Case study: Banking

FRAUDSTER TRICKS COMPLAINANT INTO DIVULGING BANK DETAILS RESULTING IN A FRAUD

Themes: Vishing; mobile devices; fraud alerts; contributory conduct of customer.

This complaint relates to a complainant who had been tricked by a fraudster into disclosing personal bank details which resulted in a fraud.

In December 2022, Ms T was called by who she believed to be her bank's fraud team. Ms T was asked a number of questions, but Ms T stated that she had not disclosed any details and the call disconnected. Ms T received a second call relating to Ms T's online banking application which she advised she could not access but the caller did mention they would send a code to Ms T's mobile device to re-enable access. During this time three payments totalling approximately £50,000 were transferred from Ms T's bank account. The next day Ms T's bank called her because two new devices had been added to Ms T's online banking profile, which was unusual. It then transpired that Ms T had not authorised the payments made the previous day and night and Ms T had unfortunately been a victim of fraud. The bank advised that their counterpart in the UK would investigate and respond.

In January 2023, as Ms T had still not received any further clarity and after numerous calls with no return of the lost funds, Ms T raised a complaint with her bank. Ms T's bank investigated and advised that two mobile devices had been added to Ms T's online banking profile after she had received the second call from who she believed was her bank's fraud team but was actually a fraudster. Ms T's bank stated that in order for these mobile devices to have been added, certain personal details must have been obtained by the fraudsters. The bank rejected Ms T's complaint on the basis that the personal details were disclosed by Ms T to the fraudster and that Ms T had ignored various fraud warnings issued by the bank, specifically alerting customers not to reveal personal bank information. Ms T referred her complaint to CIFO.

CIFO investigated and was satisfied that Ms T had not authorised the payments but had been tricked into disclosing bank information to the fraudsters, which ultimately resulted in the payments being fraudulently made. CIFO also found that two payments had been authorised from Ms T's bank account by a new device and were close to the daily payment limit. The final payment again was made for close to the daily payment limit in the early hours of the following morning and also authorised by the new device. CIFO concluded that, based on the balance of probabilities it was reasonable to have expected the bank to have made enquiries after the first two payments had been made, as they were unusual. If the bank had queried the payments at that point, it may have prevented the authorisation of the third and final payment. Therefore, CIFO upheld the complaint in part and recommended the bank compensate Ms T for the last payment of approximately £25,000.