Credit card fraud in connection with a transaction on an online sales platform

Topic: **Abuse and fraud** Case number: **2022/14**

> The client advertised a bed for sale on a well-known online sales platform. She was contacted by a supposedly interested party who pretended to transfer the money to her credit card account via a payment service of the post. She entered her credit card details on a fake postal website. Fraudsters then managed to use it to make two transactions totaling around CHF 900 to payment service providers. Although the fraud was discovered immediately, the charges could not be reversed. The credit card issuer refused to pay a share of the loss because the client had authorised the transactions with a code sent to her mobile phone as part of a so-called two-factor authentication. In the ombudsman proceedings, the credit card issuer agreed to pay half of the damages. The client agreed to this solution.

The Ombudsman was confronted with the present fraud scheme several times in the year under review. It is related to transactions on popular online platforms. The fraudsters get sellers to enter their credit card data on a fake Swiss Post website, which is supposedly used to securely transfer the purchase price to the seller's credit card account. They then use the fraudulently obtained data to make credit card transactions.

In this case, the client was accompanied by an alleged supporter in a chat during the entire process. After she had entered her credit card details on the fake website, the "supporter" told her that she would receive a code on her mobile phone so that the transfer of the purchase price for the advertised bed could be finalised. In fact, this was the code that the credit card issuer sent to the client's mobile phone via SMS to authorise the credit card charge, which the fraudsters made with the data received. The alleged supporter then pretended that the transfer of the purchase price had not worked and several times repeated the request to enter newly sent codes. In the background, the fraudsters tried to make more than one abusive credit card transaction.

The text messages with the confirmation codes showed that they were not credits but debits, which could have nothing to do with the alleged purchase price payment to the client due to the currency and the stated merchant. Although the client asked critical questions and refused several requests for disclosing the codes she had received, she was so influenced and pressured by the fraudsters that she sent them the codes for two transactions. In reality, she authorised credit card charges totaling around CHF 900 in favour of two international payment service providers. During the process, the client consulted her credit card app and immediately realised that she had fallen victim to fraud. She immediately contacted the credit card issuer, who blocked the card.

The credit card issuer refused to refund the misused payments, referring to the contractual conditions for the use of the card, as the client had confirmed the payments in the context of a so-called 2-factor authentication, i.e. by passing on the codes sent to her mobile phone. The client then took the case to the Ombudsman. She was distressed because, according to her, she was a single mother living in very modest circumstances and the loss was a great burden for her.

The Ombudsman contacted the credit card issuer and asked clarifying questions about the exact

procedure for the debits and the authentication procedure. He also asked for a more detailed explanation of the contractual basis on which the client was refused a refund. Finally, he asked the credit card issuer whether it had attempted to reclaim the amount from the beneficiary payment service providers so that they would have had the possibility to block the forwarding of the money, as is customary in payment transactions when fraud is reported, according to the Ombudsman's experience.

In its reply to the Ombudsman, the credit card issuer explained in detail the transaction process and the authentication procedure from its point of view and stated that the applicable card terms and conditions excluded the assumption of damages if card data and the code for confirming the transaction were disclosed to unauthorised third parties. In addition, the assumption of damages was generally excluded if transactions were confirmed by the client within the framework of 2-factor authentication, as in the present case. The card issuer also referred to the relevant warnings against phishing on its website and on the website of the online sales platform concerned.

Finally, she explained that, unlike a bank transfer, a card transaction that had been carried out with a 2-factor authentication could not, in principle, be subsequently reclaimed, even if the unlawfulness was established immediately afterwards. In rare cases, merchants would reverse the transaction if the delivery or service paid for with the card had not yet been provided. These conditions had not been met in this case. It remained open in the reply whether the credit card issuer had even attempted to contact the beneficiary payment service providers.

After a second contact by the Ombudsman and a discussion of the case, the credit card issuer finally agreed to reimburse the client 50% of the loss as a gesture of goodwill and without acknowledging any legal obligation. The Ombudsman explained the arguments presented to the client and recommended that she accept the offer, which he considered reasonable under the overall circumstances. The client accepted the offer.