Case study: Banking

COMPLAINANT SCAMMED BY FRAUDSTER CLAIMING TO BE FROM 'AMAZON'

Themes: Scam; remote account access; fake refund; bank failure to query or block unusual transaction.

This complaint relates to a fraudulent call a complainant received from someone pretending to be from Amazon about a supposed error when refunding an Amazon Prime subscription.

In July 2021, Mr T received a call from a fraudster who said he was from Amazon. The fraudster said he needed to refund approximately £80 to Mr T for an unwanted Amazon Prime subscription. The fraudster then sent Mr T an email asking him to confirm the refund amount, after which Mr T received another call from the fraudster saying that 'Amazon' had refunded approximately £8,000 in error. The fraudster asked Mr T to log on to his online banking to check and he saw a large credit on his current account. Assuming this to have been the 'Amazon' refund, Mr T agreed to return the overpayment to a named individual at 'Amazon'. He made an initial payment of £5,000. Mr T then saw his computer screen go blank. Unknown to Mr T, the fraudster had taken control of his online banking.

What happened next was that the fraudster, having already made a transfer from Mr T's savings account to his current account made two further payments, one for £4,000 and another for £5,000. Mr T became suspicious when his computer screen stayed blank and he telephoned the police, who telephoned the bank. The bank blocked Mr T's account which prevented any further payments from being made. The bank was unable to recover any of the money that had been paid to the fraudster and it refused to reimburse Mr T for any of the payments that had been made. Mr T accepted that he had authorised the first payment but he did not believe he had authorised the second and third payments, which totalled £9,000. Mr T asked the bank to refund that amount to him. The bank declined to do so. The bank considered Mr T had been negligent in disclosing his online login details which gave the fraudster access to his accounts. Mr T referred his complaint to CIFO.

CIFO investigated and, although unable to clearly establish how the fraudster had gained remote access to Mr T's computer to authorise the payments, noted that the bank had not identified the change in account activity before they had been contacted by the police. CIFO felt that when the third payment was being made the bank should reasonably have identified this as an unusual pattern of transactions and alerted Mr T to the potential fraud. CIFO concluded that had the bank done so, the third payment would not have been made. CIFO therefore upheld the complaint in part and recommended the bank refund Mr T the final payment of £5,000, with additional interest at 8% simple from the date the payment was made to the date of settlement.