Unauthorised debit of a prepaid card

Topic: **Abuse and fraud** Case number: **2021/09**

> At a railway counter, the customer bought a prepaid card from the issuer and loaded it with CHF 250. He then put it in a filing cabinet at home and did not use it for a long time. When he wanted to make a transaction with the card for the first time a few months later, he noticed that only just under CHF 30 of the amount he had paid in was left. The rest had been debited without his knowledge and consent. He complained to the card issuer. The card issuer replied that it could be assumed that the debit was fraudulent. However, since he had not complied with the complaint period of 30 days, it was no longer possible to reverse the charge within the credit card system. The card issuer therefore refused compensation. Within the framework of the ombudsman proceedings, it was possible to obtain full compensation for the customer.

In the year under review, the Ombudsman was presented with several similar cases, which were also reported in the consumer press. The customer stated that he had never disclosed his card data to anyone during the period in question and could not understand how someone could initiate a transaction without these data. He was of the opinion that he had fulfilled all his contractual duties of care. The card terms and conditions provided for this case that the issuer would compensate the customer for any damage resulting from misuse of the card.

The card issuer’s reply to the customer showed that it had to be assumed that the card had been used fraudulently by third parties. The third parties had probably played through a large number of card data with the help of a computer. The transaction desired by the fraudsters was then virtually stuck on the customer’s card. The card issuer invoked the fact that the customer had not complied with the complaint period from the transaction date and pointed out that the charges could be monitored with a free app and the card or certain functions could be deactivated when not in use. He therefore refused to compensate the customer.

The Ombudsman had to address the card issuer in clear terms in these cases. In his view, the question arose as to whether the damage could have been prevented if the customer had behaved in accordance with the issuer’s ideas. Invoking duties of care whose non-compliance in a specific case has no influence on the occurrence of the damage seems formalistic and unjustified. He therefore asked the publisher whether, in his opinion, it would have been possible to reverse the charge at all within the framework of a chargeback procedure if the customer had reported in time.

Irrespective of this, the Ombudsman found it unrealistic to expect a customer to check for any transactions on a prepaid card that he had never used and that was in his safekeeping. The customer does not have to expect transactions in such a situation. In the Ombudsman’s view, he may rely on the systems of this card product, which is advertised as a secure means of travel payment, to reliably prevent a charge for such transactions. He therefore found the argument that the customer had breached a duty to check and complain questionable. According to the Ombudsman’s understanding, an obligation to check and complain only exists in relation to an order execution reported by the financial institution. If the client does not place an order and does not receive a transaction overview from the financial institution, in his view there cannot be a duty to check that triggers a deadline. The obligation to check on an app whether transactions have been recorded despite not using the card

would therefore have to be at least explicitly contractually agreed, which was not the case here.

Furthermore, according to the Ombudsman’s understanding, fraud possibilities caused by system technology cannot in principle be blamed on the customer. These fall within the risk sphere of the card issuer, as the corresponding risks cannot be influenced or controlled by the customer. Since the customer had never passed on his card data, their use, which was apparently attributable to a computer-generated coincidence, could not in principle be attributed to him.

For these reasons, the Ombudsman considered the passing on of the damage to the customer to be unjustified. In its statement, the card issuer pointed out once again that the customer had missed the deadline for making a complaint and that there was therefore no longer any possibility of a chargeback via the credit card organisation’s network, as the latter was also bound by deadlines. Only in this procedure could it be reliably determined whether the transactions were fraudulent. This was not already the case because the transactions were unusual for the customer. The card issuer nevertheless compensated the customer in full and described this as a goodwill solution to maintain the good customer relationship.

The Ombudsman consequently closed the case. The card issuer then refused to pay the handling fee for the case, which was charged at a minimal level. It was eventually persuaded that it owed the fee because of its participation in the ombudsman scheme.

Recently, the Ombudsman found that the issuer had changed the card terms and conditions. Customers are now obliged to check their card account regularly, but at least every 30 days, on the card issuer’s app or website. If they fail to do so, this constitutes a breach of due diligence according to the card issuer and compensation is not payable. The Ombudsman has not yet received any cases in which the issuer has invoked this clause. However, it does not address all the concerns that the Ombudsman raised in relation to this case.