.

PCI DSS Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters. **N/A**

PCI DSS Requirement 8: Identify and authenticate access to system components. **N/A**

PCI DSS Requirement 9: Restrict physical access to cardholder datas. **N/A**

PCI DSS Requirement 12: Maintain a policy that addresses information security for all personnel. **Yes**

Explanation of Non-Applicability

Reason Requirement is Not Applicable**:** No part of our environment, including any type of media, transmits, stores or processes cardholder data. As such, there is no cardholder data to restrict access to.