mollie

Mollie's PCI DSS Customer Responsibility Matrix

May 2024

Index

Index **2**
Introduction **3**
1. Install and Maintain Network Security Controls 4
2.Apply Secure Configurations to All System Components 5
3. Protect stored card holder data 6
4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks 7
5. Protect All Systems and Networks from Malicious Software 8
6. Develop and maintain secure systems and applications 9
7. Restrict Access to System Components and Cardholder Data by Business Need to Know 10
8. Identify and authenticate access to system components 11
9. Restrict physical access to cardholder data 12
10. Log and monitor all access to system components and cardholder data 13
11. Test security of systems and networks regularly 14
12. Support Information Security with Organizational Policies and Programs 15

Mollie B.V.
www.mollie.com

Keizersgracht 126, 1015 CW
Amsterdam, the Netherlands

Introduction

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.

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 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 for 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 relevant payment interface). After Mollie receives customers' cardholder data, the data is stored/ processed in the a PCI DSS Level 1 compliant Service Provider Cardholder Data Environment.

Customer (Merchant) Responsibility

Customer is responsible for making sure that cardholder data is secure and protected before the data reaches Mollie. Depending on the integration, they would also be responsible to comply with PCI DSS requirements as well.

This document breaks down the responsibility matrix **when the cardholder data is being collected/ processed in the customer technology environment (before it reaches Mollie)**.

1. Install and Maintain Network Security Controls

PCI DSS sub requirement	N/A	Customer	Mollie	Notes
1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.		X		
1.2 Network security controls (NSCs) are configured and maintained.		X		
1.3 Network access to and from the cardholder data environment is restricted.		X		
1.4 Network connections between trusted and untrusted networks are controlled.		X		
1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.		X		

2. Apply Secure Configurations to All System Components

PCI DSS sub requirement	N/A	Customer	Mollie	Notes
2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood.		X		
2.2 System components are configured and managed securely.		X		
2.3 Wireless environments are configured and managed securely.		X		

3. Protect stored card holder data

PCI DSS sub requirement	N/A	Customer	Mollie	Notes
3.1 Processes and mechanisms for protecting stored account data are defined and understood.		X		
3.2 Storage of account data is kept to a minimum.		X		
3.3 Sensitive authentication data (SAD) is not stored after authorization.		X		
3.4 Access to displays of full PAN and ability to copy cardholder data are restricted.		X		
3.5 Primary account number (PAN) is secured wherever it is stored.		X		
3.6 Cryptographic keys used to protect stored account data are secured.		X		
3.7 Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.		X		

4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

PCI DSS sub requirement	N/A	Customer	Mollie	Notes
4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented.		X		
4.2 PAN is protected with strong cryptography during transmission		X		

5. Protect All Systems and Networks from Malicious Software

PCI DSS sub requirement	N/A	Customer	Mollie	Notes
5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.		X		
5.2 Malicious software (malware) is prevented, or detected and addressed.		X		
5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.		X		
5.4 Anti-phishing mechanisms protect users against phishing attacks.		X		

6. Develop and maintain secure systems and applications

PCI DSS sub requirement	N/A	Customer	Mollie	Notes
6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.		X		
6.2 Bespoke and custom software are developed securely.		X		
6.3 Security vulnerabilities are identified and addressed.		X		
6.4 Public-facing web applications are protected against attacks.		X		
6.5 Changes to all system components are managed securely.		X		

7. Restrict Access to System Components and Cardholder Data by Business Need to Know

PCI DSS sub requirement	N/A	Customer	Mollie	Notes
7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.		X		
7.2 Access to system components and data is appropriately defined and assigned.		X		
7.3 Access to system components and data is managed via an access control system(s).		X		

8. Identify and authenticate access to system components

PCI DSS sub requirement	N/A	Customer	Mollie	Notes
8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.		X		
8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.		X		
8.3 Strong authentication for users and administrators is established and managed.		X		
8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE		X		
8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.		X		
8.6 Use of application and system accounts and associated authentication factors is strictly managed		X		

9. Restrict physical access to cardholder data

PCI DSS sub requirement	N/A	Customer	Mollie	Notes
9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.		X		
9.2 Physical access controls manage entry into facilities and systems containing cardholder data.		X		
9.3 Physical access for personnel and visitors is authorized and managed.		X		
9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.		X		
9.5 Point of interaction (POI) devices are protected from tampering and unauthorized substitution. (If applicable)		X	X	Mollie must provide POS device training and inspection documentation to its POS customers to educate them on protecting devices from tampering, skimming and unauthorised substitution. Mollie's POS customers' responsibility here would be to read & understand the training and inspection documentation provided by Mollie. Additionally, It would be customers' responsibility to perform periodic inspection checks as per documentation and checklist provided by Mollie.

10. Log and monitor all access to system components and cardholder data

PCI DSS sub requirement	N/A	Customer	Mollie	Notes
10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.		X		
10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.		X		
10.3 Audit logs are protected from destruction and unauthorized modifications.		X		
10.4 Audit logs are reviewed to identify anomalies or suspicious activity.		X		
10.5 Audit log history is retained and available for analysis. .		X		
10.6 Time-synchronization mechanisms support consistent time settings across all systems.		X		
10.7 Failures of critical security control systems are detected, reported, and responded to promptly		X		

11. Test security of systems and networks regularly

PCI DSS sub requirement	N/A	Customer	Mollie	Notes
11.1 Processes and mechanisms for regularly testing security of systems and networks are defined and understood.		X		
11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.		X		
11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed* *Applicable for POS devices: Scope of Mollie's responsibility here is limited to any vulnerabilities found on POS devices issued by Mollie to the customer. Any vulnerabilities noted in the customers environment is responsibility of the customer to address it.		X	X	*For Customers using Mollie POS devices, Any vulnerabilities noted in the POS devices must be reported by Mollie to the the customers. Also, Mollie is responsible to send relevant patches to fix those vulnerabilities to the affected POS devices within a month of release of vulnerability. Customers are responsible for installing the patches shared by Mollie in order to fix the vulnerabilities within a reasonable timeframe.
11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.		X		
11.5 Network intrusions and unexpected file changes are detected and responded to.		X		
11.6 Unauthorised changes on payment pages are detected and responded to.		X		

12. Support Information Security with Organisational Policies and Programs

PCI DSS sub requirement	N/A	Customer	Mollie	Notes
12.1 A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.		X		
12.2 Acceptable use policies for end-user technologies are defined and implemented.		X		
12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.		X		
12.4 PCI DSS compliance is managed.		X		
12.5 PCI DSS scope is documented and validated.		X		
12.6 Security awareness education is an ongoing activity.		X		
12.7 Personnel are screened to reduce risks from insider threats.		X		
12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.		X		
12.9 Third-party service providers (TPSPs) support their customers' PCI DSS compliance.		X		
12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.		X		