

The complaint

Mr C has complained that Kroo Bank Ltd won't refund the money he lost after falling victim to a scam.

What happened

In summary, in 2023 Mr C was looking to invest. He found a company which offered to invest on his behalf. Unfortunately, this turned out to be a scam.

On the scammers' advice, Mr C opened a cryptocurrency wallet. Starting with a small first payment, he made transfers from his Kroo account to his crypto account, then he sent crypto on to the scammers' platform. Over the course of a couple of months, Mr C paid over £14,000 to the scammers across several payments.

In the end, Mr C was unable to withdraw his investment and realised he'd been scammed.

In 2024, Mr C complained to Kroo via representatives. Kroo didn't think it was liable for Mr C's loss.

Our Investigator looked into things independently and didn't uphold the complaint. Mr C's representatives asked for an ombudsman's review, so the complaint has been passed to me to decide.

I sent Mr C and Kroo a provisional decision on 26 January 2026, to explain why I thought the complaint should be upheld. In that decision, I said:

There's no dispute that Mr C authorised the payments involved, even if he didn't intend for the money to end up with scammers. So under the Payment Services Regulations and the terms of his account, Mr C is liable for the loss in the first instance. But the matter doesn't end there.

Taking into account the law, regulator's rules and guidance, relevant codes of practice, and what I consider to have been good industry practice at the time, I consider that Kroo should have fairly and reasonably:

- *Monitored accounts and payments to counter risks such as fraud and scams;*
- *Had systems in place to look out for particularly unusual transactions or other signs its customers were at risk of fraud;*

- *In some circumstances, taken further steps or made further checks before a payment went out, or even blocked it, to help protect customers – irrespective of the type of payment involved.*

I currently find that Kroo should've intervened at the point of the second payment involved. The first payment, for £200, wasn't concerning enough to warrant intervention here. But the second payment, for £5,000, was of a concerningly large size, going to a recently new payee, which was a crypto site. And by this point, the Financial Conduct Authority (FCA) and Action Fraud had published warnings about cryptocurrency scams, there was wide media coverage, and other firms were restricting such payments; so Kroo should've had a good understanding of the higher risk involved. While Mr C's account did have a substantial balance at the time, from what I've been given, I can't see that there was any comparable activity in the prior period. Overall, I currently think that the spending stood out as concerning at the point of the second payment, and it should have prompted Kroo to intervene.

Had Kroo intervened at that point and asked reasonable questions, it seems most likely that it could have uncovered the scam and stopped any further loss. I've found nothing to make me think that Mr C would not have been honest with Kroo, or that he would not have listened to his bank. He accepted he was inexperienced. And indeed, when Kroo did stop a later attempted payment, Mr C was open that he was paying an account in his own name to fund a crypto wallet, while under pressure from the (scammers') investment company. Kroo probed further, and Mr C agreed to stop further payments, which seems to have stopped the loss. So it seems most likely that earlier person-to-person intervention would've stopped the loss, too. This was a relatively prominent type of scam, involving pressuring Mr C to forward large amounts of crypto to an unfamiliar platform under the scammers' control, so I think Kroo would have been able to identify what was happening and prevent it.

Even if I didn't think that person-to-person intervention was warranted, the second payment should have at least prompted Kroo to present Mr C with a series of questions about his reasons for payment, and to provide better automated warnings tailored to his answers. An effective proportionate warning should've highlighted the key details of relevant scams, tailored to Mr C's answers, and resonated with him. And as noted, when Mr C was questioned, he gave appropriate answers and stopped the spending. So it seems more likely than not that an appropriate tailored warning would've prevented the loss here.

