

The complaint

Miss S complains that Kroo Bank Ltd won't refund the money she lost as the result of a scam.

What happened

In November 2024, Miss S received a message purporting to be from a well-known parcel delivery company. It said it had tried, unsuccessfully, to deliver a parcel to her. Miss S clicked on a link in the message and paid a small redelivery fee. In doing so, she entered her credit card details.

Not long after making the payment, Miss S received a phone call purporting to be from her credit card company. The caller said that there'd been some suspicious activity on Miss S's credit card account. Unfortunately, it ultimately turned out that the call was from a scammer. I'll refer to the caller as "the scammer" in this decision, although I appreciate that Miss S didn't realise she was talking to a scammer at the time.

The scammer told Miss S that there was a risk that the fake message and link about the parcel could have compromised other financial apps on her phone. They asked Miss S which banks she held accounts with, and how much she had in each one. Miss S told the scammer about accounts she had with three banks, including Kroo. While still on the call, the scammer said they'd contacted those banks, and the only one that hadn't reported suspicious activity was Kroo.

The scammer told Miss S that someone would contact her from one of the banks ("C"), where she held some of her savings, and Miss S quickly received a call purporting to be from C. Sadly, it turned out that the scammer was behind that call too. The scammer told Miss S to transfer her money from C to Kroo, as Kroo was the only safe account she held. Miss S then made a series of five transfers from her account with C to her account with Kroo. Between those five transfers, she emptied out her account with C entirely.

Once Miss S had transferred the money to her Kroo account, the scammer helped her to set up a new account with C. They told her she should give the account a name (which I'll refer to as "R"). That name was the same as the name of an international money transfer service. The scammer said the new account was safe, and that Miss S could transfer her money to it from her Kroo account.

Miss S gave the scammer the card details for her Kroo account. She's provided evidence that four payments were initially declined. A screenshot of a message that appeared on her screen explains that the billing address entered didn't match the address on Miss S's account. Miss S says she asked the scammer about this, and they said it had been a mistake on their part.

The scammer then made three payments using Miss S's debit card. In each case, Miss S authorised the payment using 3D Secure. But the payments didn't go to Miss S's account. Instead, they went to an account at the money transfer service which had the same name that the scammer had told Miss S to give her new account at C.

Miss S authorised the following payments. I should mention that both the statement for Miss S's account with Kroo and the screenshot she's provided from her Kroo app show the largest payment first. The statement shows payments 2 and 3 in the order shown below. The app shows them the other way round.

	Date	Time	Method	Amount
1	15 November 2024	18:01	Debit card	£2,501.90
2	15 November 2024	18:03	Debit card	£2,251.90
3	15 November 2024	18:05	Debit card	£2,351.90
Total				£7,105.70

One of our investigators considered the complaint and thought it should be upheld in part. In summary, he thought that Kroo should have realised, when Miss S made payment 3, that she was at risk of financial harm, and should have contacted her to ask about the payments. And he thought that if it had done so, Miss S wouldn't have made payment 3. But he thought that Miss S had missed some warning signs, and should bear responsibility for 50% of her loss.

Miss S acknowledged the investigator's view, but was disappointed with the outcome. Kroo didn't respond to the view, and when the time for doing so had passed, the complaint was been passed to me to make a final decision.

After considering all the evidence, I issued a provisional decision on this complaint to Miss S and to Kroo on 1 August 2025. I explained that based on what I'd seen so far, I agreed with the investigator that the complaint should be upheld in part, but the redress I was recommending was different. So I wanted the parties to have a chance to comment before I issued my final decision. I said:

"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 say straight away that I was very sorry to hear that Miss S fell victim to a cruel scam, which deprived her of money she'd worked hard to save. I have a great deal of sympathy for her, and realise that the situation will have had a significant impact on her.

It's common ground that the payments made to the scam were 'authorised'. Miss S made the payments to the scammer using her debit card. So even though she didn't intend the payments to end up with a fraudster, they were 'authorised' under the Payment Services Regulations. Kroo had an obligation to follow the payment instructions it received, and Miss S is presumed liable for her loss in the first instance. But that's not the end of the matter.

In deciding what's fair and reasonable, I'm required to take into account relevant law and regulations, regulators' rules, guidance, standards and codes of practice and, where appropriate, what I consider to have been good industry practice at the time. Taking those things into account, I think that at the time the payments were made, Kroo should have been doing the following to help protect its customers from the possibility of financial harm:

- *monitoring accounts and payments to counter various risks, including fraud and scams;*
- *keeping systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things) – especially given the increase in sophisticated fraud and scams in recent years, with which financial institutions are generally more familiar than the average customer;*
- *acting to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring that all aspects of its products, including the contractual terms, enabled it to do so;*
- *in some circumstances, regardless of the payment method used, taking additional steps, or making additional checks, before processing a payment, or, where appropriate, declining to make a payment altogether; and*
- *being mindful of -among other things – common scam scenarios, how fraudulent practices were evolving (including, for example, the use of multi-stage fraud by scammers) and the different risks these can present to consumers when deciding whether to intervene.*

However, I also need to bear in mind that banks process high volumes of transactions every day, and I consider that there's a balance to be struck. Banks have obligations to be alert to fraud and scams and to act in their customers' best interests, but they can't reasonably be involved in every transaction. And I think it was reasonable of Kroo to consider a range of factors when deciding whether to take any additional steps before making the payments.

