coface
FOR SAFER TRADE

January 2017

ALERT ON CORPORATE IDENTITY FRAUD

Corporate identity fraud is a "booming business" in the B-to-B world. Its broad scope and evolving nature means businesses must take proactive steps to protect their assets and identity against potential loss.

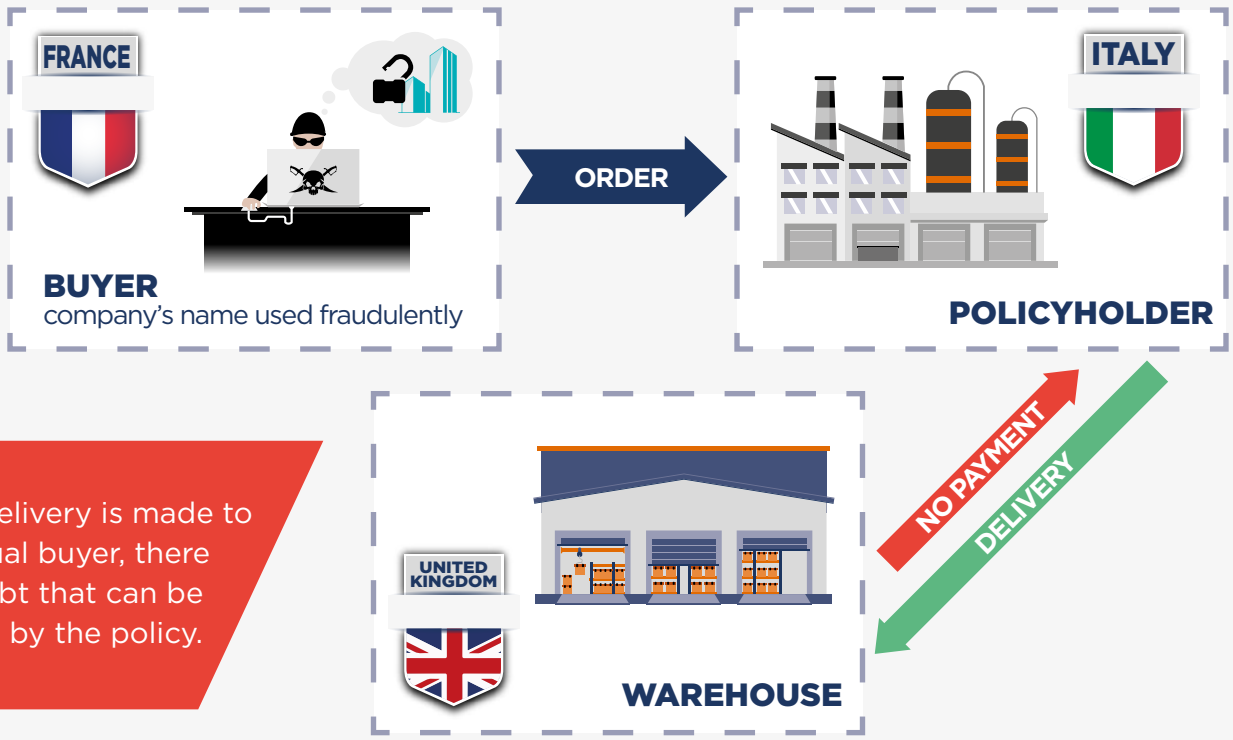
When a false corporate identity or another company's identity details are used to support unlawful activity, it represents a serious operational risk.

In the last few weeks, Coface has been informed about several scams linked to identity theft and recommends increased vigilance.

In some cases, fraudsters use the business identity of a real company, one with a good payment record and reputation, to procure goods and services from our policyholders.

Here's an example of a recent identify fraud scheme that a Coface policyholder experienced:

Corporate identity fraud: example



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

Fraudsters also establish completely fake companies -- they create phone numbers and email addresses, falsify order forms and certificates of incorporation, and invent financial statements with the aim of establishing credit.

This is the reason why precautions should be taken when you receive an order form, especially when it comes from abroad or from a new buyer.

A fake order form typically contains flaws. Stopping a fraudulent order is well worth a few moments of time taken to verify its authenticity.

When your procurement/sales department receives an order, this basic checklist can help uncover 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 be different.

• Fraudsters regularly use names of persons who really work for the company.

Compare the email address format (name of the person and the company) of your correspondent with the ones you can find on the website (often in the "Contact" section,) as there is usually a standard format for the entire company. Any difference should be considered suspicious (for example: david_smith@company.com becomes d.smith@company-service.com.)

Be especially careful of generic email addresses such as accounting@company.com.

• Compare the telephone number format.

• Check if the company operates in the country where the goods are to be delivered.

• Review all documentation such as order forms and contracts for syntax errors or spelling mistakes. It makes sense to set up internal measures to check the validity of the documents.

• Ask yourselves if the buyer's business activity is compatible with yours.

Trust, but verify. When in doubt, always call your buyer to confirm, and ensure your credit and accounting staff understand the importance of the matter.

As a reminder, phishing cases and payments made on fake bank accounts are still common. It is therefore always important to confirm all types of requests (address changes, bank account modifications) with your trading partners.

coface
FOR SAFER TRADE