Avoid card fraud in your webshop

International cards

Your digital security guard

In a physical store, you have surveillance cameras, shop detectives, alarms at the entrance and exit, and staff who keep an eye out for suspicious customer behaviour. What do you do to protect the integrity of your online web shop? Here are some guidelines that are good to keep in mind.

WHEN SHOULD YOU PAY SPECIAL ATTENTION?

- Compare the orders with the normal sales in the webshop. This can be in relation to product choice, customer behaviour, time of the order, etc.
- Use common sense when evaluating the orders: is the purchase reasonable and expected, or is it too good to be true.
- If applicable, use previously received chargebacks to identify what is characteristic of fraudulent orders in your webshop. (e.g. amount, product categories and composition, time of order, form of delivery, IP addresses, etc.)
- Remember names, e-mail addresses, billing addresses, telephone numbers, etc., with which you have previously experienced fraud.

MANUAL CHECK IN CASE OF SUSPICION

A fraudster who only has the card number usually does not know anything about the real cardholder's contact details and therefore has to invent them. Here is a checklist of procedures for handling risky orders:

- Search the name and phone number of the person who orders, and check if the name and address exists (e.g. via MobilePay, Facebook, Google, etc.)
- Compare name, phone number, address, e-mail, IP address etc. If necessary, ask your payment module for information about IP addresses on your orders.
- Call the telephone number registered at the address (and not the one stated in the order.)

A FIXED CONTROL PROCEDURE

- Make sure employees have been clearly informed about how to check an order and what to do if they suspect attempted fraud.
- Set up a policy for the number and size of orders that you want to allow to be

processed. How many orders for the same person/card/ geographical location will you accept?

- What makes orders remarkable for you? Focus on training the staff so that everyone knows when an order must go through an extra check and how this must be carried out.

USE THIRD PARTY TOOLS

It is often possible to get extra information from the payment module, e.g. about IP addresses, rejected transactions, etc. Several payment modules also offer to send fraud alerts or have dedicated fraud modules. Request these services from the supplier of your payment module.

Rejected transactions are of particular interest: If a purchase is first rejected on three different cards and then goes through on the fourth, there is a risk of fraud. Few people have several cards and simply take the next one when the first doesn't work.

SECURITY IN CONNECTION WITH ECOMMERCE

There is only one solution that secures you as an ecommerce business: 3D Secure. In the case of fraud, the solution usually guarantees your payment.

Note: The webshop is responsible for losses as a result of fraud in the case of web orders that are not fully 3D validated. This also applies even if the amounts have been approved.

WHAT IS CARD FRAUD?

Card fraud in online shopping occurs when criminals get hold of card information, for example via

- Phishing and other ways to capture card data and other sensitive data from the customer

- Data breach (hacking of a database with card information and other sensitive data)

- Systematic guesses (a robot that tests series of card numbers starting with the same 6 digits)

Often this card information is sold online, and it is other criminals who make the fraudulent purchases

Anything that deviates from the norm is suspicious

REJECT SUSPICIOUS ORDERS

If the checks do not remove the suspicion of fraud, you must reject the order. You can possibly ask the customer to identify himself further or for an account transfer instead.

Suggested checkpoints

Fraud transactions often deviate from regular orders or normal customer behavior. They often have several of the factors below in common. The more of these 'warning lights' that are on, the greater the risk of fraud:

- Orders received at night
- Orders from unusual countries
- Delivery to hotels, post boxes, c/o addresses, holiday homes, factory buildings etc.
- Free/anonymous email addresses
- Express delivery (regardless of additional costs)
- Ordering unusually large quantities and/or goods of particularly high value
- Discrepancy between delivery and billing address or IP country and delivery country, etc.
- Multiple purchases on the same card number or IP address
- The same product is attempted to be purchased with several different cards
- Discrepant customer information for multiple purchases, e.g. same email address but different names or addresses, or where IP address and delivery address do not match
- Multiple orders where all card numbers begin with the same six digits
- The goods can be easily converted into cash
- Will you normally be contacted before purchase?
- The 'customer' sounds confused (e.g. can't remember his address or what has been ordered) if you contact him/her
- The 'customer' does not know anything about the product that he/she has ordered
- Orders from abroad: Is it possible to buy the product cheaper there?
- Is the customer's name formatted abnormally (upper/lower case letters) or contains spelling mistakes or substitute letters?