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:	Caterbook Limited		DBA (doing business as):		
Contact Name:	Chris Noon		Title:	Managing Director	
Telephone:	+44 (0) 1840 298 298		E-mail:	chris@caterbook.com	
Business Address:	19A Normandy Way		City:	Bodmin	
State/Province:	Cornwall	Country:	United Kingdom	Zip:	PL31 1RB
URL:	https://www.caterbook.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	Securious Limited				
Lead QSA Contact Name:	Nigel Peirce		Title:	Senior Cyber Security Consultant	
Telephone:	+44 (0) 1392 247 110		E-mail:	n.peirce@securious.co.uk	
Business Address:	Science Park Centre, 6 Babbage Way, Science Park, Clyst Honiton		City:	Exeter	
State/Province:	Devon	Country:	United Kingdom	Zip:	EX5 2FN
URL:	https://securious.co.uk				

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:	Caterbook PMS	
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):		

***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:	N/A	
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:	N/A	

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Caterbook Ltd does not directly store, process or transmit Cardholder Data as all payment card activities are dealt with by Level 1 service providers; currently Cardstream and PCI Booking. To support online payments via the website Iframe functionality is used. This is submitted directly from the cardholder's web browser to Cardstream located at secure.caterbook.net for payment processing. If OTAs send raw CHD this is passed through PCI Bookings who store and tokenize the CHD prior to removing the CHD information before it is sent to Caterbook Ltd's PMS.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Caterbook Ltd. is in scope for PCI DSS as a service provider since Caterbook owns the Caterbook PMS and is responsible for it's future development, support and

	maintanence. Caterbook Ltd. can therefore impact the iframe payment mechanism.

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):
Example: Retail outlets	*3*	*Boston, MA, USA*
Corporate Head Office	1	Bodmin, Cornwall, UK

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)
N/A	N/A	N/A	☐ Yes ☐ No	N/A
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ 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).* • *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	The Caterbook PMS is hosted within Microsoft Azure using the Azure App Service (Platform as a Service). An iframe is used for CHD capture from cardholders and hoteliers. CHD is transmitted directly from the web browser to the level 1 service provider Cardstream who provides the iframe and supports payment processing. Any CHD retrieved from Online Travel Agents (OTAs) is via PCI Booking which is a Level 1 Tokenization service provider.

	CHD is tokenized and only the token is exposed to Caterbook PMS. Azure DevOps is used to manage the Caterbook PMS code base.
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:	N/A
QIR Individual Name:	N/A
Description of services provided by QIR:	N/A
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	Provides Azure platform (PaaS) which is used to host Caterbook PMS
Cardstream	Provides iFrame facility to allow for card payment authorisation and settlement services
PCI Booking	Tokenization Service Provider used to tokenize cardholder data received from Online Travel Agents. Payments from PCI Booking are facilitated through Cardstream

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:	Caterbook PMS

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:	☐	☐	☒	The QSA determined that the Caterbook PMS meets SAQ A eligibility, therefore this requirement is not applicable.
Requirement 2:	☐	☒	☐	As assessment aligned the requirements to SAQ A, only Requirement 2.1 is in scope. All other requirements have been classified as "Not Applicable".
Requirement 3:	☐	☒	☐	As this is a Report On Compliance, Requirements 3.2.1, 3.2.2 and 3.2.3 are included as in scope, the remaining elements of Requirement 3 is marked as "Not Applicable" as this ROC is being aligned to SAQ A and no requirements from Requirement 3 are in scope for SAQ A.
Requirement 4:	☐	☐	☒	The QSA determined that the Caterbook PMS meets SAQ A eligibility, therefore this requirement is not applicable.
Requirement 5:	☐	☐	☒	The QSA determined that the Caterbook PMS meets SAQ A eligibility, therefore this requirement is not applicable.
Requirement 6:	☐	☒	☐	As assessment aligned the requirements to SAQ A, only Requirement 6.2 is in scope. All other

				requirements have been classified as "Not Applicable".
Requirement 7:	☐	☐	☒	The QSA determined that the Caterbook PMS meets SAQ A eligibility, therefore this requirement is not applicable.
Requirement 8:	☐	☒	☐	As assessment aligned the requirements to SAQ A, only Requirement 8.1.1, 8.1.3, 8.2, 8.2.3 and 8.5 are in scope. All other requirements have been classified as "Not Applicable".
Requirement 9:	☐	☐	☒	The QSA determined that the Caterbook PMS meets SAQ A eligibility, therefore this requirement is not applicable.
Requirement 10:	☐	☐	☒	The QSA determined that the Caterbook PMS meets SAQ A eligibility, therefore this requirement is not applicable.
Requirement 11:	☐	☐	☒	The QSA determined that the Caterbook PMS meets SAQ A eligibility, therefore this requirement is not applicable.
Requirement 12:	☐	☒	☐	As assessment aligned the requirements to SAQ A, only Requirement 12.8, 12.8.1, 12.8.2, 12.8.3, 12.8.4, 12.8.5 and 12.10 are in scope. All other requirements have been classified as "Not Applicable"
Appendix A1:	☐	☐	☒	Caterbook is not a shared hosting provider
Appendix A2:	☐	☐	☒	Caterbook does not interact with CHD therefore this requirement is not applicable. The QSA also ran a scan using SSL Labs against secure.caterbook.net (which points to Cardstream) which only supports TLS 1.2.

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:	12th May 2021	
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 12th May 2021**.**

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 Caterbook Limited 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 Sec-1 Ltd

Part 3b. Service Provider Attestation

Chris Noon

Signature of Service Provider Executive Officer ↗	*Date:* 05/20/2021
Service Provider Executive Officer Name: Chris Noon	*Title:* Managing Director

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

If a QSA was involved or assisted with this assessment, describe the role performed:	The QSA performed the PCI DSS assessment, the scope was aligned and validated to SAQ A. All applicable requirements were reviewed and assessed by the QSA. The QSA completed the ROC and AOC.

N. Peirce

Signature of Duly Authorized Officer of QSA Company ↗	*Date:* 05/20/2021
Duly Authorized Officer Name: Nigel Peirce	*QSA Company:* Securious Limited

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:	N/A

[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 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	☐	☐