Payment Card Industry
Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0

Revision 1

Publication Date: December 2022

PCI DSS v4.0 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: Company Kitchen

Assessment End Date: 26-Jan-2024

Date of Report as noted in the Report on Compliance: 07-Feb-2024

Section 1   Assessment Information

Instructions for Submission

This Attestation of Compliance (AOC) must be completed as a declaration of the results of the service provider's assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures (*"Assessment"). Complete all sections. The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which this AOC will be submitted for reporting and submission procedures.

This AOC reflects the results documented in an associated Report on Compliance (ROC). Associated ROC sections are noted in each AOC Part/Section below.

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Report on Compliance Template.

Part 1. Contact Information	
Part 1a. Assessed Entity **(ROC Section 1.1)**	
Company name:	Company Kitchen
DBA (doing business as):	
Company mailing address:	1743 Maplelawn Dr. Troy, MI 48084
Company main website:	www.companykitchen.com
Company contact name:	Syed Umair Azim
Company contact title:	Compliance Officer
Contact phone number:	888.365.6282
Contact e-mail address:	syed.azim@365smartshop.com
Part 1b. Assessor **(ROC Section 1.1)**	
Provide the following information for all assessors involved in the Assessment. If there was no assessor for a given assessor type, enter Not Applicable.	
PCI SSC Internal Security Assessor(s)	
ISA name(s):	Not Applicable
Qualified Security Assessor	
Company name:	Dara Security
Company mailing address:	10580 N. McCarran Blvd. #115-337 Reno NV 89503
Company website:	www.darasecurity.com
Lead Assessor name:	Barry Johnson
Assessor phone number:	775.622.5386
Assessor e-mail address:	barryj@darasecurity.com

Assessor certificate number:	040-001

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were <u>INCLUDED</u> in the scope of the Assessment (select all that apply):

Name of service(s) assessed:	MicroMarket, Vending, & Food Service Technology

Type of service(s) assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☒ POI / card present
☐ Hardware	☐ IT support	☒ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web-hosting services		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service Provider		
☐ Other Hosting (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): Self-Service Stand Along Kiosk, Attended and unattended food service terminals and vending machines

Note: These categories are provided for assistance only and are not intended to limit or predetermine an entity's service description. If these categories do not apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.

Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were <u>NOT INCLUDED</u> in the scope of the Assessment (select all that apply):

Name of service(s) not assessed:	Not Applicable

Type of service(s) not assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POI / card present
☐ Hardware	☐ IT support	☐ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web-hosting services		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service Provider		
☐ Other Hosting (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:	

Part 2b. Description of Role with Payment Cards (ROC Section 2.1)

Describe how the business stores, processes, and/or transmits account data.	Web Presence: Customers login to the Company Kitchen LLC (Company Kitchen) web portal through a web browser and are presented with web pages served up by web servers located in the Company Kitchen virtual private cloud (VPC). These VPCs are an Infrastructure as a Service (IaaS) offered by Amazon Web Services (AWS). Cardholder data is entered on the web page and immediately transmitted to First Data or CyberSource for transaction authorization. If the transaction is approved, the requested funds are debited to the customer's gift card/account. At no time is cardholder data stored in the Company Kitchen VPC.

	Only non-transaction activity details are stored (e.g., what was purchased, quantity, etc.) for later billing back to the Operator.
	Kiosks:
	Company Kitchen provides food pantry services to Operators. Company Kitchen kiosks contain a magnetic stripe reader device (MSR) that is used to encrypt cardholder data at swipe or insertion. Operators are responsible for inspection and inventory of kiosks. Cardholder data is not stored or processed by Company Kitchen. Encrypted cardholder data is sent directly to the acquirer for authorization. Transaction information (e.g., item, quantity, time of purchase, etc.) is retained by Company Kitchen for later billing to Operators.
	Mobile App:
	The Company Kitchen mobile app utilizes the First Data or CyberSource PCI DSS certified back-end solution for e-commerce transactions.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Entity is not exposed to clear-text CHD. All CHD is collected by the POI device deployed within the kiosk and encrypted by the POI device. This information is sent directly to the processor for payment processing. Upon completion of processing the truncated PAN is provided to the Company Kitchen backend environment along with results of the transaction request. For e-Commerce transactions, all CHD is entered into an iFrame presented by the processor with CHD sent directly to the processor upon submission by the consumers web browser.
Describe system components that could impact the security of account data.	Kiosks and servers supporting the solution.

Part 2c. Description of Payment Card 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 POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.* • *System components that could impact the security of account data.*	Assessment addressed all system components within the CDE to include database servers, application servers, and web servers. Assessment covered connection to payment processors and development of the software used by entity in delivery of their services. Assessment also assessed implemented policies and procedures governing security and PCI DSS compliance.
Indicate whether the environment includes segmentation to reduce the scope of the Assessment. (Refer to the "Segmentation" section of PCI DSS for guidance on segmentation)	☒ Yes ☐ No

Part 2d. In-Scope Locations/Facilities

(ROC Section 4.6)

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this Assessment.

Facility Type	Total Number of Locations (How many locations of this type are in scope)	Location(s) of Facility (city, country)
Example: Data centers	*3*	*Boston, MA, USA*
Corporate office	1	Troy MI USA
Data Center	1	AWS Data Center

Part 2e. PCI SSC Validated Products and Solutions

(ROC Section 3.3)

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions*?

