REQUIREMENTS FOR ACCEPTING CARDS PAYMENTS ON THE INTERNET

Valid as of 18.02.2015

1. GENERAL REQUIREMENTS FOR THE POINT OF SALE WEBSITE

1.1 It is recommended to use a secure connection (SSL - Secure Sockets Layer) when requesting for client data. When using a secure connection, a certificate must be used that has been provided by a trusted certificate authority (not self-generated). Transfer of Card data is performed via the Processor server, and in this case, a secure connection between the Processor and Cardholder is always used. To ensure the security of data transfer, a 128-bit encryption (SSL - Secure Sockets Layer security protocol) is used between the Cardholder and the E-Commerce Payment Gateway, and data, which is transferred between the Merchant and Payment Gateway, is signed digitally, which excludes the possibility of third parties of altering and wire tapping the data. The Merchant has access to the Transactions report but has no access to the full Card number.
1.2 The following information must be visible to the Cardholder during a transaction at the Merchant's Point of Sale:
1.2.1 privacy policy / data security
1.2.1.1 reference to the use of SSL, MasterCard SecureCode, Verified by Visa when requesting card data.
1.2.1.2 the use/non-use of personal information given to the Merchant by the Cardholder.
1.2.1.3 information regarding the fact that the Merchant does not see the data of the inserted Card (for the transaction, the Cardholder is directed to the Processor's secure environment. Upon payment, the Cardholder's Card data is transferred to a database in the Processor's servers, and the data is also stored in the Processor's server).
1.2.2 the Merchant's full name.
1.2.3 the state and postal address of the location.
1.2.4 the full list of products/services, price list. An accurate description of the product/service, providing the Cardholder with a sufficient overview of what is being offered, with special attention to whether these are legal/usable outside the Merchant's country of origin (for example, when selling electrical equipment, the Merchant must present the conditions for effective supply voltage, which is different depending on each part of the world).
1.2.5 the logos (Visa/MasterCard) and commercial labels (SecureCode, Verified byVisa) of accepted Cards. The logos and commercial labels must be presented with the same proportions, and no brand must be preferred over the others. Correct logos can be downloaded from the Processor's website at www.nets.eu/etee/.
1.2.6 the currency used for the card transaction. When making a transaction, it is recommended to show the cross-exchange rates for the best known currencies (depending on the target market). The exchange rates should refer to their source, and mention the refresh frequency.
1.2.7 The procedures for sending/transferring goods, added costs for postage, and their determination, and for notifying the Cardholder. Limitations on shipping (not outside Estonia, goods with large dimensions being sent only through a specific service, shipping possible only to certain countries, etc.).
1.2.8 The total cost of Transaction with the cost of postage, references to possible additional costs, incl. possible tolls and obligations by the Cardholder to pay a VAT.
1.2.9 Notification to the Cardholder of their right of withdrawal. The procedures, time limits for returning goods. The warranty conditions and procedures for the exchange of goods.
1.2.10 Feedback alongside the order confirmation.
1.2.11 Notification to the Cardholder of possible complications when handling the goods.
1.2.12 The telephone number and e-mail address of customer service, and the procedures for giving feedback. In case of a phone number, operating hours, according to local time, with an indication of the time zone (GMT+2), and in case of an e-mail, the estimated period of time for a response to inquiries. Languages used.
1.3 The Merchant is obliged to prove in a reproducible format that the Cardholder has, before confirming the transaction, agreed to the conditions of sale of the goods, and/or provision of service.
1.4 The Merchant is responsible for the accuracy of the information and offers presented at the Point of Sale. In case of significant changes to the offered goods/nature of the service or assortment, the Merchant is obliged to inform the Bank thereof in advance.

2. REQUIREMENTS SET FOR THE TRANSACTION NOTICE

After sending a positive response to the Transaction, a summary of the order must be displayed for the Cardholder. The summary must be in a form, which is easy to print or save. It is recommended to send the same summary to the Cardholder via e-mail as well, if the e-mail address is known.
2.1 Requirements in accordance with legislation valid in Estonia.
2.2 Information that the Transaction has been paid for by Card.

AS SEB Pank
Tornimäe 2, 15010 TALLINN
Phone: 372 665 5100
e-mail info@seb.ee

Supervising Authority: Financial Supervision Authority
Sakala 4, 15030 TALLINN
phone 372 668 0500
e-mail: info@fi.ee

2.3 A unique identification number for the Transaction, which helps both the Cardholder and the Merchant to keep account of the Transaction and solve potential problems.
2.4 Internet address of the Point of Sale.
2.5 At the end of the Transaction notice, there must be a notation that the Cardholder should print or save the Transaction notice.

3. FRAUD PREVENTION

3.1 The Merchant is responsible for all transactions that have been made in their Point of Sale.
3.2 The Merchant must ensure the proper training of their employees according to the manual Accepting card payments on the internet and informing of risks.
3.3 Before delivery of goods, the Merchant must review the data of the Transaction.
3.4 Attention must be paid to unusual purchasing activity. In the case of suspicion, the Bank must be contacted.
3.5 3.5 Data must be compared to any fraud that has occurred previously.
3.6 Attention must be paid to addresses where goods are delivered. Suspicion should be aroused by goods being sent to the same address despite having been paid for by different cards or by Cardholders with different names.
3.7 Unusual sums of purchase must be observed. Sums larger than usual for transactions should be the subject to special attention.
3.8 Cardholder's IP addresses, transactions from the same IP address with different cards or to different recipients should be monitored.
3.9 In case of suspicion of fraud, the Merchant should immediately contact the Bank.
3.10 In the case of suspicion of fraud, the Bank retains the right to cease processing a Transaction for the duration of an investigation, or to annul a Transaction. The Bank will notify the Merchant of inspecting a Transaction and the Merchant must not ship the goods subject to the Transaction.
3.11 The Merchant is obliged to follow the legal acts of the European Union, the OECD, and the appropriate country applicable to electronic commerce and distance selling to a Cardholder.

4. ANNULMENT OF A TRANSACTION

4.1 The sole method of annulling a transaction is to send a request to the Bank alongside the data of the Transaction. The request must mention the reason for annulment. Other channels may not be used to return the money. The Cardholder, who has returned the goods and is requesting a return of the sum of the Transaction, must be notified when the annulment has been performed.