CENTRE DE DROIT
BANCAIRE ET FINANCIER

Fraudulent bank orders

Communication by email remains risky

Par Célian Hirsch le 23 June 2021

Who, the bank or the customers, should bear the damage caused by the execution of orders from hackers ? Shortly after the ATF 146 III 326 (cf. cdbf.ch/1150/), in which the Federal Court denied a trading company's gross negligence, the Ticino Court of Appeal was confronted with the same issue. Contrary to the decision of the Federal Court, it finds that the bank committed a serious offence, emphasising the danger of email communications (Judgment 12.2019.148 of 18 September 2020).

Two brothers, active in consulting in connection with the mining sector, open a bank account with a Ticino bank. They communicate mainly by email with their relationship manager and invest one million dollars in gold.

Several months after the account was opened, the bank receives, as attachments to an email apparently from the customers, two transfer orders to a Chinese bank. These orders, for USD 222,400, are nevertheless blocked by compliance. After a few emails, the bank receives the supposed invoices relating to the orders. They are for the purchase of injection pumps, pipes and connectors. The bank then executes the orders.

A few days later, the fraud is discovered. However, it is too late to recover the funds that have been sent to China. A criminal complaint filed by the bank is unsuccessful.

The customers successfully filed a request for payment against the bank with the *Pretore* of Lugano. The judge considered in particular that the parties had not agreed to the possibility of transmitting orders by email. Moreover, the employees, who had received no training in computer security, should have detected that the two orders were suspicious and unusual. They should therefore have called the customers. Furthermore, the country of destination of the orders, namely China, is known to be the source of computer fraud. Therefore, even if the orders had been transmitted in accordance with the contract (for example by fax), the serious fault of the bank prevented it from passing on the damage to the customers.

In its appeal to the Ticino Court of Appeal, the bank first argued that the orders had been sent by fax, and therefore in accordance with the contract. In any case, communication by email had not only been imposed by the clients, but they had also accepted it by conclusive acts. Finally, the orders were usual and not suspicious. The bank would therefore not have committed any serious misconduct in executing them.

The Cantonal Court began by pointing out that the case concerned the execution of fraudulent bank orders. It was therefore a question of determining whether the bank had executed the instructions in accordance with the contract and, if so, whether it could validly pass on the loss suffered to its customers.

Regarding the means of communication of the fraudulent orders, the Cantonal Court considers that it cannot determine with certainty whether the orders were only transmitted by email attachment, or whether they were also transmitted by fax, as the bank claims. It does not settle the question and moves on to the second stage, which deals with the bank's fault.

The Court of Appeal recognises that the customers themselves opted for communication with the bank by email. However, the bank accepted and used this from the outset. The hackers, having access to the electronic exchanges, were able to use these communications to better conceal themselves. The bank was therefore negligent in never drawing the customers' attention to this risk. Furthermore, email communication with foreign customers was a common practice and form of communication for the bank. The former IT manager also stated in the proceedings that this was a known risk situation. The Court of Appeal concluded that this 'situation of increased danger' required the bank to take adequate measures and to act with a certain degree of caution.

In this case, the bank was aware that the orders required more thorough verification since they were initially blocked. However, these verifications remained incomplete. In fact, the invoices sent by the *hackers* had nothing to do with the customers' activity (purchase of injection pumps, pipes and connectors). Furthermore, it was a private bank account, not a business account. These invoices, intended to justify the orders, were clearly suspicious. Moreover, it is well known that China, as a country of destination for payments, presents a high risk of fraud. The mention of an 'urgent' nature for the execution of the orders should also have raised doubts. Finally, the bank could simply have made a call-back, especially since the bank had already had telephone contact with its customers in the past.

In view of all these circumstances, the principle of equity (art. 4 CC) and the judge's discretionary power, the Court of Appeal confirms the assessment of the *Pretore* : the bank committed a serious offence. Therefore, it cannot pass on to customers the damage caused by the execution of fraudulent orders.

As mentioned in the introduction, this Ticino ruling has certain similarities with ATF 146 III 326 (cf. cdbf.ch/1150/). In both cases, the bank executed orders from hackers sent by email. In both cases, the hackers were able to use the emails between the bank and its client as inspiration, in order to go unnoticed, at least at that level. That being said, in the ATF, the orders were executed in favour of a well-known bank in the United Kingdom, and not a bank in a high-risk country. This criterion, although insufficient on its own, nevertheless played an important role in assessing the bank's fault (regarding the other relevant criteria, see Liégeois Fabien/Hirsch Célian, Ordres bancaires frauduleux : discours de la méthode, *in La* Semaine judiciaire II, Doctrine, 2021, no. 4, p. 135).