DRN-5988841

The complaint

Mrs Q complains that Kroo Bank Ltd ("Kroo") won't refund payments made as part of a scam.

Mrs Q is being represented by her son, Mr Q, in bringing this complaint.

What happened

The detailed background to this complaint is well known to the parties and has been set out previously by the investigator. Briefly, Mrs Q fell victim to an impersonation scam in December 2023 after she clicked on a parcel redelivery phishing link. She was contacted by someone who claimed they were calling from her bank "N". The caller mentioned suspicious activity on Mrs Q's account with N and, under the guise of protecting her money, persuaded her to set up an account with Kroo and transfer funds.

Mrs Q says the caller also asked her to install a remote access application on her phone. Once the funds were in the Kroo account, the caller told Mrs Q that they needed to move the funds around to secure them. And she was told not to tell her family or anyone else.

Unfortunately, five payments totalling just over £13,000 were made from Mrs Q's Kroo account over a period of five days. When she subsequently discussed this with her family, she realised she'd fallen victim to a scam. Kroo ultimately refused to refund the disputed payments. It said the payments were processed from the device that was used to set up the account and Mrs Q confirmed this belonged to her. Kroo said it wasn't possible for a third party to control Mrs Q's device remotely, given the app and the mobile device in question.

The complaint was referred to the Financial Ombudsman Service, and our Investigator eventually concluded that it was fair for Kroo to treat the disputed transactions as authorised. They also thought that Kroo ought to have taken additional steps before processing the fourth (i.e. second to last) payment, and this likely would have uncovered the scam. In recommending a refund of the last two transactions, the Investigator considered it fair that Kroo could make a 50% deduction for contributory negligence on Mrs Q's part.

The complaint couldn't be resolved informally and was passed to me to decide. I wrote to Mrs Q's representative informally – as I'm allowed to under our rules – and gave reasons for why I didn't intend upholding the complaint. I explained that while I agreed with the Investigator's findings on authorisation and the suggested trigger point for intervention, based on the evidence I wasn't persuaded that enquiries by Kroo at that point would have prevented Mrs Q's loss resulting from the last two payments.

Mr Q disagreed and asked that I reconsider my findings in light of his and Mrs Q's appeal. In summary, he submits that Mrs Q's circumstances made her vulnerable and she was subjected to compelling psychological pressure created through fear.

Mr Q also questions the finding on authorisation and states that device confirmation doesn't equate to informed consent. Additionally, he strongly believes that the transactions ought to have flagged as suspicious.

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.

I'd like to start by thanking the parties for their patience while the complaint has been awaiting an ombudsman's decision.

It's very unfortunate that Mrs Q has lost money to a scam. But Kroo doesn't automatically become liable to reimburse her. As Mrs Q says the disputed payments are unauthorised, the relevant law here is the Payment Services Regulations 2017 (PSRs). The starting point is that Mrs Q is responsible for a payment she authorised, and Kroo would generally be liable for an unauthorised payment.

Has Kroo acted fairly in treating the disputed payments as authorised?

Under the PSRs, a payment is authorised if it is correctly authenticated and consented to by the customer, or on their behalf. The PSRs say that consent for a payment transaction *"must be given in the form, and in accordance the procedure, agreed between the payer and its payment service provider."*

In other words, consent happens when Mrs Q or someone on her behalf completes the steps agreed for making a payment. And for the purposes of whether a payment is authorised under the PSRs, it doesn't matter if Ms M was deceived about the purpose or amount of the payment.

Here the relevant framework contract are the terms and conditions applicable to Mrs Q's Kroo account. In order for the disputed payments to be considered authorised, Mrs Q – or someone on her behalf – would need to have given her consent as set out in the terms.

I've reviewed the relevant terms and conditions, and they don't explicitly set out how consent is given for an electronic transfer or an online card payment. So, I've thought about what practical steps are needed to make such payments. For electronic transfers, Kroo's terms specify that it's banking app would need to be used. Beyond that, I consider the likely steps involved would be enter the payee's account information and the amount, before confirming the transaction. If prompted, additional authentication in the form of entering a one-time passcode or completing biometric verification.

For online card payments, it seems that Mrs Q's card details (long card number and associated security details) would have been needed to give the payment instructions on the merchant's website, and, if prompted, additional authentication in the form of entering a one-time passcode or completing biometric verification.

Kroo has shown that the disputed payments – both electronic transfers and card transactions – were either initiated or verified through additional layer of authentication within its banking app. And this app was installed on the only device registered to Mrs Q's account with Kroo at the time the payments were made. Kroo has also shown that this was the same device that was used to set up Mrs Q's account.

I've done my own research into the remote access software Mrs Q says was used, and the suppliers have confirmed that the software is limited in terms of its functionality on devices using the operating system installed on Mrs Q's phone – meaning while it would have allowed a third party to see the information displayed on her screen, it wouldn't have allowed them to take control of her device.

What this means is that it's unlikely that remote access software was being used to control Mrs Q's phone to access the Kroo app when the payments took place. In other words, the payments could not have been processed without Mrs Q's involvement.

