DRN-4938493

The complaint

Mr O complains about Kroo Bank Ltd.

He would like Kroo to refund him two transactions totalling £4,000 that were made from his account when he was the victim of a scam.

What happened

Mr O has unfortunately fallen victim to a safe account scam. He initially received a phone call from someone pretending to be from the Financial Services Compensation Scheme (FSCS) team at S (another bank). They explained that someone had access to his banking apps, and that he needed to secure his money.

They then asked if Mr O if he had any other accounts, and Mr O mentioned he had an account with Kroo. They explained that they would transfer him to the relevant team.

After speaking with 'Kroo' for about ten minutes, Mr O realised he was being scammed, and hung up. He then says he changed his password and email. The scammer kept trying to contact him, but he didn't answer. Mr O then reported what had happened to Kroo but didn't get much information from them about what was happening.

Mr O complained to Kroo about what had happened, but it didn't uphold his complaint, so he then brought his complaint to this Service.

Our Investigator looked into thigs and thought that the complaint should be upheld. Kroo responded with some further information, so our Investigator wrote back asking for more information, but Kroo didn't respond.

Our Investigator then provided Kroo with a second view where they explained that as Kroo hadn't responded, they were still minded to uphold the complaint.

To date, Kroo has still not provided a response to our Investigators second view, so the complaint has been passed to me to make a final decision.

What I've decided – and why

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

Having done so, I have decided to uphold this complaint for broadly the same reasons as our Investigator. I'll explain why.

The Payment Services Regulations 2017 (PSR's) outline that Kroo will be liable for unauthorised payments on their consumers accounts, unless they can show that said consumer failed with gross negligence or intent to keep their account details safe. In line with the PSR's, a payment can only be classed as authorised if it can be shown that an account holder, like Mr O, completed the payment themselves, or if they gave a third-party

permission to do so on their behalf.

Kroo has provided this Service information which shows that the two payments were made as faster payments, and a device history for Mr O's account, which shows which devices could have been used to complete the payments. It hasn't confirmed which device was used to complete the two payments in question.

Kroo has also shown that a general warning would have been shown when at least the first payment was made from Mr O's account, which says that they payment could be a scam. Kroo says that despite this warning, the payments still debited Mr O's account, and that it blocked further payments from being made.

Looking at the device history, a new device was linked to Mr O's account only four minutes before the transactions were made. Kroo has been asked to provide information about how a new device is added to an account, and what steps would need to be completed before a device is able to access the account – but it hasn't provided this.

While Kroo hasn't confirmed which device was used to make the payments, on balance, I think it's more likely that the payments were made by the scammer using the new device, and that Mr O was somehow tricked into sharing some information with the scammer to enable this to happen.

So, on balance, I don't agree that Mr O authorised the payments himself or gave permission for someone else to do this for him as in line with the PSR's, Mr O didn't complete the whole procedure himself (such as adding the payee and amount) – and instead it was the scammer who tricked him into parting with information. And I therefore consider they payments to be unauthorised.

Did Mr O fail with gross negligence or intent to keep his account details safe?

Having considered what happened here, I don't find that Mr O was grossly negligent or failed with intent to keep his account safe.

Mr O has been honest about what he can recall from the interaction with the scammer and has explained that the initial call took place via a spoofed number which matched S's website. He says he was on the phone with them for a long time, and when he was transferred through to 'Kroo' had a genuine belief that he was speaking with his genuine bank, and that they knew things he would only have expected his genuine bank to know.

I believe that the scam had a degree of sophistication to it – and I can see why Mr O was taken in by what happened – especially given that the call began from a number listed on S's website.

Mr O has also been honest that he may have divulged some information to the scammer – but can't remember what this might have been. But I think it's likely that he divulged enough information for the scammer to gain access to his account by linking a new device. However, I don't think in the context of the scam that Mr O's actions amount to gross negligence – especially given the believability of the scam, including the spoofed number and the lack of information provided by Kroo about the steps needed to add a new device to the account.

Putting things right

Kroo Bank Ltd should refund Mr O £4,000. On top of this, it should also pay Mr O 8% simple interest from the day of the transactions until the date of settlement (less any lawfully deductible tax).

My final decision

I uphold this complaint. Kroo Bank Ltd should put things right as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr O to accept or reject my decision before 21 April 2025.

Claire Pugh
Ombudsman