



Case study: Banking

COMPLAINANT SCAMMED BY FRAUDSTER CLAIMING TO BE FROM CRYPTOCURRENCY INVESTMENT

Themes: Fraud alerts; contributory conduct of customer; cryptocurrency; phishing.

This complaint relates to a bank's failure to recall funds when a complainant discovered fraudulent activity over their bank account.

Mr D met an individual through social media, and they became friends. In September 2021, Mr D's friend suggested he invest in cryptocurrency using an app. Mr D researched the investment company and, feeling comfortable, invested approximately £750 directly using his online banking facility; not through the app but Mr D was able to view his investment using the app. In February 2022, Mr D's friend encouraged him to invest more money in the company, and Mr D made another payment for approximately £7,500, again directly using different payment details. Mr D's bank contacted him about this second payment, but Mr D stated that the payment was for a legitimate cryptocurrency investment. The bank did highlight the fraud potential of these types of investment, but Mr D's bank accepted Mr D's payment instruction.

In April 2022, Mr D made another online payment of approximately £9,500, again using different payment details. In June 2022, when Mr D asked to withdraw some of the invested funds, the investment company confirmed that there had been a downfall in the market and that Mr D had lost everything. Mr D checked the app, and his investment now showed a nil balance. Believing he had been a victim of fraud; Mr D immediately contacted his bank to attempt to retrieve his funds. The bank requested a recall of the payments totalling approximately £17,750 but were only able to retrieve the second payment, leaving approximately £10,250 outstanding.

In August 2022, Mr D made a complaint as he believed the bank should have acted quicker to retrieve the funds once he had reported the scam. Mr D's bank rejected his complaint on the basis that they had contacted him and specifically advised him of the dangers of investing in cryptocurrency, but Mr D had chosen to continue and authorised the payment. The bank also advised Mr D that he had failed to complete adequate checks to ensure the beneficiaries of the investment were legitimate before making a payment. Mr D referred his complaint to CIFO.

CIFO investigated and noted that Mr D's bank had stopped the second payment and followed their suspected fraud process, but Mr D had continued with his payment request. CIFO also noted that the funds from this second transfer had been successfully recalled by the bank. CIFO concluded that the bank had provided sufficient fraud warnings, acted on the payment instructions requested by Mr D, and had attempted to recall the fraudulent payments the same day they had been made aware of the fraud. Therefore, CIFO did not uphold the complaint concluding it would not be fair and reasonable to expect Mr D's bank to reimburse him for the unrecovered funds.