

STOP FAKE BUYER FRAUD

26%

26% of executives surveyed worldwide experienced vendor, supplier or procurement fraud in 2016. In 2015 this was 17%. A rising trend.

Source: Kroll Annual Global Fraud & Risk report - 2016-2017

A LOSS THAT IS NOT COVERED

The insurance of receivables does not cover false buyer fraud. A credit insurance policy clearly identifies the buyers involved in the transactions. Fake buyers are evidently not on the list.



WHAT IS FAKE BUYER FRAUD?

It's a kind of impersonation fraud. The fraudster uses a fake identity or steals the identity of one of your regular buyers to place an order. Your company delivers the goods to an unfamiliar address and they disappear... The fraud is usually discovered when payments are overdue.

6 WAYS TO PROTECT YOURSELF



1. USE YOUR CREDIT INSURER PROACTIVELY

Does an order make you suspicious?
Ask your credit insurer to check the buyer.



2. INSPECT YOUR ORDERS CAUTIOUSLY

Fake buyer fraud is very difficult to recognise. So be on your guard. For instance: does the buyer use a Gmail account? In business to business, company e-mails are mostly standard.



3. IN CASE OF DOUBT: CHECK BY PHONE

Whenever something looks suspicious it is good to verify by phone. But watch out: even the phone number on the order may lead you to the imposter. So it's better to get the right contact details via an independent source.



4. CHECK THE PLACE OF DELIVERY

Is the place of delivery unrelated to the facilities of the buyer? You can check on Google Street View. Or you can consult your credit insurance company. Maybe the strange address is really a warehouse used by your customer. But maybe not...



5. VERIFY THE IDENTITY OF THE SENDER

Usually there have been previous contacts with the buyer. Do you recognise the name? Is it spelled consistently? In case of doubt check whether the person really works at the company.



6. TAKE CARE OF YOUR IT SECURITY

New forms of fraud involving fake identity are turning up. One example is 'pay diversion', where a fraudster exploits an e-mail address of your company to send a forged invoice, containing a fake bank account number. Sometimes imposters even steal the identity of the CFO or CMO to instruct the accountant to transfer the money.