Fraudulent registration of a credit card on an electronic wallet (digital wallet such as Apple Pay or Samsung Pay)

Topic: **Abuse and fraud** Case number: **2020/11**

> Within a very short period of time, transactions amounting to more than CHF 21’000 were charged to the client’s credit card, exceeding the limit of his credit card by CHF 2’000. The charges originated from a Scandinavian country in which the client was not staying at the time. When he complained to the credit card issuer about this, it told him that he had given his credit card details to unknown third parties, who had deposited his credit card on a digital wallet and used it to make the transactions. The credit card company was only prepared to compensate the customer for 75% of the damage caused by the misuse of his card. The customer was not satisfied with this and submitted the case to the Ombudsman. In the ombudsman proceedings, the bank increased the share of the loss to 85%, which the customer finally accepted somewhat reluctantly.

The customer told the Ombudsman that he was always very careful with his credit card, which he used mainly for online transactions. All of his electronic devices were protected with the latest anti-malware software. He had never disclosed the credit card details to any third party and could not explain how the disputed charges had come about. He claimed that these were highly unusual for him and should have come to the attention of the credit card issuer, especially since his credit limit had been considerably exceeded. He had increased the credit limit to CHF 19’000 in connection with a trip to the USA and unfortunately forgot to reduce it again afterwards. After the incident, however, he had reduced it again to CHF 2’000.

In its statement to the Ombudsman, the credit card issuer wrote that it had no doubt that the objected transactions had been carried out by an unauthorised third party. However, the use of card data on a digital wallet was equivalent to using the card with the PIN. Unauthorised third parties could only use the card with a digital wallet if they were in possession of the necessary card data. This card data was initially only ever in the possession of the cardholder. If a third party could get hold of the data, including the release code of the 2-factor authentication, this was therefore due to a breach of the cardholder’s duty of care. How this happened in the individual case was not decisive, as there was no other way by which the data could get to a third party except via the cardholder. Since the card could only be registered for use with a digital wallet with 2-factor authentication, the card issuer assumed that the transactions made with it were initiated by the cardholder or with his approval. Therefore, such transactions were not monitored according to the same rules as transactions without a 2-factor authentication.

Unfortunately, it happens regularly that customers are misled by fake e-mails or text messages into clicking on links and disclosing their credit card data. In the case of the client, it must therefore have been the case that he had disclosed all the data necessary for registering his card in the digital wallet. This was the card number, the expiry date and the Card Validation Code (CVC), as well as the mTAN to enable the registration of the card on the digital wallet.

The CVC was only noted on the back of the card and was not generally accessible. The card issuer therefore had to assume that the customer had passed on this information to third parties, possibly in the belief that he was paying for an intended service or taking part in a competition. In addition, the

unauthorised third parties must either have had access to his mobile phone or have received the code from him. The code was only accessible on the customer's previously registered mobile phone.

The credit card issuer's systems showed that both the SMS with the activation code and the confirmation SMS had been sent to the telephone number provided by the customer. When someone in possession of the necessary data initiated the request to register the card as a means of payment in a digital wallet on a smartphone, the credit card issuer immediately sent the activation code, whereupon the card was successfully activated on the digital wallet. The confirmation of this process was also sent by SMS to the telephone number provided by the customer. From the standard text of the SMS ("Please enter the activation code XXX to activate your credit card with the last digit XXXX for [Apple Pay / Samsung Pay]" and "You have successfully activated your credit card with the last digit XXXX for [Apple Pay / Samsung Pay]"), it was clear that the purpose was to activate the card in a payment app. The fraudulent card transactions, which took place a few days later, could have been prevented if the customer had reacted to these text messages in time.

Transactions with digital wallets were considered contactless transactions, as provided for in the card terms and conditions as a possible use of the card. The fact that the customer had disclosed his card data and had either confirmed the activation code himself or made it accessible to third parties showed that he had breached his duty of care. The assumption of the damage was therefore rightly refused.

Finally, the credit card issuer mentioned that limits could be exceeded under certain circumstances due to currency exchange and the use of the card abroad. Moreover, the limits were handled with a certain degree of flexibility for long-term customers. Due to the long-standing customer relationship, the credit card issuer was prepared to increase its compensation offer to 85% of the damage suffered by the customer without prejudice and without acknowledging any legal obligation.

The Ombudsman submitted the bank's adjusted offer to the client. He made the following comments on it: Transactions with a credit card are generally – this is regularly stated in the relevant contracts – attributable to the customer if they have been initiated with the agreed means of legitimation. The credit card institutions are only prepared to assume damage from misuse of the card if the transactions were initiated by unauthorised third parties without the customer having made this possible through a breach of his duties of care.

How it came about in the customer's case that the fraudsters obtained all the necessary data to register his card in a digital wallet had to remain open in the ombudsman proceedings. The credit card issuer stated that this had only been possible through the customer's involvement, in that he had been induced to release the data, probably under false pretences. The customer claimed that this had not been the case. As a neutral mediator, the ombudsman is not in a position to question the credibility of the parties. In the ombudsman procedure, no formal evidentiary proceedings are conducted in which a differently presented factual situation could be bindingly clarified according to fixed rules. Rather, the purpose of the procedure is to reach mutually agreeable solutions to disputes through mediation between the parties, whereby the Ombudsman can propose solutions on the basis of the information submitted to him by the parties. However, he does not have the authority to make binding decisions on disputed questions of fact or law. This is reserved for the ordinary courts.

As it was not possible to clarify the matter further within the framework of the ombudsman procedure and the credit card issuer had stated that it was not prepared to make any further concessions, the ombudsman recommended that the customer accept the offer made by the issuer. In the Ombudsman's view, it would have been desirable if the process of registering a card on a digital wallet had been regulated more clearly in the contract, so that a customer could at least receive a basic explanation of the product and how it works and could, for example, reject it in general. The

Ombudsman also questioned whether the contractual basis invoked by the card issuer was sufficient. This seemed to be tailored to a single transaction with a contactless function rather than to a registration of the card in a digital wallet. However, the credit card issuer was of the opinion that it was sufficiently clear on the SMS in the context of 2-factor authentication that the customer, by releasing the code, was agreeing to the registration of a card on such an electronic wallet. Due to the process, the detailed contractual provisions for the digital wallet were only visible to the fraudsters on the terminal device on which the registration of the card was carried out. This did not seem optimal to the Ombudsman.

After weighing up the advantages and disadvantages of the settlement solution, the customer decided to accept it. However, he expressed
his displeasure at the behaviour of the credit card issuer in dealing with his complaint.