I've also thought carefully about Mr C's role in what happened. In the circumstances, I can understand why Mr C might have believed the scammers. I understand that they set up a complex platform to look legitimate, kept in close contact, and added him to a group chat which would've appeared to have other investors finding success. Importantly, I understand that Mr C looked into the scammers' company online before investing, and at that point it seems that he would've found very positive reviews. Things like the regulator's warning and the rush of negative reviews don't seem to have come until after Mr C had researched the matter and started investing. It seems that the matter would've looked reasonably convincing to an inexperienced investor in Mr C's situation at the time, and I've seen nothing to suggest that Mr C was, or ought to have been, familiar with this type of scam. So I don't think that Mr C needs to share liability for the loss from the second payment onwards.

Lastly, I've considered what Kroo did to try to recover Mr C's money after being told about the scam. Unfortunately, it wasn't possible for Kroo to recover funds which Mr C had already sent on in crypto. And any funds remaining in Mr C's own crypto account were still in his name, so there'd be nothing more for Kroo to do there either. As these were payments to Mr C's own crypto account, they were not covered by schemes like the CRM Code or ASR Rules. And I'm afraid there was nothing more that Kroo should've reasonably done which would've realistically got the money back here.

But overall, I think Kroo bears liability for the loss from the second payment onwards – i.e. the £5,000 payment, and the £5,000 and £4,000 payments which followed it. I've set out below how I currently think Kroo should settle the complaint.

I said I'd consider anything else anyone wanted to give me – so long as I received it by 9 February 2026. I'll talk about the responses below.

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.

In response to the provisional decision, Mr C accepted it, and Kroo did not.

In summary, Kroo argued that the payment had gone to an account in Mr C's own name, there'd been one prior payment to that payee a few weeks earlier, his Kroo account had little historical data to compare this spending to, and while it was a current account, it was also geared towards savings which might entail larger payments.

While I do understand where Kroo is coming from, I'm afraid I already took account of those factors before making my provisional decision. In this case, the second payment was still a concerningly large amount in and of itself, going from a current account to a recently new payee (this being only the second transaction to that payee); with the payee being a crypto site which carried notable associated risk.

So even taking into account factors like the crypto account being in Mr C's name or the current account being usable for savings, it doesn't outweigh the overall concerning nature of the second payment in this particular case. I think Kroo should've carried out person-to-person intervention here. And as I explained in the provisional decision, even if I *didn't* think that person-to-person intervention was warranted here – e.g. because of the factors Kroo set out – at a minimum this second payment should've prompted Kroo to present Mr C with a series of questions, and provide better automated warnings tailored to his answers. And as I set out, Mr C gave open answers and stopped the spending when questioned, those warnings should've resonated with him, and so they would've most likely stopped the loss.

Kroo argued that it should not be held liable because the payments went to an account in Mr C's name. But Kroo should have fairly and reasonably been on the lookout for potentially fraudulent payments, even if the payments were going to another account in the customer's name. There were prominent scams which involved paying an account in one's own name, like this one. And identifying and preventing such scam payments would've still had the effect of preventing a loss to its customer. So Kroo can still be held liable for a loss which resulted from its failure to intervene – which is what I've found to have most likely been the case here. We cannot compel Mr C to complain about the crypto site, and my task here is to decide the dispute between Mr C and the parties he's complained about – which is Kroo.

So having reconsidered the case, I've come to the same conclusion as before.

Putting things right

I direct Kroo Bank Ltd to:

- Refund the loss from the second payment onwards in full; and-
- Add simple interest onto the refund at the rate of 8% simple per year. This is payable from the date each reimbursed payment debited, until the date of the refund.

If Kroo considers that it's required by HM Revenue & Customs (HMRC) to deduct tax from that simple interest, it should tell Mr C how much tax it's taken off. It should also give Mr C a tax deduction certificate if he asks for one. Mr C may be able to reclaim the tax from HMRC if he doesn't normally pay tax.

My final decision

I uphold Mr C's complaint, and direct Kroo Bank Ltd to put things right in the way I set out above.

If Mr C accepts the final decision, Kroo Bank Ltd must carry out the redress within 28 days of the date our service notifies it of the acceptance.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr C to accept or reject my decision before 9 March 2026.

Adam Charles
Ombudsman