Fraudulent payments made via e-banking

Topic: **Abuse and fraud** Case number: **2017/09**

> The client was the victim of fraudsters who managed to intercept his e-banking login details and make payments to a company holding an account with an English bank. The bank was only willing to compensate him for half of the amount transferred which the client found unsatisfactory. In mediation the bank categorically denied any obligation to provide compensation but agreed to pay 50% of the loss as a gesture of goodwill. The client ultimately accepted the bank's offer on the Ombudsman's advice.

The client received a phone call from someone claiming to be a software engineer working for his internet provider. The alleged engineer explained to him that he needed to remove malicious software that had infiltrated the system following a cyberattack. He claimed that this software was capable, in particular, of accessing the e-banking systems of certain banks. He then asked the client to send him his bank details, which the client did. The contact then asked him to only access the banking internet sites in question after entering a specific code. The client followed the instruction and the internet site disappeared briefly each time before reappearing on the screen. Finally, the alleged engineer told him that he and his colleagues were now able to remove the malicious software. The client then logged in to the e-banking system of his banks following the normal access procedures and did not notice anything out of the ordinary. A few days later, when he logged into the bank's e-banking system again, he noticed that a payment had been made, that he had not ordered, from his account to an English bank account held by a company he did not know. He informed the bank immediately who assured him they would take the necessary action. Ultimately, when the bank informed the recipient bank about the fraud, it emerged that the money had already been withdrawn from the account.

The client, who had initiated proceedings against X, believed the bank was obliged to refund the payment made without his instruction. He claimed that the other banks he had accounts with were also victims of the same type of fraud and that either they did not process the payments, or they managed, by contacting the recipient banks in good time, to obtain a refund of the payments made against his will such that he did not suffer any loss with these other banks. The client claimed that he logged into the e-banking system following the stipulated access procedure and that he is not responsible for the fact that, on this occasion, third parties were able to access his accounts. Furthermore, the bank should have recognised the unusual nature of the payment given that he had never made payments to third parties from this account. The client further maintained that the bank had waited too long after the incident was reported to contact the recipient bank, which allowed the fraudsters to dispose of the money. After all, the bank had initially confirmed to him by phone that it had been possible to stop the money with the recipient bank. For its part however, the bank denied any obligation to indemnify the client and only declared its willingness to refund 50% of the amount transferred by way of a gesture of goodwill. The client then contacted the Ombudsman so the latter could initiate mediation proceedings.

The bank explained to the Ombudsman in more detail the position it had already communicated to the client. It emphasized that the payment in question had been made after the required access details for the e-banking system had been entered and without any third parties having intervened in the bank's systems. It maintained that it was authorised to carry out such transactions under the

contractual agreements regarding the e-banking service. The bank also pointed out that the client has an obligation to keep the access details in a safe place and not to disclose them to third parties under any circumstances. Moreover, the bank is not under any contractual obligation to also examine the plausibility of every payment ordered via e-banking. In this case, it is clearly apparent from the client's statements that third parties intercepted his access details by contaminating his input device with malicious software, a wrongful act over which the bank had no control. The latter does not understand why the client did not get in contact after his telephone conversation with the alleged engineer to ask if there was in fact a problem with the access to its e-banking system. According to the bank, under the terms and contractual agreement entered into, the risks associated with the e-banking system over which it has no control are to be borne by the client. In addition, the bank was able to prove that it had notified the recipient bank about the incident promptly, on the same morning it became aware of it, requesting a refund for the amount transferred. Since the recipient bank unfortunately failed to respond, it was necessary to send a reminder. The client believed the reminder to be the first intervention and thus concluded, wrongly, that the bank had reacted too late. Finally, the bank's statement saying that it had been able to put a stop on the money in question concerned a second case disputed by the client for which it was actually possible to block the funds in time and return them to the client.

Upon the Ombudsman's intervention, the bank also denied any obligation to provide compensation but offered once again to refund 50% of the payment amount as a gesture of goodwill. Having carefully reviewed the arguments put forward by both sides, the Ombudsman advised the client to accept the bank's offer. From the description of the incident, it seemed plausible to him that the fraudsters had intervened in the client's systems and that such an act was completely beyond the bank's control. It had been contractually agreed upon that such risks were to be borne by the client as is usual practice within the industry. Furthermore, the description of the incident definitely raised doubts as to whether or not the client had been sufficiently careful during the described telephone call. The Ombudsman is also unaware of any court ruling obliging a bank to check the plausibility of any instructions processed automatically via e-banking. He is of the opinion that the case law concerning orders carried out fraudulently which arrive at the bank via different channels and are reviewed by employees does not necessarily apply to the scenario in this case. Moreover, and even in light of the above-mentioned case law, the fact that no instruction had ever been issued to pay any third party from the account in question in no way constitutes sufficient grounds to classify the instruction as unusual. Finally, the bank was able to demonstrate that as soon as it was informed about the fraud, it reported it to the recipient bank in good time. For all of these reasons, the Ombudsman considered the bank's offer to be appropriate. In the end, the client accepted the bank's proposal.