DRN-5951682

The complaint

Mr O is unhappy that Kroo Bank Ltd won't refund payments he made as part of a scam. He brings the complaint through professional representatives, but for simplicity I've referred to the actions of Mr O throughout the decision.

What happened

In November 2023 Mr O received unsolicited contact on an instant messaging service app by someone offering a job opportunity. The work was task based and involved reviewing films, in order to promote them by improving their ratings. The agent explained that you bought the tasks, and paid by depositing cryptocurrency onto the job platform, and earned commission (plus the cost of the task) back once completed. The company co-opted the name of a well-known search engine in order to imply affiliation.

Mr O was guided through setting up wallets at cryptocurrency exchanges, as well as opening and using existing accounts with firms that would easily allow payments to them – including ones with Electronic Money Institutions (EMIs) I'll call "W" and "R". He had held two accounts with a building society (I'll call "N") for a while, and that's where the funds sent to the scam originated from. Mr O opened an account with Kroo on 21 November 2023 and made four payments to a cryptocurrency provider, totalling just under £6,500. But all of those were returned to the account on 28 November 2023. Then the following day after the credits Mr O made two transfers (payments 5 and 6) to a different cryptocurrency exchange, I'll call "B", for £3,000 and £3,450.

On 2 December 2023 Mr O made three further payments to B – for £50, £1,500, and then payment 9 for £16,000. The final disputed transaction (also to B) was two days later, and for £4,800. Kroo didn't intervene on any of the payments. W asked Mr O for the purpose of some of the peer-to-peer cryptocurrency purchases, and he selected he was paying friends and family. Mr O spoke to R via its chat function about the first payment made from that account, and he gave the name of the company he was working for along with quite a few details about the job opportunity. R also later completed an automated check where 'investment' was the reason chosen and the warnings presented were related to that scam risk. Our investigator concluded R ought to have been able to uncover the scam from the first transaction, and that outcome has been provisionally accepted by the parties.

As the scam went on, the tasks started to become more expensive, and Mr O had to deposit significant amounts of cryptocurrency in order to buy them. He then didn't have enough money and couldn't purchase the tasks needed to compete a set. Mr O says he realised it was a scam when he couldn't withdraw his funds from the job platform and was given repeated excuses for why he needed to make further payments. He contacted the firms involved to report what had happened, including Kroo, but none of the funds could be recovered. Kroo asked Mr O some questions about the circumstances, after receiving notice of disputed payments from N, but didn't hear back – and so closed the account.

Mr O raised a complaint with Kroo in 2024, that said the account activity was out of character and should have prompted fraud interventions. He thought the loss would have been prevented had appropriate checks been carried out. The final response said it did find the

payments concerning, but they didn't trigger a review or raise any alarm in its system. Kroo explained that could be for various reasons, including the amounts not exceeding a certain limit or the recipient account not being flagged as suspicious. The bank therefore didn't think it wasn't liable in the circumstances. Mr O wasn't happy with the response and so referred the complaint to the Financial Ombudsman Service for review.

One of our investigators considered the complaint and didn't recommend it should be upheld. In his view, Kroo couldn't have reasonably prevented the loss – as he believed Mr O was being guided by the scammer on how to bypass the interventions from the various firms involved. So the investigator believed he would have got through Kroo's questioning without raising concerns, even if it had completed checks. The investigator added that if Kroo had refused the payments he thought Mr O would have still got the funds to the scammer through one of his other accounts elsewhere.

Mr O didn't accept the investigator's opinion, and requested an ombudsman reconsidered the matter. So the complaint was passed to me to decide. I issued a provisional decision upholding the complaint, and I've copied below the part of that outlining my rationale for the outcome:

"In broad terms, the starting position in law is that a payment services provider is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the terms and conditions of the account and the Payment Services Regulations (PSR's). Mr O 'authorised' the transactions in question (he made them), albeit under the belief they were for a legitimate job opportunity. So Kroo was under an obligation to process the payments – but that isn't the end of the story, as far as its responsibility in the matter goes.

While that's the starting position, I've also taken into account the regulator's rules and guidance; relevant codes of practice, along with what I consider to have been good industry practice at the time. I've also applied Kroo's terms for the account, which say it may require customers to take a number of steps to authorise a payment in order to limit fraud. Those together mean I consider Kroo should fairly and reasonably have been on the lookout for the possibility of fraud at the time, and intervened if there were clear indications its customer might be at risk.

