DRN-5612035

The complaint

Mr W complains that Kroo Bank Ltd (Kroo Bank, hereinafter) hasn't refunded the losses he's incurred when falling victim to an investment scam.

What happened

The facts are well known to both parties, so I have outlined the key details. In summary, Mr W found the scam via a social media platform in the summer of 2024. It was advertised as being endorsed by a TV personality and businessperson, which caught Mr W's attention.

Mr W expressed his interest and was later contacted by the scammer, who introduced him to a fake online investment platform and persuaded him to open a bank account with Kroo Bank, as well as two cryptocurrency wallet providers, that I'll refer to as B and I, to send the payments to the scammer.

Mr W funded the scam through his savings that he held at another bank account with a firm I'll refer to as Bank A. Towards the end of the scam, when Mr W ran out of funds, he was persuaded to apply for several loans to continue meeting the scammer's demands for payment in order to withdraw his returns.

From his Kroo Bank account Mr W made the following payments:

Payment #	Date	Time	Type of transaction	Amount
1	18 July 2024	19.47	Card payment to B	£1,590.60
2	20 July 2024	13.27	Card payment to B	£2,001.58
3	25 July 2024	21.00	Card payment to B	£2,004.76
4	25 July 2024	21.08	Card payment to B	£1,493.55
5	30 July 2024	21.29	Card payment to B	£3,599.89
6	1 August 2024	15.09	Card payment to B	£3,959.02
7	2 August 2024	16.10	Card payment to B	£5,015.45
8	2 August 2024	19.25	Card payment to B	£4,968.52
9	2 August 2024	22.01	Faster payment to I	£5,000
10	5 August 2024	15.56	Card payment to B	£5,006.50
11	5 August 2024	17.38	Card payment to B	£4,971.63
12	6 August 2024	14.15	Card payment to B	£5,020.35
13	6 August 2024	14.34	Faster payment to I	£5,000
14	6 August 2024	21.27	Faster payment to I	£5,000
15	6 August 2024	21.32	Faster payment to I	£5,000
16	7 August 2024	16.12	Card payment to B	£5,006.90
17	7 August 2024	16.17	Faster payment to I	£5,100
18	8 August 2024	15.36	Faster payment to I	£5,000
19	8 August 2024	-	Faster payment to I	£5,200
20	8 August 2024	19.37	Card payment to B	£5,037.18
21	9 August 2024	-	Faster payment to I	£5,000
22	9 August 2024	15.50	Card payment to B	£5,036.27

23	13 August 2024	-	Faster payment to I	£5,000
24	13 August 2024	-	Faster payment to I	£5,000
25	14 August 2024	14.49	Faster payment to I	£5,000
26	14 August 2024	14.52	Faster payment to I	£5,000
27	15 August 2024	13.38	Faster payment to I	£5,000
28	15 August 2024	13.40	Faster payment to I	£5,000
29	15 August 2024	14.34	Card payment to B	£5,007.56
30	15 August 2024	16.58	Faster payment to I	£5,000
	15 August 2024	-	Two payments for £5,000 and 3,000 cancelled at Mr W's request	
			Total payments	**£135,019.76**

Mr W realised he had fallen victim to a scam when he independently contacted his cryptocurrency wallet provider to ask if it was normal procedure to pay so many withdrawal fees and tax payments to receive his investment returns, and he was told this was sadly a scam.

Mr W then reported the scam to Kroo Bank on 16 August 2024. Mr W didn't raise the scam or make a complaint to Bank A.

Kroo Bank said all of the payments had been authorised by Mr W and the bank had appropriately intervened during the scam by telling Mr W to beware of social media scams and by reminding him that making cryptocurrency payments from its facilities was prohibited by its terms and conditions. It further said it could not initiate recovery procedures as these payments had been made to accounts in Mr W's name and control. So, it thought it had done enough to protect Mr W and declined to refund his losses.

So, Mr W referred the complaint to the Financial Ombudsman Service.

