



Payment Card Industry (PCI) **Data Security Standard**

eCorner[®]

**Attestation of Compliance for
Self-Assessment Questionnaire A-EP**
For use with PCI DSS Version 3.2.1

July 2018

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the merchant's self-assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact your acquirer (merchant bank) or the payment brands to determine reporting and submission procedures.

Part 1. Merchant and Qualified Security Assessor Information

Part 1a. Merchant Organization Information

Company Name:	eCorner Pty Ltd	DBA (doing business as):	eCorner		
Contact Name:	Grant Longhurst	Title:	Infrastructure Manager		
Telephone:	02 9494 0200	E-mail:	hosting@ecorner.com.au		
Business Address:	Level 7, 91 Phillip Street	City:	Paramatta		
State/Province:	NSW	Country:	Australia	Zip:	2150
URL:	https://www.ecorner.com.au				

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

Company Name:	Stratica Australia Pty Ltd (formerly Stratica International Pty Ltd until November 2019) ABN: 73 095 136 208				
Lead QSA Contact Name:	Manu Khurana (QSA 200-312)	Title:	Senior Associate		
Telephone:	+61396605700	E-mail:	manu.khurana@stratica.com.au		
Business Address:	Unit 8, 651 Victoria Street	City:	Abbotsford		
State/Province:	VIC	Country:	Australia	Zip:	3067
URL:	www.stratica.com.au				

Part 2. Executive Summary

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

- | | | |
|---|--|--|
| <input type="checkbox"/> Retailer | <input type="checkbox"/> Telecommunication | <input type="checkbox"/> Grocery and Supermarkets |
| <input type="checkbox"/> Petroleum | <input checked="" type="checkbox"/> E-Commerce | <input type="checkbox"/> Mail order/telephone order (MOTO) |
| <input type="checkbox"/> Others (please specify): | | |

What types of payment channels does your business serve?

- Mail order/telephone order (MOTO)
 E-Commerce
 Card-present (face-to-face)

Which payment channels are covered by this SAQ?

- Mail order/telephone order (MOTO)
 E-Commerce
 Card-present (face-to-face)

Note: If your organization has a payment channel or process that is not covered by this SAQ, consult your acquirer or payment brand about validation for the other channels.

Part 2b. Description of Payment Card Business

How and in what capacity does your business store, process and/or transmit cardholder data?

eCorner does not store credit cards of Merchants customers. eCorner uses Payment gateways such as eWay, PayPal and Stripe to process cards. eCorner uses the gateways API to send customer information to the gateway.

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)
<i>Example: Retail outlets</i>	3	Boston, MA, USA
eCommerce services hosted within the Macquarie Data Centre	1	Macquarie Park, NSW

Part 2d. Payment Application

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)
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> 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).*

eCorner provides managed e-commerce stores using the ePages platform, for which eCorner is a reseller. Customer stores are run on the ePages multi-tenant environment or within dedicated servers depending upon the selected

<ul style="list-style-type: none"> • <i>Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.</i> 	<p>service type. These hosts are located in an isolated VLAN (EC2-DMZ). eCorner has a private VMWARE cloud hosted environment on private dedicated servers provided and managed by Macquarie Telecom. Macquarie themselves are PCI compliant and provide the PCI coverage up to the physical server layer and anything above that is covered by eCorner. There two dedicated physical Fortigate firewalls sitting in front of the cloud and Macquarie provide "always on" DDOS protection. eCorner does not store credit cards but uses Payment gateways such as PayPal, Stripe and eWay.</p>
---	---

<p>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)</p>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
---	---

Part 2f. Third-Party Service Providers

<p>Does your company use a Qualified Integrator & Reseller (QIR)?</p>	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
---	---

If Yes:

Name of QIR Company:	
QIR Individual Name:	
Description of services provided by QIR:	

<p>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.)?</p>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
--	---

If Yes:

Name of service provider:	Description of services provided:
eWay	Payment Gateway
Paypal	Payment Gateway
Stripe	Payment Gateway
Mastercard Payments	Payment Gateway
Mastercard Payments	Payment Gateway
Worldpay	Payment Gateway
Payment Express (Windcave)	Payment Gateway
BPoint	Payment Gateway
Westpac Quick Gateway Interface	Payment Gateway

Note: Requirement 12.8 applies to all entities in this list.

Part 2g. Eligibility to Complete SAQ A-EP

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

<input checked="" type="checkbox"/>	Merchant accepts only e-commerce transactions;
<input checked="" type="checkbox"/>	All processing of cardholder data, with the exception of the payment page, is entirely outsourced to a PCI DSS validated third-party payment processor;
<input checked="" type="checkbox"/>	Merchant's e-commerce website does not receive cardholder data but controls how consumers, or their cardholder data, are redirected to a PCI DSS validated third-party payment processor;
<input checked="" type="checkbox"/>	If merchant website is hosted by a third-party provider, the provider is validated to all applicable PCI DSS requirements (e.g., including PCI DSS Appendix A if the provider is a shared hosting provider);
<input checked="" type="checkbox"/>	Each element of the payment page(s) delivered to the consumer's browser originates from either the merchant's website or a PCI DSS compliant service provider(s);
<input checked="" type="checkbox"/>	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;
<input checked="" type="checkbox"/>	Merchant has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; and
<input checked="" type="checkbox"/>	Any cardholder data the merchant retains is on paper (for example, printed reports or receipts), and these documents are not received electronically.

Section 2: Self-Assessment Questionnaire A-EP

This Attestation of Compliance reflects the results of a self-assessment, which is documented in an accompanying SAQ.

The assessment documented in this attestation and in the SAQ was completed on:	31 October 2020
Have compensating controls been used to meet any requirement in the SAQ?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the SAQ identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Were any requirements in the SAQ unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ A-EP (Section 2), dated 31 October 2020.

Based on the results documented in the SAQ A-EP 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**):

<input checked="" type="checkbox"/>	<p>Compliant: All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby <i>eCorner</i> has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p>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 (<i>Merchant Company Name</i>) has not demonstrated full compliance with the PCI DSS.</p> <p>Target Date for Compliance:</p> <p>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. <i>Check with your acquirer or the payment brand(s) before completing Part 4.</i></p>						
<input type="checkbox"/>	<p>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.</p> <p><i>If checked, complete the following:</i></p> <table border="1" style="width: 100%;"> <thead> <tr> <th style="width: 35%;">Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met				
Affected Requirement	Details of how legal constraint prevents requirement being met						

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

<input checked="" type="checkbox"/>	PCI DSS Self-Assessment Questionnaire A-EP, Version 3.2.1, was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
<input checked="" type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

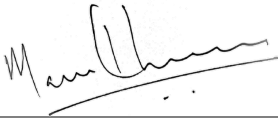
Part 3a. Acknowledgement of Status (continued)

<input checked="" type="checkbox"/>	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.
<input checked="" type="checkbox"/>	ASV scans are being completed by the PCI SSC Approved Scanning Vendor <i>Beyond Security</i>

Part 3b. Merchant Attestation

Signature of Merchant Executive Officer ↑	Date: 5/11/2020
Merchant Executive Officer Name: John Debrincat	Title: Founding CEO and Director

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

If a QSA was involved or assisted with this assessment, describe the role performed:	Review of documentation and evidence, supported remediation of penetration test results.
	
Signature of Duly Authorized Officer of QSA Company ↑	Date: 31 Oct 2020
Duly Authorized Officer Name: Manu Khurana	QSA Company: Stratica Australia

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 your acquirer or the 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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

* PCI DSS Requirements indicated here refer to the questions in Section 2 of the SAQ.

