mollie

PCI DSS compliance for online payments

May 2024

Index

Index

Introduction to PCI DSS

Welcome to the world of secure payments! At Mollie, we are committed to safeguarding your transactions and protecting your sensitive payment data. As part of our dedication to security, we adhere to the Payment Card Industry Data Security Standard (PCI DSS), a globally recognized set of guidelines designed to ensure the secure handling of payment information provided to us by our customers.

What is PCI DSS?

PCI DSS (Payment Card Industry - Data Security Standard) is a security standard adopted by major payment card scheme providers (Mastercard, Visa, and American Express etc.), PCI DSS defines a set of technical and operational requirements that when implemented correctly, helps customers to maintain customer trust, protect their cardholder data and minimise the chances of a data breach resulting from security attacks by putting in adequate measures.

Why is PCI DSS Important?

The importance of PCI DSS cannot be overstated in today's payment landscape. With threats on the rise, protecting sensitive payment data is paramount for businesses and customers alike. Compliance with PCI DSS not only helps mitigate the risk of data breaches but also builds trust with your customers by demonstrating your commitment to security.

Key Principles of PCI DSS:

- **Build and Maintain a Secure Network**: Implement robust security measures, such as firewalls and encryption, to protect cardholder data during transmission.
- **Protect Cardholder Data:** Safeguard cardholder information by encrypting it during storage and transmission. Minimise data retention and securely dispose of unnecessary data.
- **Maintain a Vulnerability Management Program:** Regularly scan for vulnerabilities and address any security weaknesses promptly. Keep systems and software up to date with the latest security patches.
- **Implement Strong Access Control Measures:** Restrict access to cardholder data on a need-to-know basis. Assign unique IDs to individuals with computer access and monitor all access to sensitive data.
- **Regularly Monitor and Test Networks:** Continuously monitor networks and systems for suspicious activity. Conduct regular security testing, including penetration testing and vulnerability assessments, to identify and address potential vulnerabilities.
- **Maintain an Information Security Policy:** Develop and maintain a comprehensive security policy that addresses all aspects of PCI DSS compliance. Educate employees about security best practices and ensure compliance with security policies and procedures.

At Mollie, we understand the importance of PCI DSS and other applicable regulations in today's payment ecosystem with evolving security and fraud threats. Our platform is built with security in mind, incorporating industry-leading security measures to protect your transactions and sensitive data. Let's take a closer look now at how Mollie implements PCI DSS compliance to safeguard your sensitive payment information and some recommendations about your PCI compliance requirements.

PCI DSS compliance for Mollie and its customers

PCI DSS applies to people, processes and technology that collect, store, process or transmit cardholder data, collectively these components can also be referred to as “Cardholder Data Environment (CDE)". In accordance with PCI DSS requirement 12.8.5 this document indicates where the Mollie or customers have responsibility to fulfil each PCI DSS requirement in order to use the Mollie’s payment processing services in a PCI-compliant manner by its customers.

Mollie’s role in PCI DSS Compliance

Mollie is responsible for maintaining PCI DSS compliance of its Cardholder Data for CDE which means Mollie (along with its service providers) is **responsible for security of cardholder data only as soon as Mollie receives the data** through the relevant payment interface.

After Mollie receives customers' cardholder data, the data is stored/ processed in a PCI DSS Level 1 compliant Service Provider Cardholder Data Environment. Mollie's PCI DSS compliance status can be verified by requesting PCI Attestation of Compliance (AoC) report by sending a message to Mollie Help.

PCI DSS Responsibility for customers

Mollie's customers using Mollie as their e-commerce PSP (Payment Services Provider) are responsible for making sure that **cardholder data is secure and protected before the data reaches Mollie**.

Please note that Mollie can't give any kind of definite advice to customers' for their PCI compliance, as we do not have all the details about customers' setup. As there is no one size fits all PCI compliance advice, If the customer is doing card data storage/ processing, they might have potentially applicable PCI requirements. Depending on the integration and setup, customers themselves would be responsible to comply with the applicable PCI DSS requirements.

Mollie's customers shall consult with their acquiring bank or a QSA (Qualified Security Assessor) to determine applicable PCI requirements for their environment. However, as a recommendation, this guide from PCI Security Standards Council could be a good starting point to start understanding the applicable requirements based on the setup and configuration.

Please note that there might be additional PCI DSS requirements applicable to the customers who are using Mollie's POS (Point of Sale) devices/ services for Card-present transactions. In case you are also using Mollie's POS devices, please read through our dedicated guide.

Recommended useful resources

- PCI DSS for online payments (this document)
- PCI DSS compliance for offline payments
    - PCI DSS - Device inspection sample checklist
- PCI DSS Customer Responsibility Matrix
- (External) PCI Security Standards Council website
- (External) PCI DSS Resource Hub
- (External) Self-Assessment Questionnaire templates (SAQ)
    - (External) SAQ - Instructions and Guidelines