Kroo has a difficult balance to strike in how it configures its systems. It needs to detect unusual activity, or activity that might otherwise indicate a higher than usual risk of fraud, whilst not unduly hindering legitimate transactions. There are many millions of payments made each day, and it would not be possible or reasonable to expect firms to check each one. In situations where firms do (or ought to) carry out checks, I would expect that intervention to be proportionate to the circumstances of the payment. Kroo didn't intervene prior to processing any of the disputed transactions. So the initial question for me to decide is whether any of the payments ought to have looked concerning enough to have prompted fraud checks.

Firstly, I should explain that these payments aren't covered by the CRM code. Kroo didn't sign up to that voluntary scheme, and it didn't apply to payments made to accounts in the customer's own name (which is the case here) or cryptocurrency transactions. So Mr O would only be entitled to a refund if Kroo made a mistake when putting them through (for example, if it didn't act on clear indications he was falling victim to a scam).

The initial payments sent to a cryptocurrency provider on 21 November 2023 weren't large enough to arouse concern – but the fourth one that day ought to have prompted an intervention from Kroo. It was a high value payment (£5,420) on a newly opened account, and Kroo should have known from the sort code that the destination was related to one of the world's largest providers of cryptocurrency – so it should have identified Mr O was at

increased risk of financial harm from fraud. That means it should have asked some automated questions before allowing the transfer, to narrow in on the type of scam Mr O might be at risk from – and provided a warning off the back of the answers.

Kroo should have known the scam risk involved cryptocurrency, but it wouldn't have known Mr O was falling for a job scam – unless his automated answers indicated that. I appreciate I'm speculating on what might have happened if Kroo had intervened proportionately, but we have some information to go on based on his interactions with W and R. During the automated interventions at both of those firms Mr O didn't select the most appropriate options about the purpose, because he was following the scammer's instruction on how to answer. So I'm not persuaded he'd have answered Kroo's questions in a way that would have led to a warning that resonated with his circumstances. Therefore I don't think Kroo could have prevented the loss from that point.

Two large payments were sent to another cryptocurrency provider on 29 November. Kroo has said it only knew they were going to an account at payment processor (that provides business to business services), but it was seemingly B's client account with that processor – again, B is one of the largest cryptocurrency exchanges in the world – so I'm surprised Kroo wasn't able to detect that. We asked Kroo for its input on why it wasn't possible to identify the recipient account was cryptocurrency related, but it didn't reply. There was a gap of over a week between the last batch of payments sent though, and those were returned to the account. An obvious scam pattern hadn't formed by the second one on 29 November 2023 either. So, at most I'd have expected another warning to be shown that day (which I don't think would have worked to uncover the scam, for the same reasons I gave earlier).

But things escalated significantly on 2 December 2023 – with three payments of increasing size going to cryptocurrency, culminating in the one for £16,000. Even if Kroo didn't know the destination was cryptocurrency related, it should have been concerned by the size and clear scam pattern (payments sent in a short timeframe for escalating amounts) on a new account, to a new payee – and intervened to ask questions. I consider the risks were great enough by that point to warrant an intervention from an agent at the bank prior to payment 9 (for £16,000), so that tailored and probing questions could be asked about the circumstances behind it.

Having read through the chats with the scammer, Mr O was being closely guided through buying and loading cryptocurrency onto the job platform. I've also mentioned that at points he didn't select the best option available when asked the purpose of payments during automated processes elsewhere. Mr O was told by the scammer was told not to share with Kroo that the payments were for cryptocurrency, as it supposedly didn't allow them (though that restriction didn't come in until 2024) – but he wasn't provided with an elaborate cover story. He was honest during the only time he actually spoke to one of the firms (R), and shared the details of the company and job opportunity when questioned – which clearly indicated it was scam. So it's difficult to know exactly how forthcoming he would have been during the call.

Even if Mr O had tried to obscure what he was doing though, the pattern and other risk factors surrounding the payments were so indicative of a scam that I don't think it would have been reasonable to take any explanation on face value. Kroo would have needed to be alive to the fact that scammers provide victims with cover stories, and have been interested in seeing something to corroborate what he was doing at those other firms that he couldn't do from his Kroo account. It would also have seen the prior cryptocurrency transactions on the account, which bounced back, and that would have been a strong indication that these payments might also be cryptocurrency related.

