PCI Responsibility Matrix

PCI Requirement	Olo Responsibility	General Customer Responsibilities	Iframe Customer Responsibilities	P2PE Customer Responsibilities	E2EE Customer Responsibilities
Various	Roles and responsibilities are documented, assigned, and understood.	Roles and responsibilities are documented, assigned, and understood.			
1: Install and Maintain Network Security Controls	Limiting network access to and from devices used within the Olo online ordering platform to the most restrictive possible.	Limiting network access of all other networks controlled by Olo customer and other third parties chosen by the customer.			Network security controls are configured and maintained. Network access to and from the cardholder data environment is restricted. Network connections between trusted and untrusted networks are controlled.
2: Apply Secure Configurations to All System Components	Adhering to standards derived system hardening policies for all devices and systems within the Olo online ordering platform.	Hardening of all other systems, including in-store systems and third parties in PCI scope.	System components are configured and managed securely.		System components are configured and managed securely. Wireless environments are configured and managed securely.
3: Protect Stored Account Data	Securely storing (or not storing) cardholder data within the Olo platform.	Protecting cardholder data stored in-store or with non-Olo providers.	Processes and mechanisms for protecting stored account data are defined and understood. Storage of account data is kept to a minimum.	Processes and mechanisms for protecting stored account data are defined and understood. Storage of account data is kept to a minimum. Sensitive authentication data is not stored after authorization.	Processes and mechanisms for protecting stored account data are defined and understood. Sensitive authentication data is not stored after authorization. Access to displays of full PAN and ability to copy PAN is restricted.
4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks	Requiring secure transmission of cardholder data into the Olo platform, and sending data to payment gateways in the most secure manner supported. Maintaining an inventory of trusted keys and certificates. Ensuring certificates used for PAN transmission over public networks are valid.	Protecting cardholder data across all non-Olo networks falling within PCI scope, including the selected payment gateway and ensuring certificates used for PAN transmission over public networks are valid.			
5: Protect All Systems and Networks from Malicious Software	Regularly scanning Olo platform servers in PCI scope for malware and viruses with up-to-date anti-malware software. This includes malware scanning removable media. Anti-phishing mechanisms protect users against phishing attacks.	Protecting in-store networks and all other third parties within PCI scope against malware. This includes malware scanning removable media. Anti-phishing mechanisms protect users against phishing attacks.			
6: Develop and Maintain Secure Systems and Software	Following secure development and change control procedures for all changes to Olo platform components, detecting unauthorized changes and ensuring that all Olo platform components have the latest vendor-supplied security patches installed. Maintaining an inventory of bespoke, custom and third-party software and software components. Protecting public-facing web applications with a WAF that blocks attacks and only loading justified, authorized and valid payment page scripts.	Ensuring that all non-Olo platform systems and components follow secure development, change control and patching processes including any scripts loaded in Serve Google Tag Manager (GTM) containers and websites that load Olo iframes, components and SDK's that can impact payment functions. Maintaining an inventory of bespoke, custom and third-party software and software components. Protecting public-facing web applications with a WAF that blocks attacks and only loading justified, authorized and valid	Security vulnerabilities are identified and addressed. Protecting public-facing web applications by only loading justified, authorized and valid payment page scripts.		Security vulnerabilities are identified and addressed.

		payment page scripts.			
7: Restrict Access to System Components and Cardholder Data by Business Need to Know	Restricting access to cardholder data to customer authorized systems and parties. Reviewing all user accounts at least every six months to ensure access is appropriate. Reviewing all system accounts to ensure access is appropriate with management acknowledgement.	Restricting access to cardholder data transmitted or stored in-store and by all non-Olo systems. Reviewing all user accounts at least every six months to ensure access is appropriate. Reviewing all system accounts to ensure access is appropriate.			Access to system components and data is appropriately defined and assigned.
8: Identify Users and Authenticate Access to System Components	Identifying and authenticating access to all Olo-controlled components in PCI scope. Meeting password length, complexity, rotation, enforcement and MFA type requirements. Protecting application and system accounts passwords.	Identifying and authenticating access to non-Olo components. Meeting password length, complexity, rotation and MFA requirements. Protecting application and system accounts passwords.	User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle. Strong authentication for users and administrators is established and managed.		Processes and mechanisms for identifying users and authenticating access to system components are defined and understood. User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle. Multi-factor authentication is implemented to secure access into the CDE.
9: Restrict Physical Access to Cardholder Data	Restricting physical access to Olo's platform to PCI level 1 hosting providers. Maintaining an up-to-date list of point-of-interaction devices.	Restricting physical access to all non-Olo-controlled devices.	Media with cardholder data is securely stored, accessed, distributed, and destroyed.	Processes and mechanisms for restricting physical access to cardholder data are defined and understood. Media with cardholder data is securely stored, accessed, distributed, and destroyed. Point-of-interaction devices are protected from tampering and unauthorized substitution. An up-to-date list of point-of-interaction devices is maintained.	Processes and mechanisms for restricting physical access to cardholder data are defined and understood. Physical access controls manage entry into facilities and systems containing cardholder data. Media with cardholder data is securely stored, accessed, distributed, and destroyed. Point-of-interaction devices are protected from tampering and unauthorized substitution. An up-to-date list of point-of-interaction devices is maintained.
10: Log and Monitor All Access to System Components and Cardholder Data	Logging and monitoring all activity occurring within the Olo platform. Using risk modeling to drive the frequency of log reviews. Detecting, alerting, and promptly addressing failures of security controls.	Tracking and monitoring activity that occurs in-store and other non-Olo systems within scope. Detecting, alerting, and promptly addressing failures of security controls.			
11: Test Security of Systems and Networks Regularly	Testing the security systems and processes for the Olo platform. Remediating Critical, High Medium and Low vulnerabilities, based on risk. Rescanning as needed. Supporting customer penetration test requests. Using IDS/IPS to detect/prevent covert malware communication. Detecting and responding to unauthorized payment page changes.	Testing non-Olo security systems and processes within PCI scope. Remediating Critical and High vulnerabilities, manage other vulnerabilities based on risk. Detecting and responding to unauthorized payment page changes.	External and internal vulnerabilities are regularly identified, prioritized, and addressed. This includes quarterly scanning by a PCI Approved Scanning Vendor (ASV). Unauthorized changes on payment pages are detected and responded to.		External and internal vulnerabilities are regularly identified, prioritized, and addressed. External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.
12: Support Information Security with Organizational Policies and Programs	Maintaining security policies for all Olo employees and contractors. Ensuring employees and contractors are trained on common security risks and how to avoid them with updates at least every 12 months	Maintaining security policies for non-Olo personnel. Training non-Olo personnel on security risks and how to avoid them at least annually. This includes training to detect tampering and/ or replacement of	Risks to the cardholder data environment are formally identified, evaluated, and managed. Risk to information assets associated with third-party service provider relationships is	A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current. Security awareness education is an ongoing	A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current. Security awareness education is an ongoing

