Client Alert | White Collar/Investigations

COVID-19 crisis in France: beware of fraudulent international wire transfers

March 2020

Authors: **Ludovic Malgrain**, **Arthur Merle-Beral**

The COVID-19 crisis has triggered a resurgence of fraudulent international wire transfers. Companies and banks should therefore be extra vigilant when dealing with international wire transfer orders.

The increase in fraudulent international wire transfers constitutes one of the several effects of the COVID-19 crisis and its consequences; notably, more online orders, receipt of online invoices, and working from home. Indeed, scammers are taking advantage of the COVID-19 crisis to carry out more and more cyber-attacks (through phishing emails and ransomwares attacks) and also to rob companies by using false identities and false purposes (*e.g.*, "urgent need for hydro alcoholic gel") to generate more international wire transfers diverting large sums of money.

To fight these types of fraud in such a critical period where companies' cash flows are strained, this note gives an overview of the disputes triggered by international fraudulent wire transfers between companies and their banks, the modus operandi of the scammers, and the need to raise awareness about these types of fraud within companies.

1. International fraudulent wire transfers give rise to litigation between companies and their banks

Companies are the first victims of such frauds followed by the banks that execute the fraudulent international wire transfers. Yet, except where the diverted sums are seized thanks to quick international judicial cooperation within a few hours of the fraud, companies and banks can point the finger at each other for the financial damage suffered.

Indeed, in parallel to international judicial cooperation to trace the diverted sums as well as the identity of the scammers and their accomplices, such transfers often trigger legal disputes before the French civil and commercial courts between the companies and their banks. In this type of litigation, companies accuse the banks for the failure of their employees to fulfil their professional, legal and contractual duties, and the banks accuse the companies of deficiencies in their internal control rules, particularly those of their finance and accounting departments.

In this respect, Article 1937 of the French civil code applies. Under this provision, "*a depositary must return the thing deposited only to the one who has entrusted it to him, or to the one in whose name the deposit was made, or to the one who has been designated to receive it*." Before the courts, banks are liable for the financial damage caused by international fraudulent wire transfers under this provision. Nonetheless, banks can exonerate themselves where they prove that the owner of the bank account, who allegedly requested the fraudulent wire transfer, committed an error that enabled or facilitated the execution of the fraudulent wire transfer.

Due to the differing nature of factual circumstances, the case law is not settled and courts often decide that banks and companies share responsibility and are each 50% liable for the financial damage caused.

2. The modus operandi of international fraudulent wire transfers and the risk of diversification of these types of fraud in the context of the COVID-19 crisis

Generally, the way international fraudulent wire transfers work follow the same pattern: scammers target an employee in the finance or accounting department of the company through a phone call or an email purportedly sent by the CEO or the CFO of the company (i.e. someone with unquestioning authority). Such contact can also come from a purported third party whose probity cannot be questioned (for instance, a Minister or a high-ranked representative of the government) or from a regular supplier known to the employee. Scammers obtain information on the employee via internet searches; these can often reveal a great deal of information and allow the scammers to build a relationship of trust with their target.

The underlying false purpose of the wire transfer will be set out in the communications with the employee. In this respect, the COVID-19 crisis has for example created a general feeling of fear associated with a desire to help the health sector that provides scammers with plenty of material to use.

Therefore, beyond the traditional false purposes such as "confidential M&A operation", "exceptional supply", etc., scammers will not hesitate to use purposes such as "hygiene masks needed", "charity for hospitals", "charity for healthcare employees", etc. In this context, all companies in all sectors, and not just those in the medical/health fields, may face such fraudulent approaches.

Eventually, scammers ask the employee to prepare an order for an international wire transfer, which they sign and email back to the employee. The employee then sends the order to the company's bank to execute the international wire transfer. Given the sense of urgency often invoked by the fooled employee, the ingenuity of the scammers, and the apparent genuineness of the order, the robustness of the bank's internal procedures can be severely tested.

Furthermore, scammers can diversify their techniques by taking advantage of the confinement imposed by the COVID-19 crisis. We can therefore fear that more and more false invoices will be sent to companies. Again, the genuineness of these invoices may be difficult to assess because most employees are currently only communicating by email, and not face-to-face.

3. Companies need to quickly raise awareness of these issues amongst their employees

In this context, raising awareness amongst employees of the financing, accounting and compliance departments is the only way for companies to stop the continued growth and diversification of international fraudulent wire transfers. Given the large sums often in question, doing so is essential to safeguard companies' financial health and continued activity.

In this respect, it may be useful to refer to the nine principles set out in October 2018 by the French banking federation in collaboration with the French police. These principles have proved their efficiency and it is critical to keep them top of mind during the current confinement, as well as prior to vacation periods and weekends:

- Implementing and complying with internal procedures re: wire transfers
- Raising awareness of fraud risks within the company

- Monitoring the evolution of frauds
- Monitoring the spreading of information within the company
- Acting with common sense
- Taking the time to double-check operations
- Making sure that remote access to banking services are safe
- Securing IT tools
- Contacting the bank and the police immediately in case of fraud or attempted fraud

At this stage of the COVID-19 crisis as confinement measures make face-to-face training sessions impossible, companies would be wise to implement e-learning sessions or live videos to remind their employees of these important issues. This is the only way to fight the increase in fraudulent international wire transfers.

White & Case LLP
19 Place Vendôme
75001 Paris, France

T +33 1 55 04 15 15