While payment 1 was a significant amount of money for Miss S, it wasn't so much that I think Kroo ought to have been concerned about it, based on its size alone. But payment 2 was just two minutes after payment 1. It was for an amount that was similar to payment 1 and took Miss S's total payments to that payee to £4,753.80 in the space of two minutes. I've looked at Miss S's bank statements for the six months before she made the payments to the scam. There had only been one payment of over £1,000. That was made a couple of weeks before the scam payments, and was clearly marked as a credit card bill payment. There's no sign that Miss S had made any previous payments to a money transfer service.

I've also borne in mind that the payments to the scam came just after a rapid series of payments into Miss S's account from her account at C, and that immediately before the payments to the scam, payments from Miss S's account to the account at R had been declined on the grounds of a mismatch between the address entered and the address Kroo had on record for Miss S.

Taking everything into account, and on the facts of this particular case, I think there were enough red flags when Miss S made payment 2 that Kroo ought to have contacted her about the payments. Miss S has told us that she doesn't remember being instructed by the scammer about how to respond to any questions or warnings from her banks if they contacted her. And I think it more likely than not that if Kroo had asked her appropriately probing questions about the payments, the scam would have been uncovered, and Miss S wouldn't have gone ahead and made payments 2 or 3.

Contributory negligence

Miss S accepted the investigator's view that she should share the responsibility for her loss with Kroo, so I won't consider this aspect in detail here. However, I agree with the investigator's view and reasons regarding this aspect of the complaint. Even allowing for the stress and feeling of urgency that the call would have instilled, I think the fact, in particular, that Miss S was asked to give her new account with C a name that wasn't hers, and to give the caller her debit card details, might reasonably have been expected to alert her to the possibility that something wasn't right. And I agree that attributing 50% of the responsibility for the loss she made on payments 2 and 3 to Miss S is fair in the circumstances.

Recovery of the money

I've considered whether, on being alerted to the scam, Kroo could reasonably have done anything more to recover Miss S's losses, but I don't think it could. The payments were made by debit card and authorised by Miss S, using 3D Secure. Once such a payment has been authorised, it can't be stopped. I acknowledge that Miss S has mentioned that she made a large payment from her savings account with another provider to the scam, and that was stopped and the money returned to her account. But in that case, the payment wasn't made by debit card, and Miss S has told us that it would have taken 24 hours to be processed in any event. I'm glad that her account provider in that case managed to prevent the transfer from going out. But that doesn't mean that I consider that Kroo should have been able to do the same.

There are limited circumstances that allow a business to make a successful chargeback claim. In this case, the payments from Miss S's account were sent to a money transfer service, and the money was then transferred on in accordance with the scammer's instructions. So even though Miss S was unaware of that happening, the transfer service would have been acting in accordance with the instructions it received, and I don't think a chargeback claim would have had a realistic prospect of success."

And I said that my provisional decision was that Kroo should put things right by doing as I've set out under the heading "Putting things right" below.

Further submissions

Miss S has told us she accepts my provisional decision. But Kroo doesn't agree. It says that my provisional decision acknowledges that:

- Miss S authorised the payments using 3D secure;
- Kroo had an obligation to follow the payment instructions received; and
- It correctly abided by the Payment Services Regulations

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 acknowledged in my provisional decision that the starting point was that Kroo had an obligation to follow the payment instructions it received. I also acknowledged that Miss S authorised the payments using 3D secure, and that they are viewed as 'authorised' under the Payment Services Regulations. But as I said in my provisional decision, there are actions which a bank can reasonably be expected to take which run alongside the general obligation to follow payment instructions.

As I explained, there's a range of things that I think that Kroo ought to have been doing by 2024, when Miss S made the payments, to minimise the risk of financial harm from fraud and scams. Those things are set out in my provisional decision, quoted above. And in some cases, a reasonable level of vigilance should have resulted in it taking additional steps before processing a payment. So I don't consider that it was automatically reasonable of Kroo simply to go ahead and follow Miss S's payment instructions without more.

For the reasons I set out in my provisional decision, my view was that in this particular case, there were enough warning signs when Miss S made payment 2 that Kroo ought to have contacted her about the payment, and asked her some probing questions about it. And I thought that if it had done so, it was likely, on balance, that she wouldn't have made payments 2 or 3. I've borne in mind what Kroo has said in response to my view. But it hasn't said anything which has made me change my mind.

Taking everything into account, I'm not persuaded that there's any good reason to depart from the findings I set out in my provisional decision

Putting things right

To put things right, Kroo Bank Ltd should:

- Refund £2,301.90, being 50% of payments 2 and 3; and
- Add simple interest at 8% per year to the refund from the date Miss S made the payments to the date of settlement.

If Kroo is legally required to deduct tax from the interest, it should provide a tax deduction certificate if Miss S asks for one, so that she can reclaim the tax from HMRC if appropriate.

My final decision

My final decision is that I uphold this complaint in part. I require Kroo Bank Ltd to put things right by doing as I've set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss S to accept or reject my decision before 10 September 2025.

Juliet Collins
Ombudsman