☐ Yes   ☒ No

Provide the following information regarding each item the entity uses from PCI SSC's Lists of Validated Products and Solutions:

Name of PCI SSC-validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which Product or Solution Was Validated	PCI SSC Listing Reference Number	Expiry Date of Listing
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD

*   For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components, appearing on the PCI SSC website (www.pcisecuritystandards.org) (for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Payment Applications (PA-DSS), Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, and Contactless Payments on COTS (CPoC) solutions).

Part 2f. Third-Party Service Providers

*(*ROC Section 4.4*)*

For the services being validated, does the entity have relationships with one or more third-party service providers that:	
• Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage))	☒ Yes ☐ No
• Manage system components included in the entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers)	☒ Yes ☐ No
• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	☒ Yes ☐ No

If Yes:

Name of Service Provider:	Description of Services Provided:
Amazon Web Services	Data Center Provider
Heartland Payment Systems First Data CyberSource	Processors

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

Part 2g. Summary of Assessment
(ROC Section 1.8.1*)*

Indicate below all responses provided within each principal PCI DSS requirement.

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If Below Method(s) Was Used	
	In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Customized Approach**	**Compensating Controls**
Requirement 1:	☒	☒	☐	☐	☐	☐
Requirement 2:	☒	☒	☐	☐	☐	☐
Requirement 3:	☒	☒	☐	☐	☐	☐
Requirement 4:	☒	☒	☐	☐	☐	☐
Requirement 5:	☒	☒	☐	☐	☐	☐
Requirement 6:	☒	☐	☐	☐	☐	☐
Requirement 7:	☒	☐	☐	☐	☐	☐
Requirement 8:	☒	☒	☐	☐	☐	☐
Requirement 9:	☒	☒	☐	☐	☐	☐
Requirement 10:	☒	☐	☐	☐	☐	☐
Requirement 11:	☒	☒	☐	☐	☐	☐
Requirement 12:	☒	☒	☐	☐	☐	☐
Appendix A1:	☐	☒	☐	☐	☐	☐
Appendix A2:	☐	☒	☐	☐	☐	☐

Section 2   Report on Compliance

(**ROC Sections 1.2 and 1.3.2**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*	2023-12-01
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	2024-01-26
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No
Were any testing activities performed remotely? If yes, for each testing activity below, indicate whether remote assessment activities were performed:	☒ Yes ☐ No

• Examine documentation	☒ Yes	☐ No
• Interview personnel	☒ Yes	☐ No
• Examine/observe live data	☒ Yes	☐ No
• Observe process being performed	☒ Yes	☐ No
• Observe physical environment	☒ Yes	☐ No
• Interactive testing	☒ Yes	☐ No
• Other:	☐ Yes	☐ No

Section 3   Validation and Attestation Details

<table>
<tr><td colspan="2">Part 3. PCI DSS Validation
(ROC Section 1.7)</td></tr>
</table>

This AOC is based on results noted in the ROC dated *(Date of Report as noted in the ROC 2024-02-07).*

Indicate below whether a full or partial PCI DSS assessment was completed:

☒ **Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.

☐ **Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the ROC noted above, each signatory identified in any of Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document *(select one):*

☒	**Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT** rating; thereby Company Kitchen has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby *(Service Provider Company Name)* has not demonstrated compliance with PCI DSS requirements. **Target Date** for Compliance: YYYY-MM-DD An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.
☐	**Compliant but with Legal exception:** One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Service Provider Company Name)* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction. This option requires additional review from the entity to which this AOC will be submitted. *If selected, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement from being met

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:

(Select all that apply)

☒	The ROC was completed according to *PCI DSS*, Version 4.0 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
☒	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

DocuSigned by:

Chad Young

5BAF7B7CB5B84DF...

Signature of Service Provider Executive Officer ↑	Date:	2/7/2024
Service Provider Executive Officer Name: Chad Young	Title:	VP – PMO, IT, Security

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:	☒ QSA performed testing procedures.
	☐ QSA provided other assistance. If selected, describe all role(s) performed:

Barry Johnson

Signature of Lead QSA ↑	Date: 07-Feb-2024
Lead QSA Name: Barry Johnson	

Barry Johnson

Signature of Duly Authorized Officer of QSA Company ↑	Date: 07-Feb-2024
Duly Authorized Officer Name: Barry Johnson	QSA Company: Dara Security

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:	☐ ISA(s) performed testing procedures.
	☐ ISA(s) provided other assistance. If selected, describe all role(s) performed:

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has Non-Compliant results noted in Section 3.

If asked to complete this section, select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement below. For any "No" responses, include the date the entity expects to be compliant with the requirement and provide a brief description of the actions being taken to meet the requirement.

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 network security controls	☒	☐	
2	Apply secure configurations to all system components	☒	☐	
3	Protect stored account data	☒	☐	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	☒	☐	
5	Protect all systems and networks from malicious software	☒	☐	
6	Develop and maintain secure systems and software	☒	☐	
7	Restrict access to system components and cardholder data by business need to know	☒	☐	
8	Identify users and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholder data	☒	☐	
10	Log and monitor all access to system components and cardholder data	☒	☐	
11	Test security systems and networks regularly	☒	☐	
12	Support information security with organizational policies and programs	☒	☐	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	☒	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☒	☐	