

# Trading safely online

**Practical procedures and secure systems minimise the risk of running into difficulties on the internet**



Selling goods and services online brings fantastic opportunities – but also risks. Computer hacking and the misuse of card data are a real worry, and this is an area where both we and the card networks are investing heavily in order to ensure that we stay one step ahead. For merchants who want to do business online, this means opportunities to minimise the risk of exposure to fraud.

To begin with, you should always use a Payment Service Provider (PSP) which is certified in accordance with the Payment Card Industry Data Security Standard. You should also ensure that you always use the 3D Secure standard for safe online payment by Visa and MasterCard.

On the next few pages, you will find recommendations and the card networks' requirements for all those who process card data. Following these will allow you to minimise the risk of running into difficulties on the internet. Make things hard for fraudsters.

## **PCI DSS – the Payment Card Industry Data Security Standard**

PCI DSS is a standard for processing card data securely. The standard was developed by the international MasterCard, Visa, Diners Club, American Express, JCB and Discover card networks. As a merchant, you

need to comply with the PCI DSS security requirements. These requirements vary depending on your volumes (number of card transactions), industry and risk classification.

As a Euroline customer, you will be contacted to keep you updated with additional information about the specific requirements and the action you need to take.

## **Use 3D Secure**

3D Secure is a standard for secure online payment by MasterCard and Visa. This involves the customer entering his card number in the normal way. The card issuer checks the number using encrypted communication and a special secure server. The customer then identifies himself using a pass-  
▶

### **Make things hard for fraudsters.**

- Always include the CVV2/CVC2 security code during the authorisation process.
- Set limits. For example, only allow one purchase per card each day, or a certain number of purchases from a single IP address. Also, set a maximum limit over which all purchases have to be checked manually. These limits can be built into your own systems. Alternatively, check with your PSP what parameter settings they can offer.
- Get to know your customers! New customers should be treated with more caution than existing, well-known customers.
- Assess reasonability before delivering goods, especially to customers abroad.
- Check that the customer's IP address matches the country which the customer has given as a delivery address.
- Block the IP address if the customer makes multiple attempts using different cards.
- Call Euroline and ask for an address check if you are uncertain about large purchases.
- Inform Euroline at once if you notice unusual behaviour, unusual increases in transaction volumes, etc.
- Analyse and learn from all fraud-related complaints. What went wrong? How can you prevent the same thing from happening again?
- Refunds should always relate to a purchase transaction, and should always be credited to the same card as used for the original purchase.
- The value of a refund should never exceed the original purchase transaction amount.

word, the bank provides verification, and the merchant is given the go-ahead for completing the purchase.

3D Secure requires that the merchant has the Merchant Plugin software. Be sure to use a PSP which can offer this technology. Your customers, however, do not need any special software in order to use 3D Secure.

### **Ask for information**

A relatively simple way of making online fraud more difficult is to ask your customers for more information. For example, ensure that your customers create a customer profile before ordering, and make the profile fields mandatory.

### **Check the information**

Use a directory enquiries service to check that the telephone number provided matches the delivery address. If you have any doubts, call the telephone number listed for the address to check.

### **Deliver to registered address**

Advise your customers on your website that you only send goods to addresses registered to civic registration numbers. When delivering, never give out the parcel number online or by telephone. Fraudsters often try to find out the parcel number since this is easier than actually receiving the delivery notification.

### **Secure payment**

An authorisation code for an approved purchase doesn't necessarily mean that everything is ok. The authorisation code means that sufficient funds have been earmarked in the account to which the card is linked. However, this is no guarantee that the card has not been used fraudulently or is counterfeit. And if this turns out to be the case and you have failed to process the card payment in accordance with the applicable agreement, it is you who will bear the risk of any fraud. It is therefore crucial that you carry out your own checks.

## **Would you like to find out more?**

You can find out more at [www.euroline.se](http://www.euroline.se) or by calling Risk Control on +46 (0)8 14 69 90.