Payment Services

# Security tips for Mail-/Phone-Order

**The fraudulent use of card numbers in the distance payment business causes substantial losses each year, which are also associated with high administrative costs. By providing the following information, we would like to help you better protect yourself from card defrauders.**

The defrauders often proceed according to the following pattern:

– A large order is placed per fax, e-mail or phone, which should be delivered immediately per express or through a package courier at the ordering party's expense. The delivery address is generally located abroad, or delivery to a hotel or a general delivery is requested.
– Payment is often made using several cards.

According to the contract conditions for the distance business, you are obligated to obtain an authorization for all transactions. However, the authorization only confirms the validity of the card and the cardholder's creditworthiness at the point in time in question.

Whether the person placing the order is the legitimate cardholder or whether someone else is making an illegal order using that person's card and data cannot be verified beyond all doubt.

For this reason, the card organizations disclaim all liability for orders placed per fax or phone.

## You bear the risk

While the defrauder receives the goods, the legitimate cardholder refuses to accept the charges. This often can be very unpleasant for the merchant concerned. He/she suffers both the loss of the merchandise and receives a chargeback for the entire transaction amount.

**The following tips should help you to minimize the risk:**

## 1. Card acceptance

According to the card acceptance contract, orders can only be accepted by fax and phone or through a Web shop. If you receive orders by e-mail that contain card data, inform the sender that this type of order is not permitted.

Be sure to delete the card number in the e-mail before replying to it. Print the e-mail out and then totally delete it from every electronic store, including your inbox trash, and any backup server.

## 2. Physically present card data

Make sure that paper documents that list complete card numbers are never left unattended and please dispose of them properly. Such documents are to be destroyed with a paper shredder so that no information can reconstructed.

Implement a policy of only retaining document containing card data for the absolute minimum length of time necessary.

## 3. Transmission of card numbers

Before you transmit card numbers, consider whether the recipient needs the complete card number. If not, then send the card number in the following format: xxxx xxxx xxxx 1234. This way of displaying the card number is known as PAN truncation.

Unencrypted card numbers may never be sent by e-mail. If necessary provide the card data either by phone or fax.

## 4. Internet orders

We recommend that operators of online shops use the new standard security solutions, "Verified by Visa" and "Mastercard SecureCode" with the appropriate payment software (Merchant Plug-in, MPI). These processes can significantly reduce the risk of fraud.[1]

If you have your own order form, be sure that the ordering procedure adheres to the PCI DSS standard (no requesting of CVC2/CVV2). Within the ordering procedure, be sure to check whether card data is transmitted or potentially also (temporarily) saved.

## 5. Scrutinize the order

Take care with orders involving unusually high volumes and amounts, a rapid ordering rhythm or which originate from e-mail addresses from free providers such as yahoo.com, gmx.com or hotmail.com.

## 6. Checking the delivery address

Check the delivery address very precisely if it does not match the ordering party's residential address.

We strongly advise you against making deliveries to developing countries, particularly Africa, the Far East and South America, as well as countries from the former Soviet Union, unless you are dealing with established customers who are known to you.

Also be careful with deliveries to be sent to a P. O. box or a hotel.

## 7. Weigh the risk

Would you also make the delivery with payment per invoice? While credit and debit cards, such as Maestro, are very practical means of payment, they are not collection tools.

You know best how your business cases generally proceed. If you are in doubt, but would still like to make the deal, then we recommend that you contact your bank regarding an export risk guarantee.

[1] No Merchant Plug-In is required for the Diners Club and Discover card brands.

110.0174.02 INT_EN/07.2018

Your local point of contact can be found at: www.six-payment-services.com/contact

**SIX Payment Services Ltd**
Hardturmstrasse 201
8021 Zurich
Switzerland

**SIX Payment Services (Europe) S.A.**
10, rue Gabriel Lippmann
5365 Munsbach
Luxembourg

**SIX Payment Services (Austria) GmbH**
Marxergasse 1B
1030 Vienna
Austria

**SIX Payment Services (Germany) GmbH**
Langenhorner Chaussee 92-94
22415 Hamburg
Germany