Case study: Banking

SOCIAL MEDIA SCAMMERS TRICK COMPLAINANT INTO SENDING MONEY

Themes: Authorised Push Payment (APP) Fraud; fraud alerts; process and procedures.

that scammers were duping the complainant into sending them a large amount of money over an extended period of time.

In 2020 and 2021, Mr T made hundreds of payments to various individuals he met on social media. Most of the transactions were small, but a few were five figure sums. In total, he paid more than £300,000 to the scammers. Initially, the payments were made from Mr T's personal account but later he made them from a joint account he held with his partner.

Part of the overall arrangement was that Mr T would receive back all his money and more. Unfortunately, when he travelled to meet one of the individuals in person to collect his money, no-one was there. It was at this point Mr T felt he had been a victim of fraud. He discussed the transactions with his partner and contacted his bank complaining they had failed to notice the many inconsistent payments that had been made from his accounts. He asked to be reimbursed, but the bank said Mr T had authorised the payments and they were unable to recover any of the money so they rejected his complaint. Mr T referred his complaint to CIFO.

CIFO investigated and noted that, because the majority of the payments were fairly small, they would not likely have triggered the bank's fraud alert systems. Whilst the UK code of practice relating to the reimbursement of fraudulent payments does not apply in the Channel Islands, banks are nevertheless required to have systems in place to identify potentially fraudulent transactions to protect their customers. In Mr T's case, the bank had questioned Mr T about some of the larger payments, but he had told them he knew what he was doing, and the payments were genuine. Therefore, CIFO concluded on balance that, even if the bank had done more than they did, it was unlikely Mr T would have listened or done anything different to avoid the fraud. Mr T and his partner rejected CIFO's initial recommendation, saying the joint account transactions had been inconsistent with past account activity and, because Mr T had been taking strong medication at the time, they felt he was vulnerable and that the bank should have done more to identify the fraud.

CIFO recognised that the bank had a duty to act on the instructions of either party to the joint account without 'cross-checking' with the other party. Moreover, the bank had issued regular statements to Mr T and his partner which had shown the volume of payments and the transactions, but at no point had this raised any suspicion. CIFO also reviewed the type of payments that had been made and felt that at least some of them should have alerted Mr T to their fraudulent nature – not least because he had previously been the victim of a similar fraud. CIFO further noted that Mr T had not told the bank he was taking strong medication so the bank could not be reasonably expected to see him as having been vulnerable. CIFO concluded that Mr T would have continued making

payments to the scammers even if the bank had explained the fraud risks more than it did. CIFO did not uphold the complaint.