If Mr O had said it was just another account of his elsewhere, then that wouldn't explain why

he was sending funds through his Kroo account, from his one at N – or why he was sending them in this pattern. I don't consider there was a reasonable explanation for the payments that would have satisfied Kroo he wasn't at risk, even with the scammer's support – so I think the bank would have at least wanted to see confirmation the destination account was under his control (which would have revealed he was buying cryptocurrency). I think at that point Mr O would have had to come clean about what he was doing, or risk the funds being frozen – but I'm not persuaded anyway that he would have been motivated to mislead Kroo to that extent. He believed the job opportunity was legitimate, and so wouldn't have thought he needed to hide what he was doing, and Kroo had allowed cryptocurrency related transactions to go through already (contrary to what the scammer had told him).

Once aware of the underlying reasons for the payments, Kroo would have quickly worked out what was happening – as the circumstances were typical for a job scam (initial contact out of the blue, no employment contract, tasks becoming increasingly expensive, paying for them upfront in cryptocurrency etc). I haven't seen anything to suggest Mr O wouldn't have been receptive to a good intervention and clear warning – he wasn't completely under the scammer's spell either (the chats show him questioning what he's told). Even if he needed some persuading then Kroo could have asked him to try and withdraw all his funds from the platform, which he wouldn't have been able to do – and that's what eventually alerted him to the fraud.

Overall, I'm confident a proportionate intervention prior to payment 9 would have likely prevented any further loss. I'm conscious that the funds originated at N, who also had a responsibility to monitor for signs Mr O was at risk of financial harm from fraud. I've considered that complaint separately, and have concluded it has liability in the matter too. N also should have prevented the loss of the funds resulting in the last two payments from Kroo (9 and 10), so both firms will share responsibility for any refund of those – subject to the below consideration of Mr O's role in the loss.

I've thought about whether Mr M should bear any responsibility for his loss. In doing so, I've considered what the law says about contributory negligence, as well as what I consider to be fair and reasonable in all of the circumstances of this complaint. That includes taking into account Mr M's own actions and responsibility for the losses he has suffered. I recognise that there were sophisticated aspects to this scam, including a professional looking platform for the tasks and an onboarding process that would have added to the legitimacy. Mr O was able to withdraw a small amount of commission from the first set of tasks, which would have been reassuring. He was also added to a group chat with other 'employees', which would have been persuasive, and I don't doubt the social engineering or manipulation skills of the scammer.

But there were some obvious red flags to the opportunity, that I think ought to have been spotted – even if unfamiliar with this type of remote working. The initial contact was out of the blue and on an instant messaging app, which isn't how recruiters would usually make contact – and Mr O says he hadn't uploaded his CV recently, nor was he looking for work. So the approach should have struck him as odd and he should have proceeded with some scepticism. Then the work itself should have prompted further questions, as he was supposedly reviewing films, but not watching them – and getting paid quite a lot for what was essentially clicking a few buttons. Mr O was also having to pay large sums upfront before earning anything, which isn't a traditional model of employment – and he was buying tasks plus getting paid in cryptocurrency, which was unusual at best. Those were clear red flags. By the time I've said Kroo should have uncovered the scam Mr O was paying thousands of pounds for each review, and that ought to have seemed implausible as a job opportunity – as not many could afford to do it.

I know the scammer directed Mr O in what he should select during the automated

processes, but the reasons given for hiding what he was doing didn't really add up – so needing to lie should have struck him as odd. So I've also considered that Mr O could have been clearer with his automated answers to R and W, which might have led to warnings that resonated with him and helped prevent some of the loss. He has mentioned that he was vulnerable at the time, having lost his father recently – and I was sorry to hear that. Kroo wasn't aware of his circumstances though, and I haven't seen any obvious indication that it was impacting his judgement. Mr O didn't mention it when reporting matters either, even though he was directly asked about any factors affecting him. So I think there were steps he could have taken to protect himself, and red flags that were missed – and I'm not persuaded he couldn't have mitigated the risks involved. Therefore I've decided Mr O should fairly share responsibility for the loss – and I plan to apply a 50% deduction to the refunds of the transactions I consider the firms shouldn't have processed.