I'm also mindful that in a call with our Investigator, Mrs Q showed awareness of funds needing to be moved. Her understanding that funds would be leaving would be sufficient to say the payments would be deemed authorised under the relevant regulations. I appreciate that she was tricked into the reason for why payments needed to be made. But that isn't a consideration under the PSRs for deciding whether the payments would be deemed authorised.

While I accept that Mrs Q didn't intend to consent to a payment and likely completed the steps in her banking app because she was being tricked by a third-party, her intention in the situation isn't a consideration under the PSRs. The test here is whether she consented to the payment.

Also, under the PSRs, the concept of giving consent is a formal one. Being tricked or coerced doesn't invalidate consent. There's no concept of 'informed' consent (something often seen in healthcare). So, while I accept the difficult situation Mrs Q was in when the scam happened, I can't fairly conclude that the payments were unauthorised.

Is there any other reason it would be fair for Kroo to be held liable for the disputed payments?

Kroo has a duty to act on authorised payment instructions without undue delay. However, there are circumstances when it might be appropriate for Kroo to take additional steps before processing a payment. Such as when there are grounds to suspect that the payment presents a fraud risk. That might occur when a payment is significantly unusual or uncharacteristic compared to the normal use of the account.

The account in question was recently set up. As such, there wasn't any previous account activity to compare the disputed payments with. Considering their value and their destination, I don't find the first three payments were that unusual or significant to the extent that Kroo would be expected to intervene.

Kroo did block a payment attempt two days prior. It's system notes show that it asked Mrs Q some questions about the payment via it's in-app messaging. Kroo received a response from Mrs Q which said the payment in question was a transfer to a friend or family member. Questions were also asked about the recent deposits into the account followed by payments, and whether someone else was involved in creating the Kroo account. The responses Kroo received were reassuring. It was also forwarded what appears to be a text message from the beneficiary of the flagged payment, confirming their account details.

Given what we know about limitations on the type of phone Mrs Q has when it comes to controlling a device remotely using the software that the scammer asked her to download, it's unlikely that the scammer could have typed up the responses that were sent to Kroo. I fully accept that the scammer likely coached or instructed Mrs Q on how to respond. They might have even helped her with the text message that was shared with Kroo. But based on the technical evidence before me, on balance, I'm persuaded that it was Mrs Q who responded to Kroo. This particular payment didn't go through as Kroo received instructions from Mrs Q to cancel it.

There was a further intervention a few days after the first three payments were made. The payment was for £100 and again Kroo was advised that Mrs Q was paying a friend or family

member. This time too, instructions were subsequently received to cancel the payment and so it didn't go through.

With the above in mind, I'm not persuaded that things would have gone differently had Kroo taken additional steps when the fourth disputed payment, which was larger in value, was made. Given the responses Kroo received in its earlier interventions, on balance, I think it's more likely than not that Mrs Q would have responded to Kroo's questions in a similar way. As such, I don't think the scam would have been uncovered had enquiries been made before processing the payment in question (or the subsequent payment). What this means is that I don't think Kroo could have prevented losses stemming from the last two payments either.

Mr Q feels strongly that my conclusions on causation are speculative. I can't know for certain what would have happened if Kroo had made enquiries with Mrs Q at the suggested intervention point.

In such situations, I reach my conclusions not based on mere possibilities but rather on what I find most probable to have happened in the circumstances. In other words, I make my decision based on the balance of probabilities – so what I consider most likely to have happened considering the evidence that is available and wider circumstances of the case.

As I've mentioned, Mrs Q had previously been asked if someone else was involved in creating the Kroo account. She was also asked about the purpose of the transactions. The responses Kroo received show the extent to which she'd been coached into withholding information if questioned. Given this, I think it's unlikely that she would have been forthcoming about the true purpose of the payments had Kroo questioned her. That means I don't think Kroo could reasonably have done anything more to prevent or limit Mrs Q's losses.

I've also carefully considered Mr Q's comments about Mrs Q's vulnerability. I thank Mr Q for sharing some details about her situation. I don't doubt what he's told about how her circumstances could impact his decision-making. But this isn't reason alone to tell Kroo to refund Mrs Q in full. Kroo wasn't aware of Mrs Q's circumstances.

I've considered whether Kroo should proactively have identified potential vulnerability. But I don't consider there was anything during its intervention on the two occasions that I've mentioned above which ought to have put it on notice about Mrs Q's circumstances. Mr Q has suggested that a phone call would have been a stronger intervention. But Kroo is an app-based bank. In the circumstances, I don't think it could or should have taken different or additional steps.

In conclusion, I realise that this outcome will come as a significant disappointment to Mrs Q. Not least because this complaint has been ongoing for some time. Despite my natural sympathy for the situation in which she finds herself, for the reasons given, it wouldn't be fair of me to hold Kroo liable for her loss.

My final decision

For the reasons given, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs Q to accept or reject my decision before 29 December 2025.

Gagandeep Singh
Ombudsman