Payment Card Industry
Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0.1

Publication Date: August 2024

PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: Olo Inc.

Date of Report as noted in the Report on Compliance: 2/26/2025

Date Assessment Ended: 2/26/2025

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:	Olo Inc.
DBA (doing business as):	
Company mailing address:	Olo Inc., One World Trade Center, 285 Fulton Street, 82nd floor, New York, NY 10007 USA
Company main website:	www.olo.com
Company contact name:	Nick Edmonds
Company contact title:	CISO
Contact phone number:	212-260-0895
Contact e-mail address:	pci@olo.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:	SecurityMetrics, Inc.
Company mailing address:	1275 West, 1600 North Orem, UT 84057
Company website:	www.securitymetrics.com
Lead Assessor name:	Trevor Hansen
Assessor phone number:	801-705-5694
Assessor e-mail address:	aoc@securitymetrics.com

Assessor certificate number:	QSA #202-895

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the Assessment (select all that apply):

Name of service(s) assessed:	Olo Platform Engage (Wisely) Omnivore

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): Chat application		
☐ 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 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 2. Executive Summary *(continued)*

Part 2a. Scope Verification *(continued)*

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

Name of service(s) not assessed:	None

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:	N/A – No services were excluded

Part 2b. Description of Role with Payment Cards (ROC Sections 2.1 and 3.1)

Describe how the business stores, processes, and/or transmits account data.	Olo Inc. (referred to as Olo throughout this document) provides mobile and web-based online ordering for restaurants. For online and mobile ordering, cardholder data is collected for payment and processed using Olo's processors. Credit card data can be collected when an account is opened and saved for future orders, or can be collected at the time of order. Olo uses tokenization solutions offered by its various processors to allow customers to save payment information for future purchases without storing cardholder data in the Olo cardholder environment.

Olo provides a service (referred to as Omnivore) that facilitates integration between different POS solutions and vendors. Restaurants can receive card-present transactions and integrate them among different technologies, facilitated by a public-facing API and an agent that runs on the POS system at the merchant location.

Olo also provides a service (referred to as Engage or Wisely) that allows restaurants to require a deposit for reservations or waitlisting. This payment data is also tokenized. If the restaurant's customer keeps the reservation, the payment card is not charged.

All cardholder data is received and transmitted over an HTTPS connection. Olo does not store PAN or sensitive cardholder data. Because of its transaction volume, Olo has been classified as a Level 1 Service Provider.

Olo provides mobile and web-based online ordering for restaurants. For online and mobile ordering, cardholder data is collected for payment and processed using Olo's processors. Credit card data can be collected when an account is opened and saved for future orders or can be collected at the time of order. Olo uses tokenization solutions offered by its various processors to provide customers with the ability to save payment information for future purchases without the need of storing cardholder data within the Olo cardholder environment. Olo does not store PAN or sensitive cardholder data.

For the Omnivore offering, Olo customers (either restaurants or service providers representing them) receive card-present transactions at a point of interaction and send the cardholder data to the Omnivore API, hosted in AWS, which forwards the transaction to an Omnivore virtual POS or to a customer-controlled, on-premise POS system via an established session with the Omnivore agent. The POS or virtual POS forwards the cardholder data to the designated processor for processing or tokenization.

For the Engage offering (referred to as Engage or Wisely), a restaurant hosts their own website or uses a third-party service provider for hosting their website. When an end-user wants to make a reservation, the website calls an iframe (managed by Olo and hosted in AWS) that uses stripe.js to load Stripe's payment page for credit card acceptance. The Engage page is served by the AWS CloudFront CDN service and code for the contents of the iframe stored in S3. No cardholder data is sent through Wisely systems.

	All cardholder data is received by Olo systems and transmitted over an HTTPS connection over the internet or public-facing API.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Olo provides a service (referred to as Omnivore) that facilitates integration between different POS solutions and vendors. Restaurants can receive card-present transactions and integrate them among different technologies, facilitated by a public-facing API and an agent that runs on the POS system at the merchant location.
Describe system components that could impact the security of account data.	Olo has the ability to send order transaction information to a customer's POS systems through POS integration. The POS system contacts the Olo platform to open a secure session. Order information is sent through that session back to the POS as it is received. This POS integration is different from the Omnivore product described above, in that cardholder data is not sent to the POS, but is in scope of Olo's PCI program due to the connectivity aspect.

Part 2. Executive Summary *(continued)*

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.*	Olo provides an eCommerce-based ordering platform. The entire Olo CDE is hosted within the AWS environment. All cardholder data is received and transmitted through the use of HTTPS. All management (SSH and RDP) is through the use of a two-factor VPN or the AWS management console. No cardholder data is stored. All cardholder data is sent through the Olo platform to the processors, to the merchant's POS system, or redirected at the browser to the processors for processing or tokenization.
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*
N/A – Handling of all cardholder data, including storing, processing, and transmitting, is handled within the PCI-validated, third-party service provider environment (provided by AWS).	Not Applicable	Not Applicable
Corporate Office	1	New York, NY, USA

Part 2. Executive Summary *(continued)*

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, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions), and Mobile Payments on COTS (MPoC) products.

