

Ten tips for safer e-commerce

E-commerce continues to grow, and according to the Swedish daily Svenska Dagbladet (5 August 2005), card payments over the Internet are on the rise. Intraregional sales with credit cards over the Internet, mail and telephone order has increased by about 74 percent this year compared with last year. This in-

crease provides substantial opportunities for you as a merchant.

Increased sales also mean more customers, and with that a heightened risk a swindler will cause damage through fraudulent purchases. There are, however, several measures you can take to reduce your risks.

- Use the standard 3D Secure – Verified by Visa and MasterCard SecureCode.
- Use a payment service provider that is certified in accordance with the Payment Card Industry (PCI) Data Security Standard.
- Keep in mind that if you handle credit card information in your systems, you may also need certification in compliance with the Payment Card Industry (PCI) Data Security Standard.
- Always submit the security codes CVV2 and CVC2 in an authorisation. The three- or four-digit security code is on the back of the signature panel on the customer's card.
- Make reasonable assessments before you deliver goods abroad.
- If possible, allow only one purchase per card number per day.
- Verify that the customer's IP address agrees with the country he/she has specified in the delivery address.
- Call Euroline for an address verification if you feel uncertain about high purchase amounts.
- Inform Euroline immediately if you notice deviating sales patterns, such as unusual increases of transaction flows, etc.
- Get to know your customers! New, unknown customers demand more caution than old, familiar customers.

Contact your payment service provider (PSP) or Euroline, in case you want to find out whether your payment solution supplier provides support for 3D Secure, and also if they have undergone certification in accordance with the Payment Card Industry (PCI) Data Security Stan-

dard. At the following website address (http://www.visaeu.com/acceptingvisa/pdf/AIS_Certified_Service_Providers.pdf), Visa has listed payment service providers that have thus far applied for certification, along with the status of their certification.

PCI – Payment Card Industry Standard

The payment card industry has agreed on a common standard for handling card information. The standard is called Payment Card Industry (PCI) Data Security Standard and has been accepted by all global card payment schemes including Diners Club, MasterCard and Visa. This standard places demands on credit card information storage and handling by merchants, as well as by their partners and suppliers. The purpose is to protect all parties submitting and receiving credit card information against unauthorised access. PCI helps you protect yourself against risks such as man-in-the-middle attacks and spoofing.

Man-in-the-middle attack

A man-in-the-middle attack entails the situation where a third party monitors, and in some cases changes, traffic between two parties. There are several variants of man-in-the-middle attacks. One of them is IP spoofing.

Spoofing/IP spoofing

Spoofing is an umbrella term for various ways of committing fraud. IP spoofing entails that a hacker alters communications so that they appear to be coming from a trusted IP address (usually an address that is perceived as safe and known) when they are actually coming from another. The purpose of IP spoofing is to circumvent security controls and access sensitive information in systems.