Case study: Banking

AUTHORISED PUSH PAYMENT (APP) TRANSFER TO FRAUDSTERS

Themes: authorised push payment (APP) fraud; fraudulently 'cloned' firm; bank failure to challenge customer-authorised payments; 'balance of probabilities' test re anticipated customer response to hypothetical bank challenge of customer's payment instructions; customer's contributory failure.

This complaint related to an authorised push payment (APP) fraud and the bank's refusal to refund the customer's losses arising from the fraud.

In mid-2019 Mr G was approached by a "well-known investment firm" that recommended an investment opportunity. Over a period of time, Mr G made five payments from his Jersey-based bank account at a UK branch of his bank totalling £1,004,580. The payments were to invest in what he believed to be the investment firm's recommended investments, but which later turned out to be an account operated by a fraudulently 'cloned' version of the real investment firm.

Mr G later suspected he had been a victim of fraud and contacted his bank, but it was too late to retrieve any of the transferred funds. Mr G asked his bank to reimburse the payments made to the fraudsters, but the bank declined to do so. Mr G then brought his complaint to CIFO. Informed of CIFO's £150,000 limit on compensation for losses, the complainant indicated that he had no other prospect to recover the lost funds and asked that CIFO proceed with a review of his complaint acknowledging the limit on redress available through CIFO.

Mr G felt that the bank should have provided a warning regarding fraudulently 'cloned' firms and asked him to check that he was dealing with the genuine investment firm when initiating the large payments while at the bank branch. Mr G believed that at no time did the bank question the payments or the recipients of those payments and felt that the bank was subject to a "Secure Banking Promise" and the UK's "Authorised Push Payment (APP) Scam Voluntary Code".

The bank stated that they are required to check that payment instructions are authorised by genuine customers, and they are obligated to make those payments as instructed. The bank also mentioned that its "Secure Banking Promise" was not relevant to this circumstance because it relates to online or mobile banking account fraud, not customer-authorised payments made to fraudsters. Finally, the bank said that the UK's "Authorised Push Payment (APP) Scam Voluntary Code" was not relevant as the complaint was about payments made to a fraudster from a Jersey account. Jersey is not part of the UK and establishes its own laws and regulatory requirements.

CIFO investigated and noted the bank's policies and processes to protect both themselves and their customers from fraud, including having an awareness of fraud indicators and – where appropriate – bringing these to the attention of their customers. The bank did ask about why some of the

payments (starting with the second) were not going to an account in the 'investment company's' name. Mr G reassured the bank that they were the correct beneficiary details by referring to the payment instructions he had received from the fraudsters. However, Mr G felt the bank should have gone further given its awareness of such frauds. CIFO concluded that, even if the bank had raised specific concerns, on the balance of probabilities Mr G would still have asked the bank to proceed with the transfers because he was firmly convinced that he was dealing with the genuine investment firm. CIFO did not uphold the complaint.

While it was not the basis for the decision in this case, CIFO also felt that Mr G could have undertaken further due diligence checks before sending the substantial fund payments which may have highlighted the possibility that he was dealing with a fraudulently cloned firm.