Part 2. Executive Summary *(continued)*

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:
Cloudflare	Cloudflare provides the WAF and other related security services for the Olo environment
AWS	Physical security, hardware configuration and installation, IDS, antivirus, logging (Infrastructure-as-a-service)
Sumo Logic	Security Services (Logging)
Microsoft Azure	Mobile Development
Adyen N.V.	Payment Processor and tokenization services
Paymentech LLC.	Payment Processor and tokenization services
CyberSource	Payment Processor and tokenization services
Elavon, Inc.	Payment Processor and tokenization services
First Data Merchant Services, LLC	Payment Processor and tokenization services
FreedomPay	Payment Processor and tokenization services
Heartland Payment Systems, LLC	Payment Processor and tokenization services
Merchant Link, LLC	Payment Processor and tokenization services
Stripe	Payment Processor and tokenization services
TD Merchant Solutions	Payment Processor and tokenization services
TSYS Acquiring Solutions	Payment Processor and tokenization services
Vantiv Acquiring Systems	Payment Processor and tokenization services
Worldpay Mercury Integrated	Payment Processor and tokenization services

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

Part 2. Executive Summary *(continued)*

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

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

For all requirements identified as either "Not Applicable" or "Not Tested," complete the "Justification for Approach" table below.

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: Olo Platform, Engage (Wisely), Omnivore

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If a Compensating Control(s) Was Used
	In Place	Not Applicable	Not Tested	Not in Place	
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:	☐	☒	☐	☐	☐

Justification for Approach

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	1.2.6, 2.2.5 – No insecure services, protocols, ports, or daemons are allowed in the environment. 2.3.1-2.3.2 – No wireless networks are used in or to connect to the CDE. 3.3.3-3.7.9 – No CHD is stored in the environment. 4.2.1.1 – Future-dated requirement, best practice until March 31, 2025. 4.2.1.2-4.2.2 – Wireless networks are not permitted in the environment. PAN is not stored in the environment and is never sent via end-user messaging technologies. 5.2.3-5.2.3.1 – All systems in the environment have anti-malware. 5.3.2.1 – Continuous behavioral analysis is performed to meet requirement 5.3.2 6.4.3 – Future-dated requirement, best practice until March 31, 2025. 7.2.5-7.2.5.1 – Future-dated requirement, best practice until March 31, 2025. 7.2.6 – No CHD is stored in the environment. 8.2.3 – Olo does not have remote access to any customer premises. 8.2.7 – No third-party user accounts exist in the CDE that aren't part of the validated managed services provided by the respective third party. . 8.3.10-8.3.10.1 – No accounts exist where passwords/passphrases are used as the only authentication factor for customer access. 8.3.11 – No physical or logical security tokens, smart cards, or certificates are in use for authentication in the Olo environment. 8.5.1 – Future-dated requirement, best practice until March 31, 2025. 8.6.1-8.6.2 – No application or system accounts exist that can be used for interactive login. 9.4-9.5.1.3 – The entire Olo CDE is housed within the PCI DSS-validated AWS hosting environment. The respective service provider manages Requirement 9 on behalf of their customers, as attested to in their Attestation of Compliance. No other media is generated. No point-of-presence devices exist. 10.2.1.1 – No CHD is stored in the environment. No access to CHD exists to log. 10.3.4 – Sumo Logic only allows read-only view of log messages stored on the log repository. It is natively impossible to alter these files. 10.4.2.1, 11.3.1.1- – Future-dated requirement, best practice until March 31, 2025. 10.3.2.1 No significant external changes occurred in the environment. 11.4.7 – Olo is not a multi-tenant service provider.

	11.6.1, 12.3.1 – Future-dated requirement, best practice until March 31, 2025. 12.3.2 – No requirements in this ROC used a customized approach. 12.3.3-12.3.4– Future-dated requirement, best practice until March 31, 2025. 12.5.3 – No significant changes occurred in the environment during the audit period that could affect the PCI scope. 12.6.2, 12.10.4 – Future-dated requirement, best practice until March 31, 2025. Appendix A1 – Olo is not a multi-tenant service provider. Appendix A2 – No POI devices exist within the environment.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	Not Applicable

Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*	2024-11-19
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	2025-02-26
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No
Were any testing activities performed remotely?	☒ Yes ☐ No

Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated *(Date of Report as noted in the ROC 2025-02-26)*.

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 *Olo Inc.* 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 3. PCI DSS Validation *(continued)*

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:
(Select all that apply)

☒	The ROC was completed according to *PCI DSS*, Version 4.0.1 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of 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

Signed by:
Nick Edmonds
97354137034E437...

Signature of Service Provider Executive Officer ↑	Date: 2/27/2025 | 13:32 MST
Service Provider Executive Officer Name: Nick Edmonds	Title: CISO

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:

Signed by:
Trevor Hansen
EA190EC3A26A491...

Signature of Lead QSA ↑	Date: 2/27/2025 | 17:21 MST
Lead QSA Name: Trevor Hansen	

Signed by:
Gary Glover
490DC91BF4FD4DF...

Signature of Duly Authorized Officer of QSA Company ↑	Date: 2/27/2025 | 11:34 MST
Duly Authorized Officer Name: Gary Glover	QSA Company: SecurityMetrics

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	☐	☐	

Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance accepting organization to ensure that this form is acceptable in their program. For more information about PCI SSC and our stakeholder community please visit: https://www.pcisecuritystandards.org/about_us/