Case study: Banking

FAILURE TO IDENTIFY A FRAUD INVOLVING AN AUTHORISED PUSH PAYMENT (APP) INSTRUCTION

Themes: inadequate systems and procedures; authorised push payment fraud; bank reluctance to compensate.

This complaint relates to an authorised push payment (APP) fraud and the reluctance of the bank to compensate a customer's losses due to the fraud.

Miss R asked her bank to make a payment from her account to an investment company and she sent the relevant recipient account information by email. Not long after, Miss R sent an updated request to her bank by email saying the recipient account information had changed. She provided the amended details she believed had been sent, by email, by the investment company. Because the transfer amount was a large sum, the bank required the transfer to be authorised in person at their branch, which Miss R complied with and the bank then made the payment.

After a week, the bank received a distraught email from Miss R saying the payment had not been received. The investment company provided some insight as to why, confirming they had not amended any recipient account information and they believed Miss R's email account had been hacked, ultimately causing the fraud by enabling the fraudsters to send Miss R new "fake" payee account information. The bank immediately completed an "authorised push payment scam notification form" and sent this to the receiving bank, but they were unable to retrieve the full amount of funds Miss R had transferred as most of the funds had already been withdrawn from the recipient account. Miss R complained to her bank as she believed they should have alerted her to the risk that payment details received by email could be fraudulently intercepted and changed. Her bank rejected the complaint, believing that Miss R should have been more conscientious and alert when receiving payment instructions supposedly from the investment company.

Miss R then brought her complaint to CIFO. CIFO investigated and found that her bank should have recognised the underlying 'email intercept' fraud risk and warned Miss R. Had the bank provided a warning about the risk of relying on payment instructions received by email, or noted the change in payment details that Miss R had provided, the fraud would likely have been identified and the loss could have been prevented. CIFO recommended that the bank reimburse Miss R the funds they were not able to recover, plus cover the interest she would have earned on the lost funds in the interim. The bank was reluctant to accept CIFO's initial recommendation and requested that the issue be raised with the regulator as they believed that this type of 'authorised push payment' fraud was not prevalent locally at that time, therefore staff training did not address this risk. They also felt that Miss R should have been more vigilant and that, if she had noticed sooner that the money had not been received by the investment company, they may have been able to retrieve the full amount

of the funds transferred. However, CIFO noted that in most circumstances, the funds are withdrawn almost immediately once received into the fraudster's account.

CIFO investigated further and found that the bank had insufficient systems and procedures in place to protect both themselves and their customers from this type of fraud, which was a known risk at the time. Based on this, CIFO's final decision was for the bank to reimburse Miss R for the lost funds of £150,000 (CIFO's statutory limit for a binding decision). CIFO made a non-binding recommendation for the bank to pay the remaining amount of the lost funds of £14,113 as well, plus interest on the total amount. The bank agreed to pay the recommended amount in addition to the statutory limit. Miss R received the £164,113, plus £27,121.50 in interest, totalling £191,232.50 in total compensation.