Merchant Instructions

The Merchant Instructions is part of the Agreement. The definitions in the Terms and conditions also apply to the Merchant Instructions. The Merchant Instructions published at www.nets.eu/payments are subject to change without notice if such change is due to changes in legislation or to requirements imposed by Card Organisations or public authorities. The Merchant Instructions in force at any given time can be found at www.nets.eu/payments.

Requirements for Cardholder-Activated Terminals
All Cardholder-Activated Terminals must be able to read chip, and must be equipped with a PIN pad. All the terminals must fulfill requirements of PCI DSS. Cardholder-Activated Terminals must not print vouchers or pay out cash.

The following also applies to Cardholder-Activated Terminals:

- Only trained personnel may have access to card readers and PIN devices
- Authorization to run programs/systems must be administered restrictively
- Codes/keys to the terminal must be stored securely and may only be given out to authorized personnel
- The terminal cabinet must be kept locked at all times, even when the terminal is not in use
- The Merchant must not modify the physical functions of the terminal
- The Merchant must constantly monitor alerts from the terminal and must secure the terminal against inadvertent access or attempts to "break in".

Requirements for Mail and Telephone Order transactions

Order form requirements – Mail order
The order form, which your customers need to fill out in order to shop in your mail order business, must comply with the following requirements:

- Clear description of the goods
- Clear indication of the possibility for card payments
- The order form cannot be designed as an open postcard, as it contains personal Payment Card information
- Name and full address of the Merchant must be clear (post office box is not adequate)

The Cardholder must provide at least the following information

- Name, address and phone number
- Card type
- Card number, expiration date and CVV number
- Amount
- Date
- Signature

Requirements for receiving card information by telephone
Merchants selling goods/services using telephone orders must provide the Cardholder with adequate information about the terms and conditions that apply to the agreement/transaction, including:

- Delivery costs
- Other costs/charges
- Terms and conditions of delivery (including cancellation rights)

The Cardholder must provide the Merchant with the following information

- Name, address and telephone number
- Payment Card type
- Card number, expiration and Security Code

The Merchant must not accept Maestro-cards for mail and telephone order transactions.

PCI DSS

All merchants accepting Card Payments and service providers handling Card Data must comply with the PCI DSS requirements. Depending on the number of annual transactions, Merchants must provide different documentation for meeting the PCI DSS requirements. The rules apply to all types of agreement.

The Card Organizations have divided Merchants into four categories:
Level 1 - Merchants with more than six million transactions annually
Level 2 - Merchants with one to six million transactions annually
Level 3 - Card-Not-Present Merchants with 20,000 to one million transactions annually
Level 4 - All other merchants

Nets will contact you if your Merchant is categorized as level 1, 2 or 3.

For detailed information regarding the Card Organizations requirements for each level, please visit the Card Organization's homepages;

- https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/merchants-need-to-know.html
- http://www.visaeurope.com/receiving-payments/security/merchants

All Merchants, including level 4 merchants, with access to card data must meet the PCI DSS requirements and must inform Nets if card data is handled. Most data theft occur at small and medium size merchants without the necessary security.

List of Qualified Security Assessors (QSA) – businesses certified to carry out system revisions, which must comply with the PCI DSS requirements.

- https://www.pcisecuritystandards.org/approved_companies_providers/qualified_security_assessors.php

List of Approved Scanning Vendors (ASV) – businesses approved to scan IT systems.

- https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php

Transaction limits for Contactless transactions

The transaction limits are established by the Card Organizations and are subject to change without notice at any time. For Contactless transactions above these limits, the cardholder must be verified. Currently prevailing transaction limits can be found here:

Country	Currency	Cardholder Verification limit MC	Cardholder Verification limit Visa
Estonia	EUR	50	50
Latvia	EUR	50	50
Lithuania	EUR	50	50

Please contact Nets for applicable cardholder verification limits for other countries.