coface
FOR TRADE

FRAUD

IS A FAST-GROWING THREAT

Prevent identity fraud and scams

coface.com

FRAUD IS A FAST-GROWING THREAT

Corporate identity fraud is a "booming business" in the B-to-B world. Its broad scope and evolutionary nature means businesses must take **proactive actions in protecting their assets and identity** against this threat.

Beware of the goods delivery scam!

Coface's customers have recently had to deal with multiple cases of identity fraud regarding the delivery of goods (wines, building materials, etc.). Fraudsters usurp the names of well-known retail distributors, or even transport companies, to place orders: the goods are sent, but the invoice is never paid.
Increased vigilance is therefore recommended. Practice shows that companies with strict internal procedures in the field of customer and order acceptance and adequate credit management are far less likely to be victims of unfair trading practices.

The operating method of scammers (not exhaustive).

Fraudsters often use the identity of a bona fide company in these cases. The so-called buyer gives the contact details (surname, first name, email) of a distributor whose name has been usurped. Individuals then impersonate or represent this company and place orders on its behalf. The fraudster contacts the seller by phone or email to request information on the products and announces a large order with payment within 30 or 45 days after receipt.
The fraudster presents his alleged company in writing and provides all the documents necessary to put the seller in confidence (certificate of incorporation, bank account number, etc.) which are also usurped.
The delivery address might be a place not related to the retail distributor, or the driver can be notified, at the last minute, of a change in delivery address.
Once delivered, it appears that the contact person does not work for this company (or the real person has not ordered anything) and the goods have not arrived there. The invoice is of course never paid.
Sometimes, the fraudster quickly passes a second order after the delivery of the first.

How to prevent such frauds?

A fraudulent order can sometimes be recognized. Therefore, please take the time to check some important points when you receive a new order. Fraudsters are well organised: they create new phone numbers and e-mail addresses, order forms, or deposit false financial statements in order to obtain delivery on credit. It is therefore advisable to be extra alert, especially if an order is placed by a foreign company or if the client is still unknown to you.

Trade Register.

Request a recent extract from the official trade register. This applies to all new clients, of course, but it is also advisable to request and check a new extract periodically for existing clients.
In addition to an extract from the trade register, you can request a copy of the ID of the director authorised by the register. Clients who are in good faith will have no problem providing such proof.

Verify information through the Internet.

- Verify available business information as far as possible on the Internet and social media, including:

- The names of directors and/or persons representing a company. Although many crooks are smart enough not to show themselves on the internet, some of them have been caught with something in the past.
- The business address. Through programs such as Google Maps it is easy to take a look at the (alleged) business address and/or delivery address of the potential customer.
- The company website. Most companies nowadays have their own website, which is also often mentioned in the Chamber of Commerce extract. Check if this website is still active and if the contact details match the details of the new customer/order.
- Compare the company logo on the website with that of the order.

Other points of attention in the order phase.

- In case of a telephone order, especially if it is a first order, it is wise to look up the general telephone number of the company and ask if you can speak to that person again. Always register the name and contact details carefully.
- Compare the telephone number format.
- Errors in spelling and/or grammar in written correspondence occur regularly, especially in the special terms and conditions. It is recommended to pay extra attention to this, you can draw up an internal working method to establish the authenticity of these documents.
- Check whether the company actually operates in the country of destination of the order, or whether it has a subsidiary there and/or ongoing projects.
- Check whether the debtor's business activities are appropriate for yours. If in doubt about the order, call the debtor for confirmation. Make sure that your employees understand the importance of this working method.

Delivery phase.

- In addition to the business address, you should also check the delivery address (Google Maps, etc.), especially if these addresses differ from each other. Make sure that it is clear in advance who will receive the goods on behalf of the debtor (preferably record this in writing) and instruct the driver to always ask for ID proof and not to deliver without consultation in case of deviating or suspicious situations.
- Sometimes the fraudster will come and collect the goods himself. Again, it is important that it is established in advance (in writing) who will collect the goods on behalf of the debtor and that this person can provide proof of identity.

A fraudster may also pose as your supplier.

Some of the points mentioned also deserve attention when a supplier or creditor asks you to change the address or the bank account details. Cases of phishing and transfers to fake bank accounts are also still common. It is therefore important to always verify all requests for changes (of addresses or bank account numbers) via the details of your supplier known to you.

Prevention is better than cure.

A few more tips, because in most cases of fraud a cure is not possible:

- Scammers often forget to negotiate prices, although this may be common in your industry.
- Don't be fooled by the knowledge of a potential customer, they are often surprisingly well informed about what to do and what not to do in the market in which you operate.
- Scammers often make their move during the holiday period or in the weeks leading up to national holidays. They know that the occupancy of many companies is under pressure during these periods and/or that in some sectors it is a peak period, which sometimes reduces the alertness in order acceptance or accounts receivable management.
- It is always advisable to deliver to new customers on a prepayment basis. Note that in many cases a scammer tries to "build" trust by paying a number of small deliveries in advance or quickly before taking a hit with a larger order on a credit basis.

Finally.

If you are the victim of fraud, report it. In some cases the perpetrators can be identified and with sufficient evidence they can be punished for i.e. participation in a criminal organisation, bankruptcy fraud, embezzlement, fraud, forgery, money laundering and/or handling stolen goods.

ENG_FRAUD_122020_REV01

coface.com

coface
FOR TRADE