

Fraudulent transfer instructions

Topic: **Abuse and fraud** Case number: **2018/22**

The customer, represented by a lawyer, complained about two transfer instructions which had brought about the closure of his account with a credit balance of approximately 100,000 CHF. He claimed that the transfer instructions were clearly fraudulent which the bank should have noticed. He therefore demanded the reinstatement of his account balance. The bank believed that it had complied with its due diligence obligations when checking the transfer instructions. Since the parties were unable to reach an agreement, the customer referred the matter to the Ombudsman. It was also impossible to reach any agreement during mediation proceedings as well however, whereupon the customer initiated court action.

The customer, residing in South Africa, had held an account with the bank for several years. On the basis of a transfer instruction, a large part of his account balance was transferred to an account with a bank in Asia allegedly held in the customer's name. A few days later, his account was closed and the remaining balance was transferred to the same account in Asia. According to the customer, both of the transfer instructions were fraudulent. His enquiries with the bank revealed that an unknown perpetrator had apparently managed to initially give the bank a new telephone number. The perpetrator had phoned the bank first to request a fax number and had then sent the new telephone number by fax. The first payment instruction had been made in writing at the bank's request. The accompanying identity card copy had been certified by a Notary Public. The bank accepted the instruction to close the account a few days later verbally. The bank used the new telephone number that the perpetrator had previously sent to it by fax to verify the instructions. Once the customer discovered the fraud, he filed a criminal complaint and asked the bank to reinstate the account balance since he felt that it had breached its due diligence obligations when checking the payment instructions. In his view, the instructions contained several discrepancies which the bank should have noticed.

The bank responded to the customer's arguments in detail and expressed the view that there was no breach of the due diligence obligations on its part. It refused the customer's request to reinstate the account balance. The Ombudsman, having had the matter referred to him by the customer, asked the bank to reconsider its position. He felt that the request by telephone for a fax number for sending a new telephone number ought to have been questioned since the customer had previously sent messages by fax and therefore knew the bank's fax number. Furthermore, particular caution should be exercised when new contact details are provided and a control call to the previous number is also advisable. This was the case not least because of the customer's place of residence. In the Ombudsman's experience, South Africa is a country that is known among banks to be a high-risk area for crime involving cards and payment transactions. In particular, perpetrators there manage to intercept mail and gain access to bank details that way. During the phone call looking to close the account, the customer had to be given the bank's address which, given the fact that the customer must have already known this, should once again have warranted the utmost caution.

Moreover, the Ombudsman felt that the written payment instruction also contained a number of elements that would also have called for careful examination. It included the transfer of a relatively

large sum, one that covered almost the entire account balance, to a country that was unusual for the customer with which there was no discernible relationship. Unlike on the customer's other correspondence, the name of the bank was written incorrectly on the fraudulent payment instruction. The font, layout and, to some extent, the style also differed from previous instructions. The instruction was also stated to be extremely urgent. The reason given was that the money was needed in the Asian country for personal reasons. The customer also maintained that the signature was clearly different to the sample signature that the bank held on file. The telephone number that had been specified on the certificate confirming the authenticity of the identity document copy was not that of the law firm that allegedly drafted the certificate. Finally, this certificate was issued in South Africa on the same day as the instruction when the customer allegedly needed the funds in Asia urgently for personal reasons. The bank's callback to check the instruction was apparently made to the new telephone number recently provided by the suspected fraudster.

Payment transactions are a bulk business. A bank cannot be expected to check every instruction with forensic precision, to do so would render any kind of reasonable service impossible. The Ombudsman felt however that in this case there were some elements that, given the relevant jurisprudence from the Federal Supreme Court (including decision 4A_386/2016 of 5 December 2016), raised the question of whether the bank had fulfilled the due diligence obligations incumbent upon it when checking the payment instruction. He therefore suggested that the bank accommodate the customer's request in full.

The bank maintained that it had exercised due diligence when checking the transfer instructions. The instruction had been initiated following the pattern that was known for this customer. The customer had also previously told the bank that he would be in Asia. In the absence of any suspicious factors, further checks were not appropriate. The bank further claimed that apart from the customer's statement, there were no substantiated arguments showing that a fraud had occurred. If payment had indeed been made to an unknown party, which the bank disputed, the bank had validly passed the corresponding risk onto the customer within its General Terms and Conditions. The execution of the transfer and closure instructions and the corresponding communications and statements are thus to be deemed approved in the absence of a complaint within the specified period from the customer. If he did not receive monthly account statements thereafter, he would have been obliged to complain to the bank about this. The bank further claimed that the Federal Supreme Court decision cited by the Ombudsman could not be applied to this dispute because in that decision, unknown perpetrators had manipulated the customer's mailbox and were therefore able to send and intercept emails. Finally, the fact that, according to the customer's statement, unknown parties had managed to gain access to his banking documents, suggests a breach by the customer of his own due diligence obligations.

During attempts to settle the dispute amicably, the bank was willing, without prejudice and without acknowledging any legal obligation, to compensate the customer for approximately 20% of the loss suffered. The Ombudsman presented the bank's settlement proposal to the customer but indicated that he had hoped for more of a gesture of goodwill given the overall circumstances of the case. No settlement was reached on the basis of the bank's proposal. The Ombudsman closed the case when he learned that the customer had initiated court action for his claim.