DRN-5973750

The complaint

Mrs A is complaining that Kroo Bank Ltd hasn't provided a full refund of payments she said she didn't make after falling victim to a scam.

The complaint is brought on her behalf by a professional representative, but I'll mainly refer to Mrs A here.

What happened

On 5 June 2024 Mrs A was called by someone she believed to be from Kroo. She said that the caller ("the scammer") had her full name, address and account details, and completed a security check to confirm her identity.

The scammer told Mrs A that her Kroo account had been compromised, and she needed to take steps to keep it safe, by cancelling her card and re-setting her password. She was told by the scammer to forward a password re-set email she'd received from Kroo to an email address which Mrs A thought also belonged to Kroo, but was actually operated by the scammer.

Using the password re-set link, the scammers were able to access Mrs A's Kroo account and they instructed payments totalling £34,000 from it. Kroo asked for the purpose of some of the payments in the in-app chat and it was told they were to pay friends and family.

Shortly after the call ended Mrs A realised that payments had been made from her account and reported what had happened to Kroo. Kroo took some time to investigate but on 26 July 2024 it told Mrs A it would refund £17,000, with interest at 4.6% (which was roughly the interest rate applicable to credit balances on Mrs A's account at that time). The refund was made to Mrs A's account on the same day.

Mrs A wasn't satisfied with this as she thought the full value of the payments should be refunded. She complained to Kroo and when it didn't change its position she brought her complaint to the Financial Ombudsman Service.

Our Investigator didn't think Mrs A had authorised the payments or that Mrs A had acted with gross negligence, and so he thought Kroo should refund all the payments she hadn't authorised. But Kroo didn't agree. It replied to say it didn't dispute that the payments hadn't been authorised by Mrs A. But it thought she had failed with gross negligence in sending the password re-set link to a third party, which meant it wasn't liable to make a further refund.

Mrs A's complaint has now been passed to me for review and a 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'm upholding Mrs A's complaint, for much the same reasons as the Investigator.

Authorisation

I've started by considering whether Mrs A authorised these payments. This is relevant as, in line with the Payment Services Regulations 2017 (PSRs), she would generally be liable for payment she authorises – whereas Kroo would be liable for unauthorised payments.

The PSRs specify that authorisation depends on whether the payer (in this case, Mrs A) has given consent to the execution of the payment instruction. The PSRs specify how consent is given: it must be in the form, and in accordance with the procedure, agreed between Mrs A and Kroo.

Kroo's terms and conditions set out how Mrs A consents to payments, as follows:

To make a payment you must use the App. We will normally only make the payment if your account has enough money in it, or if you have an arranged overdraft sufficient to cover the payment. In certain circumstances a payment may go through even if you do not have enough money in your account. The payment will still be valid, and you must then bring your account back into credit (see also Conditions 21 and 22). Your instructions will be taken as your consent to make payment.

Here, Kroo accepts that Mrs A's account was compromised, and it was the scammer who gave the payment instructions in the app, not Mrs A. So, Mrs A didn't complete the agreed form and procedure for making the payments. Mrs A shared the password re-set link thinking she was safeguarding her account, not with the intention of allowing a third party to make payments from her account, so I don't think it would be fair to say that in doing so she gave a third-party permission to consent to payments on her behalf.

Kroo has provided some information to show that it asked for the payment purpose for some of the payments and it was confirmed in its in-app chat that they were being made to friends and family. It's not particularly clear whether Kroo thinks it was Mrs A that answered these questions. However, assuming it was Mrs A responding to Kroo's questions here, I think the purpose of these interventions was to determine the purpose of the payments, rather than if the payment instructions were genuine. So, I don't think it means Mrs A was agreeing to the payments.

And in any event Kroo has accepted that these payments weren't authorised by Mrs A and I'm reaching my conclusion with this in mind. And taking everything into account here I'm satisfied the disputed payments were unauthorised.

Gross negligence

Kroo says that it shouldn't be liable for the unauthorised payments because Mrs A failed with gross negligence to comply with the terms of the account and keep her security details safe – something which, if proven, would mean she wouldn't be entitled to a refund under the PSRs.

I would consider gross negligence to be a lack of care which goes *significantly* beyond what we would expect of a reasonable person. To assess whether Mrs A acted with gross negligence, I've reflected on the circumstances that led to the scammer gaining access to Mrs A's Kroo account through her sharing the password re-set link by email, which enabled the payments to be made.

Mrs A says she believed she was speaking to Kroo and was acting to safeguard her account and I've no reason to doubt that this was the case. The scammer was able to convince her of this because they had personal details about her as well as information about her account that she thought only Kroo would know.

I can see that Mrs A was instructed to send the password re-set email to an email address which contained the word Kroo, but to an email domain which Kroo wouldn't normally use. Kroo has pointed out this domain provided disposable email addresses and it says Mrs A ought to have completed more due diligence in verifying who she was sending the password re-set link to.

But I must bear in mind that Mrs A was being put under a lot of pressure by the scammer to act to safeguard her account, and that she believed she was speaking to a Kroo representative, so it doesn't seem unreasonable that in such a high-pressure situation she would have followed their instructions. And I don't think the email address Mrs A was given was so clearly not related to Kroo that it would have been obvious to Mrs A at the time that she was sharing her secure details with a third party, or that Mrs A ought reasonably to have been aware that this was a domain that provided disposable email addresses.

This isn't to say Mrs A acted perfectly reasonably - but although her actions could be considered careless, she was under a lot of pressure at the time. And having considered all the circumstances carefully, I'm not persuaded Mrs A showed a lack of care which fell significantly below what I would expect of a reasonable person. So, I don't consider that Kroo has shown she failed with gross negligence here.

Conclusion

It follows that, in line with the PSRs, I don't consider Mrs A can be fairly held liable for these unauthorised payments and Kroo must put things right – by refunding her remaining loss from the disputed payments along with 8% simple interest per year for the time she's now been out of pocket.

My final decision

For the reasons I've explained, I uphold Mrs A's complaint. Kroo Bank Ltd must:

- Pay Mrs A the total of the unauthorised payments that remains outstanding - £17,000; and

- Pay 8% simple interest per year on this amount, from the date of the unauthorised payments to the date of settlement (less any tax lawfully deductible).

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs A to accept or reject my decision before 23 December 2025.

Helen Sutcliffe
Ombudsman