December 2018

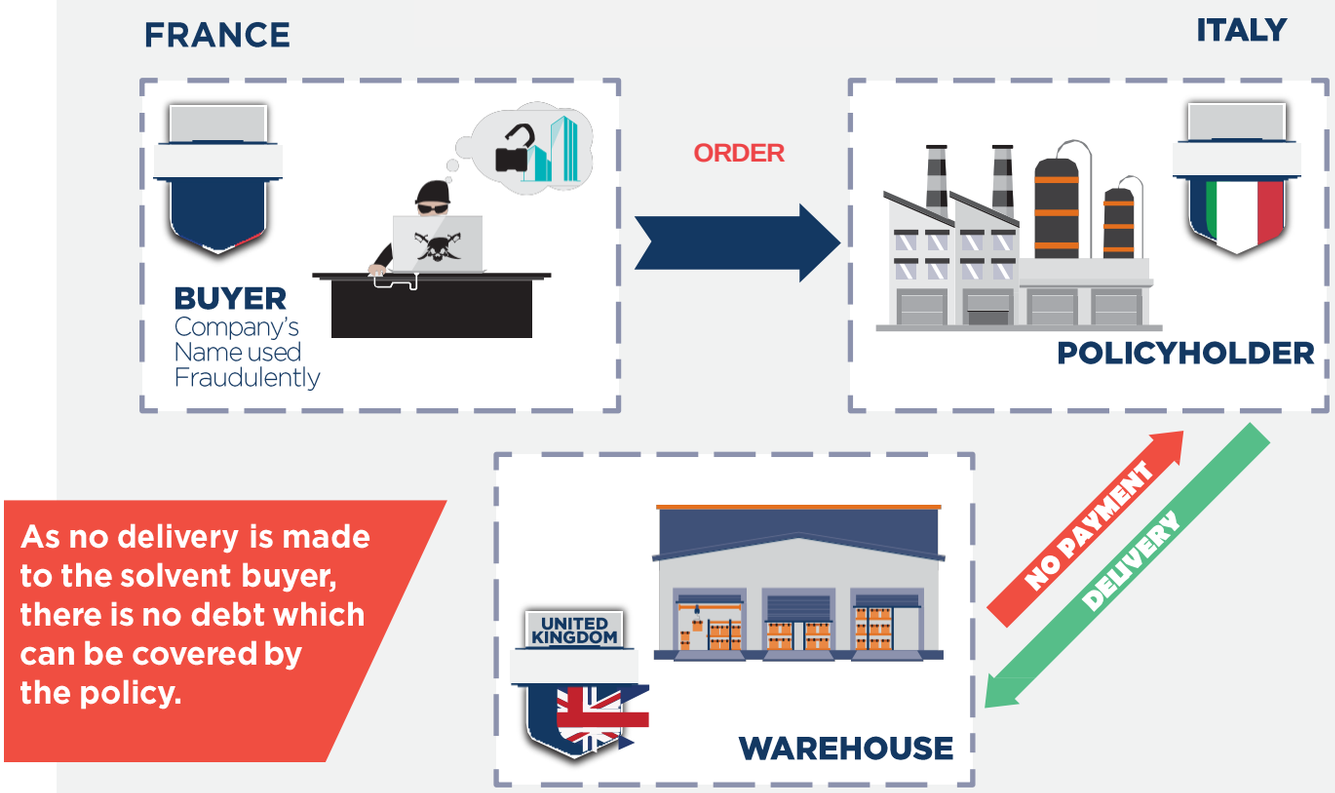
ALERT ON CORPORATE IDENTITY FRAUD

Corporate identity fraud is one" 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 plague.

When a false corporate identity or another company's identity details are used to support unlawful activity, it represents a serious operational risk.
In the last few weeks, Coface has been informed for several scams linked to identity theft and recommends increased vigilance.

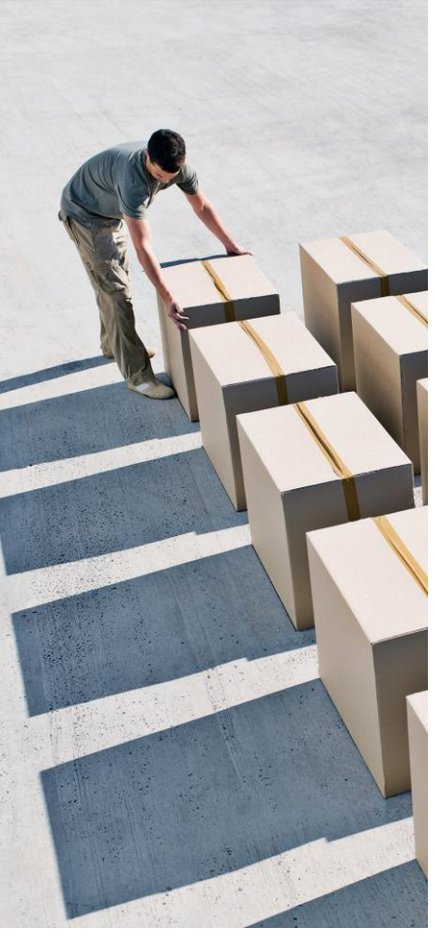
In practice, fraudsters use the business identity of a real company, preferably with good payment record and reputation, to procure goods and services from our customers / policyholders
The recent scheme of fraud, we have been recently confronted with, can be described as follows:

Corporate identity fraud: example



As no delivery is made to the solvent buyer, there is no debt which can be covered by the policy.

To process, the fraudsters are rather well organized, they open phone lines, create email addresses, falsify order forms, buy certificates of incorporation and financials to the commercial register in the aim of opening a buyer account in a company.
This is the reason why some precautions should be observed when you receive an order form, especially when it comes from abroad and from a new buyer.



Indeed, a fake order form proves to never be perfect. Stopping a fraudulent order is well worth a few moments of time taken to verify.
When your procurement/ commercial department receives an order, this basic checklist can highlight any obvious areas of concern. So make sure you:
- **Compare the company's logo on the website with the one on the order, it could be sometimes different.**
- **Compare the email address format (name of the person and of the company) of your correspondent with the ones you can find on the website (often in the navigation link "Contact"), as there usually is only one format for all the company. Any difference should be considered suspicious (ex : david_smith@company.fr, becomes d.smith@company-service.com, or smith_david@company-group.eu ....)**
- **Be especially careful to the generic email addresses ex: accountancy_company.com**
The fraudsters regularly use names of persons who really work for the company.
- **Compare the Telephone number format (especially the first 2 digits)**
- **Check if the company is operating, have a subsidiary or a project in the country where the goods have to be delivered.**
- **Syntax errors or spelling mistakes can be found in the order form and especially in the specific conditions. Hence, you need to pay attention to such document and set up internal measures to check the validity of the document.**
- **Ask yourselves if the buyer's activity is compatible with yours.**

Trust, but verify: when in doubt (order, change of bank details...), always call your buyer to confirm, and ensure your accounts employees understand the importance of the matter.
As a reminder, phishing cases and payments made on fake bank account are still common. It is therefore always important to confirm all types of requests (address, bank account) modifications with your supplier.

FAX AND E-MAILS ARE NOT SAFE

coface
FOR TRADE