	and as threats evolve. Reviewing cryptographic cipher suites, protocols, hardware and software technologies in use at least once every 12 months. Documenting and confirming PCI scope at least every 6 months and upon significant changes. (Service Provider) Reviewing and documenting the impact to PCI scope and applicability of controls upon significant changes to organizational structure. (Service Provider) Supporting customers' requests for PCI information. (Service Provider)	POI devices. Managing Third-Party Service Provider's, includes performing due diligence, understanding responsibilities, having appropriate agreements in place, and monitoring compliance at least annually. Reviewing cryptographic cipher suites, protocols, hardware and software technologies in use at least once every 12 months. Documenting and confirming PCI scope at least every 12 months and upon significant changes.	managed. Suspected and confirmed security incidents that could impact the CDE are responded to immediately.	activity. Risk to information assets associated with third-party service provider relationships is managed. Suspected and confirmed security incidents that could impact the CDE are responded to immediately.	activity. Risk to information assets associated with third-party service provider relationships is managed. Suspected and confirmed security incidents that could impact the CDE are responded to immediately.
Other	All Olo Pay P2PE payment processing solutions are validated PCI-listed P2PE solutions. Customers using Olo Pay P2PE have implemented all controls in the P2PE Instruction Manual (PIM) provided by the Solution Provider. All Olo Pay E2EE payment processing solutions are approved PCI-listed PIN Transaction Security point-of-interaction devices. Customers using Olo Pay terminals do not otherwise receive, transmit, or store account data electronically.			All controls in the Instruction Manual provided by the Solution Provider are implemented.	All applicable controls in the Instruction Manual provided by the Solution Provider are implemented.

Guide

- Olo's Responsibilities details Olo's Payment Card Industry (PCI) responsibilities
- General Customer Responsibilities details customer PCI responsibilities when using Olo API services such as Ordering API
- Iframe Customer Responsibilities details customer PCI responsibilities when using Olo iframe services such as Credit Card Submission Frame (CCSF)
- P2PE Customer Responsibilities details customer PCI responsibilities when using Olo Pay with Point-to-Point Encryption (P2PE)
- E2EE Customer Responsibilities details customer PCI responsibilities when using Olo Pay with End-to-End Encryption (E2EE)

Examples of Olo's Responsibilities

- Preventing credit card data from being intercepted in-transit between a customer submitting credit card data on Olo hosted front-ends and our platform servers.
- Preventing credit card data stored or transmitted within our platform from being stolen by unauthorized parties.
- Restricting access to sensitive data transmitted and stored by Olo's platform to only those with a business need.

Examples of Customer Responsibilities

- Restricting traffic in and out of stores behind suitable firewall rules.
- Regularly updating operating systems and applications installed in-store and managing any end-of-life technologies.
- Security of third-party developers or agencies directed by customer to develop to an Olo API.
- Security of Point of Sale system(s), payment processor(s) and loyalty service provider(s).
- Security of Point of Interaction devices in-store and at any distributor.
- If applicable, training remote workers how to correctly handle payment data.

Examples of Guest Responsibilities

- Security of the device or browser being used to enter credit card data. For example, Olo is not responsible for malicious browser plugins or key loggers.
- Using a strong and unique password

Additional guidance on Payment Card Industry Data Security Standard (PCI-DSS) and Payment Card Industry PIN Transaction Security Point of Interaction (PCI PTS POI) requirements can be found at: https://www.pcisecuritystandards.org