Identity fraud

Good advice on how to avoid being cheated by a buyer with a false identity.
“Identity fraud is when a swindler uses the identity of established and creditworthy companies”.

False identity fraud on the rise

The false identity is used to “purchase” products on credit. The swindler assumes the identity of a creditworthy company and places orders in the company’s name.

The swindler ensures that the products are delivered to a different address from the real company’s address or offers to collect the products himself. When the supplier later presses for payment, the swindler has disappeared and it turns out that the real company (which was thought to be the buyer) does not know anything about the case. The real company is therefore not obliged to pay and the supplier is left with a loss. It should be noted that a credit limit covering the real company does not cover the loss, as there is no valid claim against this company.

The products, which are most often involved in this type of fraud, are easily marketable standard products such as fish, dairy products and meat, IT-related products and construction materials, where it is common for the buyer and the seller to have limited knowledge of each other.

In recent years, Atradius has experienced a steady increase in this type of fraud in England, Germany, Italy and Poland. The swindlers continuously refine their methods of appearing credible by creating false websites and email addresses, which bear a close resemblance to those of the real company.
How do you avoid identity fraud?

In practice, two conditions must be fulfilled in order for the fraud to be successful. The supplier must be kept from having contact with the real company until delivery has taken place and the products must not be delivered to the real company’s address.

Call the company at the official telephone number for confirmation that they know the buyer who has contacted you.

Companie...
The creative fraud

A supplier of IT products receives a promising enquiry by email from a Dutch company, which is a subsidiary of a large French transport group. The buyer states that they are responsible for the IT operation of the group, and that important parts have to be replaced. They therefore request an offer, which they accept after some negotiation. The supplier issues an invoice, which must be forwarded by email according to instructions from the buyer. The supplier then sends the equipment through a forwarding agent to the company’s official address in the Netherlands.

When the invoice falls due, the seller starts pressing for payment but cannot get through to the Dutch company. The seller then contacts the French parent company, which states that they don’t know anything about the case and denies any payment liability by them or their Dutch company.

A further investigation then reveals that the Dutch subsidiary is a very small entity, which has therefore had its address at an office hotel. The identity swindlers had also rented premises at the office hotel, but on a different floor and with an “IT department” added to the name.

The reception staff at the office hotel had probably been informed by the identity swindlers that they should just call them when the products were delivered to the company.

This case illustrates that the “identity fraud business” involves product development. In this case, an elegant solution had been found for delivery of the products to the registered address. A comparison between the email address from the buyer and the email addresses on the real buyer’s website would have revealed inconsistencies. Two persons have allegedly been arrested in connection with this case. It is unlikely that only one company has been subjected to this fraud and the swindlers must have been caught in the act at a point where someone has become suspicious of them.

The failed fraud

A Danish supplier of foodstuffs is contacted by email by Mr. Lucas Cotterill, the manager of a well-established English food company. The email includes a link to the company’s website, but only a mobile telephone number and an address, which has no connection to the correct company, are stated. TheDanish supplier therefore becomes suspicious and contacts Atradius.

We are then able to inform the Danish supplier that one month earlier the company had sent us an email with a warning that they had been the victim of identity fraud. When we receive such warnings involving otherwise creditworthy companies, we inform our customers, who do business, or think they do business with the real company, that we have found cases of identity fraud. We add the following text to the credit limits which we issue: “We have become aware of attempted fraud by persons pretending to be representatives of the buyer. You should therefore be extra careful to ensure that you are doing business with the real buyer.”

One month earlier, the company had sent us an email with a warning
Disclaimer
This report is only for information purposes and is not in any way intended as a recommendation of any particular transactions, investments or strategies for the reader. Readers should make their own independent decisions, commercially or otherwise, in respect of the information. While we have made every effort to ensure that the information in this report has been obtained from reliable sources, Atradius is not liable for any errors or omissions or for the results achieved from using this information. All information in this report is provided “as is” without any guarantee of completeness, accuracy or topicality, or of the results of its use and without any guarantee of any kind, either express or implied. Atradius, its affiliated partnerships or companies or their partners, agents or employees will not under any circumstances be liable to you or anyone else for a decision made or action taken on the basis of the information in this report, or for any consequential damage or special or other damage, even if you have been informed of the possibility of such damage.

Copyright Atradius N.V. 2015