

The bank's conduct following a report of fraudulent payments

Topic: **Abuse and fraud** Case number: **2024/07**

The client had searched for the bank's e-banking entry page via Google and clicked on the link for the top search result. She then visited a fraudulently replicated website of the Bank and entered her e-banking access data. The fraudsters were able to use these data to trigger a payment of around CHF 5,000 from her account. The following day, she noticed this and reported the fraudulent incident to the bank. Five calendar days later, the sending bank contacted the recipient bank and asked it to return the amount. The client complained to the bank and explained that she did not have to confirm the payment on the app, which is standard practice for payments to unknown recipients. She also felt that the receiving bank had been informed of the fraud too late. The bank responded to the client that she had confirmed the payment on the app and explained that the callback had been made in a timely manner. In the Ombudsman proceedings, the bank confirmed its position, so the case had to be closed without mediation.

In the present case, the client was the victim of a widespread fraud pattern. With Google, it is possible to pay to have search results for certain terms appear at the top with corresponding links. This is apparently also exploited by fraudsters who ensure that their fake phishing websites, which are deceptively similar to the real websites of banks, appear at the top of the list when clients search for the e-banking entry page of their bank using a search engine. Google always marks such paid search results as "sponsored". If the client then clicks on the link in the top search result, he or she will be redirected to a fraudulent phishing website where he or she is asked to enter the login information. In the background, the fraudsters steal the client's access data and open the bank's real e-banking website. The police, financial institutions, consumer organisations and even the Ombudsman regularly warn about this fraudulent scheme. It is surprising that it still works apparently despite the findings.

Once the fraudsters have logged into the client's e-banking, they carry out the payment transactions that are possible with the stolen data. Often, the client must confirm a beneficiary to whom she has not yet sent any payments via e-banking using 2-factor authentication via an app or an SMS code sent to his mobile phone. According to the Ombudsman's experience, the corresponding security notices are often not read carefully enough by the clients. This therefore overrides an important and efficient security measure of the common e-banking systems.

In its response to the Ombudsman, the bank explained that it regularly warned its clients, among other things with references on its e-banking login page, about the known fraudulent methods, including the one that the client had fallen victim to. The client had in fact confirmed the disputed payment using the app. There was no indication that the confirmation process did not work. The bank was unable to recognise that the client had become the victim of fraud. According to the provisions on the bank's electronic services, it is the client's responsibility to ensure that she is on the correct e-banking page when entering the access data.

With the confirmation in the app, the payment instruction was irrevocable and could no longer be stopped. In such a case, the bank would offer the client the possibility of requesting a callback of the executed payment. According to the bank's internal guidelines, this was to be carried out within a

certain number of days. Only bank working days were relevant for the deadline. Since there was a weekend between the fraud report and the callback, the latter was made in a timely manner after five days.

In such a case, the recipient bank would have to obtain the account holder's consent to reverse the payment. The bank could not guarantee that such a callback would be successful and was not responsible for it either. In the present case, the recipient bank was also informed one day after the recall that the payment had a fraudulent background. After contacting the receiving bank twice, it reported about a month after the recall that the recipient had not given his consent to the reversal.

The bank took the view that the client was solely responsible for the loss. In the present case, the bank had taken all reasonable measures in a timely manner and therefore refused to accommodate the request.

The Ombudsman explained to the client that, according to the applicable contractual provisions, the responsibility for payments that had been confirmed by the client using 2-factor authentication via an app lay in principle with the client. Based on the explanations provided by the bank, which had documented them with copies of the log files, he had to assume that the payment instruction had indeed been confirmed via the client's app. Experience shows that the recipients of fraudulently obtained transfers usually withdraw or transfer the money immediately at the recipient bank, so that any recall requests to the recipient bank are very often unsuccessful if they are not made immediately after the transaction is triggered.

The Ombudsman understood the client's criticism that the bank had delayed the callback in her case. He considers it important in such cases that the recipient bank is informed as soon as possible about the fraudulent background to the payment. A simple callback, as is usually made in the case of payments that are misdirected due to incomplete information, is not sufficient since the recipients of a fraudulently triggered payment are unlikely to ever agree to a reversal. Whether faster action would have resulted in a successful blockage and refund of the payment in the present case, however, remained an open question. Since the bank categorically refused to accommodate the client's request, the case had to be closed without mediation.