BNP PARIBAS

The bank for a changing world

TRANSFER FRAUD: COMPANIES IN THE FIRING LINE

Credit transfer scams are on the rise, and no company, be it a large group or an SME, is safe. In this two-part article, Corinne Bertoux, Divisional Commissioner and Head of the OCRGDF (French Central Office for the Repression of Great Financial Crime), sheds some light on this phenomenon and gives some advice on how to avoid falling for it.

COMPANIES IN THE FIRING LINE

Since 2010, a large number of French companies have fallen victim to fraud through identity theft. Can you give us an overview of the damage suffered to date?

We estimate that French companies have been defrauded of more than 550 million euros since 2010 using the social engineering technique. If large French companies were the first victims of this type of fraud, **criminal groups have since turned their focus towards organisations of varying sizes**, which are more vulnerable as they are often not as well informed. Impersonation fraud, what law and order forces call international credit transfer scams, now target everyone.

What are the most common types of impersonation fraud seen today?

International credit transfer scams can take various forms. **CEO fraud is still extremely common**. The fraudster assumes the identity of the CEO, the CFO, a company lawyer, etc. and asks an employee to carry out an urgent transfer to a third party under the pretext of an acquisition, tax audit or something similar. Thinking they are doing the right thing, the employee makes the transfer.

Another common scam is **change of bank details fraud, also known as vendor scam**. This involves fraudsters contacting a company's accounting department while pretending to be a supplier. The fraudster asks invoices to be paid into another bank account, whose number is provided by the fraudster.

We are also seeing **fake technician scams**. In this case, the fraudster poses as a technical officer informing you of a migration, test or incident on the tool that manages the accounts and transfers. Generally, they then work on their target's computer under the guise of carrying out maintenance.

Recently, we have also seen **fake minister scams**, directly targeting company CEOs or honorary presidents. Fraudsters succeed in gaining direct contact to convince the person concerned to move money abroad under the proviso of fighting the so-called Islamic State.

This type of fraud aims at convincing employees that the request is legitimate. How do the fraudsters handle themselves to be able to build up such a trusting relationship?

They instil confidence as they have detailed knowledge of their victims. Thanks to the internet, today fraudsters can gather a huge amount of open-source information on their targets through social networks, interviews or social and financial reports, for example. By creating an e-mail address closely resembling that of a director, client or supplier, they deceive their victims, who then carry out their requests. **Knowledge of the company as well as an extremely convincing tone of voice are key for these scams to succeed.**

Some fraudsters will even impersonate police services (e.g. police headquarters or the OCRGDF) when contacting companies for bogus transactions. The thieves' imaginations are boundless, and they are constantly evolving according to their victims' reactions. **We are talking about social engineering.**

What is the profile of these fraudsters?

Credit transfer fraud began with and was developed by Franco-Israeli criminal groups. Using call centres generally located in Israel as well as anonymous technical methods, they first targeted large French-speaking companies and their subsidiaries abroad. They have since moved on to attack companies and organisations of all sizes, impacting the whole of Europe and even the United States and Canada.

They use voice-over internet protocol (VOIP) services, which are difficult to trace, allowing them to simulate local phone calls. They also use software that enables them to impersonate those whose identity they have stolen.

They open intermediary bank accounts and use international money-laundering networks to retrieve the stolen funds, which generally pass through China.

How do you lead the fight against these criminal groups?

First and foremost, our goal is to block funds wrongly transferred abroad with the aim of recovering them. To do this, we are developing proactive cooperation among international police forces and **ask that companies who have fallen victim to fraud, or who have suffered attempts at fraud, communicate to us as soon as possible any useful information** so that we can cross-check different cases and start recovering funds.

To combat the anonymous nature of the entire system, we are focusing on money laundering by tracing the financial movements from one intermediary account to another to identify the different players taking part in these scams. **It is therefore important to pass on any bank account details provided by the fraudsters**, so that we can find, and act upon, the accounts from which the criminals are going to retrieve the stolen money.

