Case study: Banking

VISHING ATTACK ON COMPLAINANT LEADS TO LOSS OF FUNDS

Themes: Authorised push payment fraud; vishing; safe account

A customer lost their funds after authorising online payments to a fraudster who was inciting fear by pretending that the customer's bank accounts were under threat from criminals.

In January 2021, Mrs Y received a 'vishing' phone call from a fraudster claiming that her funds were in jeopardy from criminals who had accessed her joint accounts. The fraudster told Mrs Y to make various payments throughout the day to move, and thereby safeguard her money. The fraudster instructed Mrs Y not to contact anyone or use her mobile phone during the interaction, which lasted most of the day. Mrs Y, who was in a state of shock and fear, was first instructed by the fraudster to make a payment of £20,000 to a bank account in the UK which Mrs Y's bank intercepted. Mrs Y's bank contacted Mrs Y as they believed it to be fraudulent, but Mrs Y was told by the fraudster to tell the bank that the payment was genuine. Having received her assurance, the bank then proceeded with the transaction as instructed.

The fraudster continued to terrorise Mrs Y on the phone by warning her that the criminals were still in her joint accounts. The fraudster then instructed Mrs Y to make another online payment of £25,000 to a different UK bank account, and that transaction went through. Later that afternoon, Mrs Y was again instructed by the fraudster to authorise two more transactions, each for £25,000. Both payments were intercepted by the bank and neither went through.

When Mrs Y's husband was alerted later that day, he tried to contact the bank but could not get a response. When Mr Y finally reached the bank, they assured him that the first transaction of £20,000 was still being held for fraud checks. However, the bank had in fact already completed this transaction, along with the second transaction of £25,000 - meaning that £45,000 had been transferred to the fraudsters. The bank was able to recover approximately £17,000 of that amount, leaving Mr & Mrs Y with a loss of approximately £28,000. Mr & Mrs Y complained to the bank asking to be reimbursed, but the bank declined to do so. The bank did however agree that they had provided incorrect information to Mr Y on the phone and offered a distress and inconvenience payment of £300. Mr & Mrs Y rejected that offer and brought their complaint to CIFO.

CIFO investigated and noted that the first transaction had been stopped because the beneficiary's bank account in the UK was on a UK banks' watch list – which the Channel Islands bank had access to. CIFO also noted, from the bank's recording of the first transaction call, that the fraudster's voice could be heard at the very end, instructing Mrs Y to hang up. CIFO felt that the bank should have noted that and been put on notice of potential fraud as it could reasonably have been feared that Mrs Y was potentially acting under duress, partly from hearing the fraudster's voice on the call but also more generally from the content of the call and the answers Mrs Y gave to the bank's questions. This was even more concerning as the bank had intercepted the first attempted payment because of

concerns about the beneficiary account. Had the bank recognised these signs and made more enquiries (possibly including contacting Mr Y) before releasing the first payment, CIFO concluded – on balance – that the fraud would have been uncovered and no additional payments would have been made.

CIFO upheld the complaint and recommended that the bank compensate Mr & Mrs Y for the amount which had not been recovered from the beneficiary banks, plus interest at an annual rate of 8% simple, plus a distress and inconvenience award of £500 – in total, about £30,000.