Case study: Banking

BANK'S REFUSAL TO REIMBURSE FRAUD LOSS LEADS TO COMPLAINT

Themes: fraud; business account; contributory error; fraudster remote access to complainant's bank account.

This complaint relates to a bank's failure to reimburse fraudulent payments that were made from a complainant's personal and business accounts.

In May 2023 Mr P received a text message that appeared to be from his bank advising of a potential fraud on his account and that he would receive a call from their fraud team. Mr P received the call and was advised to log on to his bank account using a specific web address and download an app which would allow the caller to monitor Mr P's account. That same day, Mr P received another call from who he believed was his bank's fraud team and was advised to allow the caller remote access to his computer, he initially questioned this but eventually allowed the caller access. Later that evening, Mr P became suspicious and contacted his bank. After numerous communications Mr P finally was able to speak with the bank. It became clear that Mr P had been a victim of fraud. Three payments had been made from Mr P's personal and business accounts, totalling approximately £45,000. The bank had managed to intercept and refund further payments totalling approximately £37,000 but was unable to recover the initial payments and advised Mr P to complete a fraud claim.

In July 2023, Mr P had not received an update to his fraud claim and made a complaint to the bank. Mr P believed that the bank had caused a delay in realising the fraud when he was unable to get in contact with them and that the bank should have alerted Mr P to the potential of fraud. Mr P's bank rejected Mr P's complaint, and he referred it to CIFO.

CIFO investigated and initially recommended the bank reimburse Mr P the full amount of the fraudulent transactions that they had been unable to reclaim. Mr P's bank did not accept this decision stating that Mr P had not acted in accordance with the terms and conditions of the account, specifically when he disclosed account information. Multi-factor authentication had been used to authorise the transactions. Mr P had given a one-time pass code to the fraudsters and Mr P had also given the fraudsters direct access to his computer. Mr P's bank emphasised that it was due to Mr P's negligence in allowing access to his device and sharing the one-time passcode that had enabled the fraud.

CIFO noted that although a bank is expected to act in accordance with a customer's instructions, the payment instructions had not technically been made by Mr P but rather by the fraudsters using Mr P's device. CIFO also noted that, despite the view that Mr P's actions in providing access to his bank accounts were unwise, Mr P's bank could not provide evidence of gross negligence or fraud on his part and were therefore liable for the losses. CIFO upheld the complaint and recommended Mr P's bank reimburse Mr P the full loss amount plus interest of 8% to be paid from the date the fraudulent activity had taken place to the date the compensation was paid.