mollie

PCI DSS compliance for offline payments

May 2024

Index

Index

Introduction to PCI DSS 3

Why is PCI DSS Important? 3

Key Principles of PCI DSS 4

PCI DSS compliance for customers using POS Devices 5

Mollie's role in PCI DSS Compliance as a provider of POS Devices 5

PCI DSS Responsibilities for customers handling POS Devices 7

Guidelines for Device Inspection 9

Useful resources 11

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 customers using POS Devices

In order to ensure proper security of POS devices, Mollie and POS customers must work together based on a shared responsibility model to do their part to implement best practices and security measures. In the below section, we have clearly outlined both the Mollie and Customer's responsibilities to ensure safe and secure operation of POS devices.

Mollie’s role in PCI DSS Compliance as a provider of POS Devices

As part of the PCI shared responsibility model, below requirements are the responsibility of Mollie with regards security of POS devices:

Regular Software Update and Patches
Mollie ensures to regularly push software updates and vulnerability patches to the POS terminals. This helps to address known vulnerabilities, thereby improving the security of the POS devices and guard against emerging cyber security threats.

Encryption
The application running on the terminals protects sensitive data such as data for CDE by implementing data encryption for any data stored or being transmitted on the POS devices. This helps to prevent unauthorised access and interception by attackers.

Access Control Management
The tools used for remote terminal management are protected through 2FA authentication to prevent authorised access.

Issuing security Guidance and Documentation for customers
Another key responsibility of Mollie is to provide her valued customers with comprehensive best practices guides on how to securely maintain and use POS devices in order to mitigate security risks effectively.

Continuous Monitoring

Finally, Mollie continues to monitor and evaluate the security of the POS devices proactively identifying and addressing emerging threats and vulnerabilities.

Compliance and Standards

Mollie ensures that the applications running on the terminal and the hardware adhere to the applicable security standards and regulatory requirements such as PCI DSS, that is PCI DSS compliance. One of the ways Mollie does this is by periodically accessing the security practices of third party/vendors/partners providing POS devices/ applications to ensure they are compliant with relevant security standards and certifications.

PCI DSS Responsibilities for customers handling POS Devices

Mollie's customers who use POS devices also have some responsibilities in ensuring the security of their systems and protecting both the terminal hardware and the sensitive data processed through them. Here are the key responsibilities of customers using POS devices:

Accept and install Software Update Pushed to the Terminals
Mollie expects Merchants to accept software updates and vulnerability patches when they are pushed to the terminals, and not to unnecessarily postpone these updates.

Network Security
Customers should ensure that their network infrastructure is secured through firewalls intrusion detection systems (if applicable). Customers are also responsible for ensuring that their integration systems with Mollie are secured and safe from tampering.

Physical Security Measures
Customers should implement physical security measures to protect POS devices from theft, tampering or authorised access. This may include installing security cameras, lockers and restricting access to areas where POS devices are placed.

Employee Training
Customers should provide regular security training to their employees who handle and use POS devices. They should cover topics such as phishing, skimming and substitution awareness by communicating them the guidelines linked below

Verify the Identity of any third-party persons or remote connection requests
You must first verify the identity of any third-party persons (claiming to be repair or maintenance personnel who either showed up in-person to your place of business or attempted to remotely connect with you/your terminal online) before granting them access to modify or troubleshoot your devices.

Maintain an up-to-date list of devices

When you receive your POS device from Mollie, check your merchant dashboard or invoice to validate that you have received the correct device before you start using it.

You can keep track of your devices in your own inventory e.g a spreadsheet or you can use the Mollie's merchant dashboard.

Periodic Device Inspection

As required by PCI DSS, Customers shall periodically carry out periodic inspection of their POS devices to ensure devices are safeguarded against tampering and unauthorised substitution.

Please note that Customers' using POS devices or other Mollie payment services are responsible for maintaining their own PCI compliance, above mentioned are suggested best practices and in no way indicate complete set of applicable PCI requirements outside the POS devices scope. Customers must contact their acquiring bank or a PCI Qualified Security Assessor (QSA) to understand the full set of applicable requirements to them based on their setup.

Guidelines for Device Inspection

Following are general guidelines for customers to follow when inspecting their POS devices.

When inspecting devices, you must check to ensure that the devices are safeguarded against skimming, tampering and authorised substitution.

Defining POS device substitution, tampering and skimming

Unauthorised substitution is a type of fraudulent activity where legitimate hardware or software components of a POS device are replaced or substituted with malicious or unauthorised ones without the knowledge or consent of the customer. This substitution is typically done with the intention to steal sensitive information such as payment card data, or to compromise the security of the POS device for financial gain.

Tampering and skimming are forms of unauthorised substitution that involves the installation of tampering or skimming devices on legitimate POS terminals. These skimming devices are discreetly placed on or within a legitimate POS device/terminal with the sole intent to steal cardholder information during a transaction.

PCI-DSS requirement calls for the protection of devices that capture payment card data through direct physical contact from tampering and substitution.

How do customers do this?

1. Maintain an up-to-date list of devices
2. Periodic inspection of POS devices

More details below.

Maintain an up-to-date list of devices

When you receive your POS device from Mollie, check your merchant dashboard or invoice to validate that you have received the correct device before you start using it.

You can keep track of your devices in your own inventory e.g a spreadsheet or you can use the Mollie's merchant dashboard.

Periodic Inspection of POS devices/terminals

As required by PCI DSS, Customers shall periodically carry out periodic inspection of their POS devices to ensure devices are safeguarded against tampering and unauthorised substitution.

The frequency of inspections will depend on factors such as the location of a device and whether the device is attended or unattended. For example, devices left in public areas without supervision by the organisation's (customer) personnel might have more frequent inspections than devices kept in secure areas or supervised when accessible to the public. This frequency should be determined by the customer themselves based on the environment in which the device operates. Device inspection can be carried out using the device inspection template provided below.

Missing Terminal?
If you notice a theft, report immediately to Mollie so that the terminal can be blocked and you can begin your investigation afterwards. *You can also use the self service features in the Mollie dashboard available for you to block the missing terminal*.

Suspicion of Skimming/Tampering or other POS related security incidents?
Immediately stop using the device and report this to Mollie through the pos-support@mollie.com

Useful resources

- PCI DSS compliance for online payments
- PCI DSS compliance for in-person payments (this document)
    - 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