Case study: Banking

FRAUDSTERS USE AN EMAIL INTERCEPT TO TRICK COMPLAINANTS INTO SENDING MONEY

Themes: Email intercept; fraud alerts; authorised push payment (APP) fraud.

This complaint relates to a bank's failure to identify that the complainants had made a payment to a fraudster.

In October 2017 Mr & Mrs D made a payment to their builder who had completed some building work for them. The following day, the complainants received an email from their builder's email account advising that a further payment of approximately £2,000 was required and asked them to make the payment to a new bank account. Mr & Mrs D made the payment the following day which was a Saturday. Later that day the complainants' builder contacted them to say his email account had been compromised and his customers were receiving fake payment requests. Mr & Mrs D immediately contacted their bank to retrieve the payment they had made. The second payment had been made to fraudsters. The bank advised that they were unable to retrieve the funds and, as the complainants had made the payment themselves, the bank would not assist any further.

In September 2023 the complainants referred their complaint to CIFO. Unfortunately, CIFO only had limited information within the complaint file due to the time that had elapsed between the event and the submission of Mr & Mrs D's complaint to CIFO. Mr & Mrs D complained that the bank should have known that the payee details from the earlier payment had been changed and that this should have alerted the bank to the fraud.

CIFO investigated and noted that there was nothing in the payment request to lead the bank to believe the transaction was suspicious. In 2017 banks were aware of this type of fraud. However, CIFO did not agree that the bank should reasonably be expected to have identified this transaction as unusual. CIFO also noted that the bank had taken reasonable steps to try to reclaim the funds when they were alerted to the fraud. CIFO did not uphold the complaint.