Attestation of Compliance, SAQ A, Version 3.1

Section 1: Assessment Information

Part 1. Merchant and Qualified Security Assessor Information

Part 1a. Merchant Organization Information

Company Name: Rhys Williams

DBA(s): CODEWORKSHOP

Contact Name: Rhys Williams

Title: Company Representative

Email: rwilliams@codeworkshop.com.au

Telephone: 0404123300

Business Address: 87 Elvy Street

City: Yanderra

State: NSW

Zip: 2574

Country: AU

URL: www.codeworkshop.com.au

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

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

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:

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 share cardholder data with any third-party service providers (for example, 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:

YES - Merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions);

YES - All processing of cardholder data is entirely outsourced to PCI DSS validated third-party service providers;

YES - 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;

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

YES - Merchant retains only paper reports or receipts with cardholder data, and these documents are not received electronically.

YES - For e-commerce channels, all elements of the payment page or pages delivered to the consumer's browser originate only and directly from a PCI DSS validated third-party service provider.

Section 2: Self-Assessment Questionnaire A

9.5: Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)? Media refers to all paper and electronic media containing cardholder data. N/A

9.6: Is strict control maintained over the internal or external distribution of any kind of media? Controls should include the following: 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: Is all media destroyed when it is no longer needed for business or legal reasons? Media destruction should be performed as follows: N/A

9.8.1: (a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed? (b) Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents? N/A

12.8: Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows: YES

12.8.1: Is a list of service providers maintained? 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

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

Based on the results noted in the SAQ A dated 2016-06-26, 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 2016-06-26:

YES - Compliant: All sections of the PCI SAQ are complete, and all questions answered **yes**, resulting in an overall COMPLIANT rating, thereby Rhys Williams has demonstrated full compliance with the PCI DSS.

NO - 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 Rhys Williams 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 your acquirer or the payment brand(s) before completing Part 4.

NO - 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

YES - This PCI DSS Self-Assessment Questionnaire, Version 3.1, was completed according to the instructions therein.

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

YES - I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.

YES - I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.

YES - If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

YES - No evidence of full track data1, CAV2, CVC2, CID, or CVV2 data2, or PIN data3 storage after transaction authorization was found on ANY system reviewed during this assessment.

N/A - ASV scans are being completed by the PCI SSC Approved Scanning Vendor (ASV Name).

Part 3b. Merchant Attestation

Signature of Merchant Executive Officer: *Rhys Williams*

Date: 2016-06-26

Merchant Executive Officer Name: Rhys Williams

Title: Company Representative

Merchant Company Represented: Rhys Williams

Part 3c. QSA Acknowledgement (if applicable)

N/A

Part 3d. ISA Acknowledgement (if applicable)

N/A

Part 4. Action Plan for Non-Compliant Requirements

N/A

Appendix C: Explanation of Non-Applicability

Requirement: 9.X **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.