I don't think the deduction made to the amount reimbursed to Mr O should be greater than 50%, taking into account all the circumstances of this case. I recognise that Mr O did have a role to play in what happened, and it could be argued that he should have had greater awareness than he did that there may be something suspicious about the opportunity. But I have to balance that against the role that Kroo, a firm subject to a range of regulatory and other standards, played in failing to intervene proportionately. Mr O was taken in by a cruel scam – he was tricked into a course of action by a fraudster and his actions must be seen in that light. I do not think it would be fair to suggest that he is mostly to blame for what happened, taking into account Kroo's failure to recognise the extent to which he was at risk of financial harm from fraud, and given the degree to which I am satisfied that a business in Kroo's position should have been familiar with a fraud of this type. Overall, I remain satisfied that 50% is a fair deduction to the amount reimbursed in all the circumstances of the complaint.

I've thought about whether Kroo ought to have done more when alerted to the fraud and I've decided it couldn't have. Recovery wouldn't have been an option, as the funds were converted into cryptocurrency at the beneficiary account shortly after the disputed transactions and sent onto the scammer. I also haven't seen any customer service issues that I consider would warrant an award – and the interest applied to the redress should compensate Mr O sufficiently him for the time he was deprived of use of his funds."

Mr O accepted my provisional findings. Kroo didn't agree, and in summary raised the following points:

- Kroo offers accounts with attractive interest rates, meaning many of its customers use them for savings rather than day to day spending. So it's not uncommon for customers to transfer significant sums into their Kroo accounts, and then move them onto other institutions in the pursuit of better rates elsewhere, often after periods of relatively low activity.
- Mr O indicated when opening the account that he intended to use it for receiving and withdrawing funds – and that his source of income was investments. That meant Kroo considered the pattern of large outbound payments from his account weren't anomalous or unexpected.
- The payments were sent to an account in his name (full Confirmation of Payee match) and under his control – as evidenced by the chats with the scammer.

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, and bearing in mind the responses I had to my initial findings, I've still

decided to uphold Mr O's complaint in part – and for the same reasons I gave in my provisional decision. I've carefully considered the further points raised by Kroo, but I've not been persuaded to depart from the outcome I set out above. I'll explain why.

Kroo has provided some helpful insights into the expected or typical use for it's accounts, in order to explain why these payments wouldn't have seemed unusual. It says customers often use them as savings vehicles, and so large outbound payments (after a period of inactivity where the funds have sat there) isn't unexpected – and that modelling fit Mr O's anticipated usage based on the information gathered during the opening process. But that's not what happened here.

Mr O didn't deposit money and then leave it there to earn interest before making large outbounds payments to take advantage of interest rates elsewhere. Instead, immediately after opening, he started washing his money (under the scammer's direction) through the account to cryptocurrency, starting with small payments that escalated in size over a number of days. At no point did the activity on the account match what Kroo says it anticipated – and I've set out in detail the reasons why I consider the pattern clearly indicated Mr O was potentially falling for a scam on 2 December 2023.

I'm not certain of the point Kroo is making when it says the payments went to cryptocurrency wallets Mr O set up and controlled – that's never been in dispute. The fact that the payments were going to another account in his name didn't mean they weren't fraud related, these actually strongly indicated he was falling victim to multistage fraud (where victims are persuaded to move money through one or more accounts in their name before being lost). We've seen a huge rise in this type of fraud over the last few years, particularly involving cryptocurrency, and no doubt Kroo will be fully aware of it given its prevalence.

Cryptocurrency transactions carry a heightened risk when occurring like this, and Kroo should fairly and reasonably have been on the look out for signs its customer might be falling for a multistage scam involving them. I've found the bank failed to intervene proportionately in this case and that's what resulted in the loss here. So I maintain it's fair that Kroo (along with the firms involved) and Mr O share responsibility for the payments that shouldn't have been allowed.

Putting things right

In order to put things right, Kroo Bank Ltd should:

- Refund 25% of payments 9 and 10 (25% to be covered by N and a 50% deduction for Mr O's contributory negligence).
- Apply 8% simple interest yearly to the refunds, calculated from the date of the transactions until the date of settlement.

If Kroo considers that it's required by HM Revenue & Customs to deduct income tax from that interest, it should tell Mr O how much it's taken off. It should also give him a tax deduction certificate if he asks for one, so he can reclaim the tax from HM Revenue & Customs if appropriate.

My final decision

I've decide to uphold Mr O's complaint against Kroo Bank Ltd, and direct the bank to settle the complaint in line with what I've set out above, under the 'putting things right' heading.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr O to accept or reject my decision before 12 December 2025.

Ryan Miles
Ombudsman