Unauthorised transactions with a prepaid card

Topic: **Abuse and fraud** Case number: **2020/09**

> The customer was travelling and wanted to withdraw cash from an ATM with his prepaid card in a faraway country. He inserted the card into the machine and also entered his PIN. The withdrawal did not work and the machine retained the card. He immediately tried to contact the card issuer, which unfortunately he did not succeed in doing. He later discovered that his card had been charged for unauthorised transactions. The customer asked the card issuer to cancel the charges, as they did not originate from him and he had fulfilled his duty of care in handling the card. The card issuer refused, as the charges had been made with the original card and the correct PIN code. The customer then brought the case to the Ombudsman. After several interventions, the Ombudsman was able to persuade the card issuer to cancel the charges.

Apparently, the customer had got hold of a manipulated ATM. The perpetrators probably used the ATM to obtain the customer's original card and the PIN code. This allowed them to use the prepaid card to make transactions worth around 2'000 Swiss francs until it was blocked. When the customer realised that the withdrawal did not work and the machine had confiscated his card, he remained at the machine and phoned the card issuer on the number it had given him for the card to be blocked. He was, however, unable to reach the card issuer as this number is not serviced from 10 p.m. to 8 a.m. Swiss time. He then went to his hotel and informed the bank about the incident by e-mail. Later, he checked his card account online and realised that unauthorised withdrawals had taken place.

He wrote several more emails to the card issuer. A few days later, the card issuer reacted for the first time and inquired by e-mail about an address for the delivery of a replacement card. About 20 days after the incident, the card issuer informed the customer by email that it was not liable to pay compensation for the unauthorised withdrawals. It argued that a duty to pay compensation only existed if a customer had complied with all duties of care in handling the card. The disputed withdrawals had been made with the original card and the correct PIN code. The PIN code was already correct the first time it was entered. By disclosing the card and the PIN code to unknown third parties, the customer had breached his contractual duty of care, as laid down in the card conditions. It was up to him to take action against the operator of the ATM if he suspected a criminal offence. After the card issuer had confirmed this position in a letter following a further complaint from the customer, the customer submitted the case to the Ombudsman.

The Ombudsman contacted the card issuer and asked it to reconsider its position on the breach of due diligence. Inserting the card and entering the PIN are indispensable for withdrawing money from an ATM. The fact that an ATM is manipulated and that criminals thereby gain access to his card and the PIN is not usually apparent to a customer. In the Ombudsman's view, a customer may also expect that a hotline for blocking a card is continuously in service.

The card issuer maintained that the customer had breached his duty of care by making the card and the PIN code available to unknown third parties. It argued in addition that the client had failed to report the matter to the police, which would also have been part of his duty of care. Since the transactions were carried out with the original card and the corresponding PIN code, they did not qualify as fraud in the system of the credit card network and, according to the credit card issuer, did

not correspond to a known pattern of fraud. The credit card issuer was therefore not liable to reimburse the customer under any legal title. It also stated that it could not check whether the ATM had been manipulated in any way. However, the customer was free to file a complaint with the police against the operator of the ATM.

The credit card issuer finally confirmed that its hotline would only accept orders for card blocking between 8 a.m. and 10 p.m. Outside these hours, a customer could block the card via their app. The customer's blocking order was received by e-mail at 11:51 p.m. At that time, it was no longer possible to prevent the disputed withdrawals. The card issuer's reply left open when exactly these withdrawals had taken place and whether a blocking order via app would still have been processed after 10 p.m. It also remained open whether the customer's blocking request by e-mail was processed immediately after it arrived.

The Ombudsman then exchanged two more letters with the credit card issuer, as he found its statement largely incomprehensible. As he understood it, it would have been the card issuer's task to investigate the customer's allegation that the ATM had been manipulated within the card network. In addition, the insufficient availability of the card issuer seemed to him to have contributed significantly to the fact that the card could have been misused. The card was a typical means of travel payment used in different time zones all over the world. At the time of his attempts to contact the card issuer by telephone, the customer was only expecting a malfunction of the ATM and was not aware that he had been the victim of a crime. The country where the customer was located is known more for high corruption than for the good functioning of its authorities. A report to the police could at most have prevented further people from becoming victims of the manipulation, if it had been followed up at all. However, it would most likely have been too late to prevent the actual card misuse. In summary, the Ombudsman was of the opinion that there had been no breach of the customer's duty of care and that the card issuer therefore had to pay for the damage.

The card issuer maintained its position in its last letter, but eventually credited the customer in full for the amount of the unlawful withdrawals due to the good business relationship.