Olo's PCI Compliance Policy

What is PCI Compliance?

PCI Compliance refers to the Payment Card Industry Data Security Standard (PCI DSS) designed to protect cardholder data. Every company that accepts credit card payments must be PCI compliant.

What do I need to know about PCI Compliance with Olo?

Olo is PCI Compliant, which means our white-label ordering platforms (web, mobile, apps) are PCI Compliant. This matrix outlines PCI responsibilities for Olo and restaurant brands. This covers all of our customers, not just those building a custom application on the Olo API.

Brands that build custom applications on the Olo API are responsible for ensuring it is PCI compliant. We are not qualified to advise any third-party on PCI scope. If a brand is looking to assess their PCI scope, we suggest working with a PCI Qualified Security Assessor (QSA).

Ensuring your Ordering API project is PCI compliant

Olo is not in the position to advise third parties on how to address PCI compliance. The third-party and the brand hold this responsibility. In the past, we have seen other partners use these approaches successfully:

- A third-party agency can become PCI compliant if they are not already.
  - If a brand is looking to assess or understand PCI scope, we suggest working with a PCI Qualified Security Assessor (QSA). A list of QSAs is available here.
- Third-party can outsource credit card payment data to a PCI compliant third party.
  - There are vendors that offer solutions to capture cardholder data and pass that information to the Olo API on behalf of the brand.
  - If a brand chooses to work with a third-party vendor, the front-end developer, and the third-party need to work together to ensure that the final basket submission is completed via the Order Submission API endpoint, with full payment data from the customer (not a token).