Case study: Banking

FOREX AND CRYPTO CURRENCY SCAMMERS DUPE COMPLAINANT INTO FRAUDULENT INVESTMENT

Themes: Forex; crypto currency; cloned website; fraud; terms and conditions.

This complaint relates to a bank's failure to protect the complainant from being targeted and transferring money to a forex and crypto currency scam.

In March 2022, Mr M made several online payments totalling approximately £44,000 from his bank account to a legitimate website offering crypto currency trading. Mr M then transferred funds from this trading website to another trading platform, which unfortunately turned out to be a clone of a genuine trading platform. Mr M had taken advice to invest using the fraudulently cloned trading platform from an individual that had befriended him on a social media website. Mr M had initially made inquiries into the investment, which looked credible, and had believed his new social media friend was a forex trader specialising in crypto currency.

In July 2023, when the fraud came to light Mr M made a complaint to his bank on the basis that the payments he had made to the legitimate crypto currency website were inconsistent with his usual bank activity and that during the six calls that the fraud team made, the bank should have done more to identify that Mr M was being subjected to a scam. Mr M's bank responded by advising that specific scam questioning and warnings about crypto currency had been discussed with Mr M but, as he had proceeded to make the payments, they could not provide reimbursement. Mr M referred his complaint to CIFO.

CIFO investigated and noted that Mr M's bank's fraud team had contacted Mr M six times prior to releasing his payments to the same legitimate crypto currency website, because of the higher risk of fraud involved with the payments. During this contact Mr M had been repeatedly warned about fraudulent crypto currency investments. Mr M's bank had also asked if there was an investment adviser or broker involved, but Mr M declined to tell the bank about his social media friend who had encouraged him to transfer his money from the legitimate crypto currency website to the fraudulent trading platform. CIFO also noted that as the payments were instructed and positively clarified by Mr M, the bank had a duty to fulfil those instructions in accordance with their terms and conditions.

CIFO concluded that Mr M's bank had identified that the payments were out of character and had a higher risk of being a scam or a fraud and had contacted Mr M prior to the release of the payments. However, as Mr M had not provided truthful information regarding the transactions, it was almost impossible for the bank to identify these as fraudulent and stop Mr M from continuing with payments which were subsequently transferred to the fraudulent trading platform. CIFO did not uphold the complaint.