How has the international partnership taken shape?

International cooperation is the cornerstone of succeeding in dismantling these organised and sophisticated criminal networks. **We have made significant progress over the years.** The OCRGDF has extensive knowledge of this issue and the partnership with Europol and Interpol has allowed significant information exchanges to be put in place with other European countries as well as those outside the European Union. Regular discussions have also taken place with the Chinese and Israeli authorities through internal security attachés from the international cooperation department in an attempt to curb this phenomenon. While the differing legislation does not make our job any easier, fraudsters have been arrested and prosecuted in France and abroad.

Do companies play a direct role in this fight?

The signing of agreements with MEDEF (French Business Confederation) on 10th March 2015 and the CDSE (*Club des Directeurs de Sécurité des Entreprises*) on 20th January 2016 by the Central Headquarters of the Judicial Police (DCPJ) allowed the partnership to be strengthened and exchange of information on the subject to be increased. **Private-public partnerships are essential in combating fraud; however, the trend is now moving towards attempted fraud rather than proven fraud.**

We should also mention the awareness campaigns run by companies, the police and the banks. These campaigns are the front line in the fight against fraud and continue to bear fruit.

ADVICE TO PROTECT YOURSELF AND REACT

How should a company react in the event of fraud or suspected fraud?

The first reaction should be **to contact their bank immediately so they can block the funds that have been wrongly transferred and to try to retrieve them.**

Next, the company should file a complaint with the police as soon as possible, who will in turn inform the OCRGDF so they can call on international partners to play a pivotal role in blocking the funds, if necessary.

In the event of attempted fraud, it is essential that the victim sends all relevant information (timeline, e-mails, telephone number, bank account details, etc.) to the OCRGDF so they can use and cross-check it against similar cases, to the following address: ocrgdf-sec.dcpjaef@interieur.gouv.fr

Do companies who have fallen victim to fraud have any chance of seeing misappropriated funds again?

To maximise the chances of recovering stolen funds, **it is essential to act as fast as possible, within 24 hours of the crime**. If not, things become very difficult as the funds are generally withdrawn or moved on to other accounts quickly.

We have seen a growing trend of fraud. Is this phenomenon set to continue?

Fraud will always exist – **the methods are becoming increasingly imaginative and the targets more and more wide-ranging**. Fake minister scams targeting celebrities or company CEOs, fake phone calls and directories targeting entrepreneurs, or even FOREX and binary option fraud targeting individuals, are all recent and common.

The risk of fraud is all around us. How can we limit it as much as possible?

The first thing to do is take a moment to **verify where e-mails come from and check the information they contain**. Even if we are in a world that cannot sit still, particularly in the financial sector, it is essential to talk about these things, define in-house procedures and strengthen checks.

Here are a few simple rules to bear in mind:

- **Inform and raise awareness among your employees**, particularly those responsible for payments, accounting and IT.
- Be vigilant day in, day out – take the time to verify and **limit the information made available over the phone or by e-mail**.
- Be mindful of what you post on social networks – avoid divulging information that could give a fraudster an insight into the inner workings of the company, for instance.
- **Strengthen the verification and signing procedures** for international transfers.
- Be even more vigilant during holiday periods or with lease payments, which are a favourite for fraudsters.
- When dealing with e-mails concerning international transfers, enter the originator's address you have on file yourself.
- Update the IT security system regularly.

Besides these preventive measures, here are some other signs that you should watch out for:

- An unexpected request for an international transfer, which is apparently urgent and confidential.
- A person using flattery or threat in an attempt to convince you, and providing large amounts of information about the company and its environment to back up their story.
- **An unexpected change of bank details**, telephone numbers or e-mail addresses.
- A technician calling and offering to help you with your banking solution.
- **Any request for information by e-mail or telephone**: a client asking that an invoice be re-submitted, a tax inspector, etc.