Claim for damages due to a payment initiated by unknown persons via e-banking

Topic: **Abuse and fraud** Case number: **2020/14**

> In the present case, a customer was harmed by means of a phishing attack. A husband wanted to log into the bank's e-banking system on a Sunday to check the balance of his wife's savings account. He was unable to log in. He then received an SMS containing the amount of CHF 3'000. The customer mistakenly assumed that this was the balance of the account. Early on Monday morning, he was able to log into e-banking without any problems and discovered an unauthorised transfer of CHF 3'000. He immediately contacted the bank and reported the incident. The bank, which held the account of the payee (the recipient bank), was contacted by SWIFT only at 4:30 p.m. and was demanded to return the payment. Unfortunately, it was not possible to secure the amount at the recipient bank. The customer subsequently made a claim for damages against his bank on behalf of his wife. When he could not reach an agreement, he contacted the Ombudsman. In the Ombudsman proceedings, the bank also refused to make concessions.

The bank used a 2-factor authentication with a so-called mTAN code for its e-banking system. This code is sent to customers to their pre-registered mobile phone after they have entered their login data. They then have to confirm their login by entering this code in e-banking. When the client's husband tried to do this on a Sunday, the screen went black after entering the mTAN and reported maintenance work on the bank's e-banking. He aborted the login attempt and tried to log in again, which once more failed. Due to the circumstances, it could be assumed that his computer was probably infected and that he had entered the login data on a so-called phishing website, which had been set up by fraudsters to obtain these data and probably looked deceptively similar to the bank's website. With the help of the fraudulently obtained data, unknown third parties logged in via e-banking and triggered a transfer from his wife's account to the account of a so-called "money mule" at a third bank. The recipient, according to the criminal proceedings initiated by the client, a student who had also been deceived about the true transactions, then forwarded the money to the fraudsters in exchange for compensation. The fraudsters could not be identified and the money remained missing.

The basic problem in these cases is that the damage cannot usually be obtained from the actual perpetrators. The question then arises as to whether the bank client or the bank must bear it in whole or in part. This is a question of the applicable contractual terms. According to the usual contractual provisions, a bank can and must execute a payment order that was entered into the e-banking system with the correct means of identification. With regard to liability for misuse, the contracts generally follow a risk sphere theory. This theory states that, in principle, each party is liable for errors that occur in the area that it can influence and that it could have prevented with due diligence. Based on the contractual provisions, the bank rejected liability in the case at hand, since in its view its systems had functioned perfectly and the client was solely responsible for the security of his terminal device, which in the case at hand had presumably been infected.

In the present case, however, the additional question arose as to whether the bank should not have reacted more quickly vis-à-vis the recipient bank so that the amount transferred by the fraudsters

could still have been seized. The bank was of the opinion that its reaction had been timely. However, the Ombudsman considered the bank's reaction, which only took place in the late afternoon after the fraud report had been received in the early morning, to be very late. Experience shows that one of the typical features of such fraud is that the perpetrators (or the money mules they instruct as assistants) withdraw the money as soon as it arrives, thus preventing it from being seized. A discussion about whether the reaction had been timely would have been superfluous if even an intervention at the beneficiary bank immediately after receipt of the fraud report had also been late because the money had already been disposed of. The Ombudsman therefore tried to find out from the beneficiary bank exactly when the money had been disposed of. The bank refused to provide detailed information on the grounds of banking secrecy, stating only that it dealt with such reports immediately. The Ombudsman was therefore unable to clarify this point with the desired precision, but pointed out to the client that the documents from the criminal investigation could probably help here.

According to the Ombudsman's experience, banks handle such claims differently and are sometimes more generous than the bank involved in the present case. In view of the bank's unwillingness to make concessions, he unfortunately had to conclude this mediation procedure with a final notice to the client without success.