Our Investigator found that Kroo Bank should have intervened when Mr W made the fourth scam payment on 25 July 2024. However, they said that Mr W should also bear part of the responsibility for his loss, as he should have carried out more checks before investing such an amount of money and he should have picked up on the scam's red flags. So, our Investigator recommended liability for the losses should be shared equally. Our investigator originally miscalculated the net losses Mr W sustained, but this was rectified with both parties after Kroo Bank raised this issue.

Kroo Bank disagreed with our Investigator's view on the basis that the payments weren't identifiably going to cryptocurrency providers, so it could not be expected to intervene so early in the scam. Moreover, it said its warnings were appropriate in the circumstances, and Mr W would have been unlikely to take notice of any further warnings, as he was being heavily coached by the scammer and had already lied to Bank A about transferring funds for home improvements, as opposed to a cryptocurrency investment.

In light of this disagreement, I have been asked to review everything afresh and reach a decision on the matter.

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've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

I'm aware that I've summarised this complaint briefly, in less detail than has been provided, and in my own words. No discourtesy is intended by this. Instead, I've focused on what I think is the heart of the matter here. If there's something I've not mentioned, it isn't because I've ignored it. I'm satisfied I don't need to comment on every individual point or argument to be able to reach what I think is the right outcome. Our rules allow me to do this. This simply reflects the informal nature of our service as a free alternative to the courts.

Where the evidence is incomplete, inconclusive, or contradictory, I must make my decision on the balance of probabilities – that is, what I consider is more likely than not to have happened in the light of the available evidence and the wider surrounding circumstances. I've thought carefully about whether Kroo Bank treated Mr W fairly and reasonably in its dealings with him, when he made the payments and when he reported the scam, or whether it should have done more than it did.

Having done so and for the reasons I shall set out below, I consider Kroo Bank should, at the least, have provided a written warning specific to cryptocurrency investment scams prior to the fourth payment. If it had done so, I'm satisfied the scam and losses to Mr W from that payment onwards, would more likely than not have been prevented. But I am also satisfied that in the circumstances of this complaint, Mr W should bear some responsibility (50%) for the losses he suffered.

I have kept in mind that Mr W made the payments himself, and the starting position at law is that Kroo Bank is expected to process payments and withdrawals that a customer authorises it to make. So, under the Payment Services Regulations 2017 (PSR 2017) Mr W is presumed liable for the loss in the first instance.

I must also take into account that the basis on which I am required to decide complaints is broader than the simple application of contractual terms and the regulatory requirements referenced in those contractual terms. I must determine the complaint by reference to what is, in my opinion, fair and reasonable in all the circumstances of the case (DISP 3.6.1R) taking into account the considerations set out at DISP 3.6.4R.

So, considering the relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time – Kroo Bank should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.
- Have had 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). This is particularly so given the increase in sophisticated fraud and scams in recent years, which payment service providers are generally more familiar with than the average customer.
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or make additional checks, before processing a payment, or in some cases decline to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.
- Have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-

stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

- Have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so.

So, I've thought about whether the transactions should have highlighted to Kroo Bank that Mr W might be at a heightened risk of financial harm due to fraud or a scam.

Should Kroo Bank have intervened?

I'm aware that most cryptocurrency exchanges generally stipulate that the card used to purchase cryptocurrency at its exchange must be held in the name of the account holder, as must the account used to receive cash payments from the exchange. Kroo Bank would likely have been aware of this fact too. So, it could have reasonably assumed that the payments would be credited to a cryptocurrency wallet held in Mr W's name.

When Mr W made these payments, firms like Kroo Bank had been aware of the risk of multi-stage scams involving cryptocurrency. Scams involving cryptocurrency have increased over time. The FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018 and figures published by the latter show that losses suffered to cryptocurrency scams have continued to increase since. They reached record levels in 2022. During that time, cryptocurrency was typically allowed to be purchased through many high street banks with few restrictions.

By the end of 2022, however, many of the high street banks had taken steps to either limit their customer's ability to purchase cryptocurrency using their bank accounts or increase friction in relation to cryptocurrency related payments, owing to the elevated risk associated with such transactions. These restrictions – and the reasons for them – would have been well known across the industry.

So, taking into account all of the above, I am satisfied that around the time Mr W was making the scam payments, Kroo Bank ought fairly and reasonably to have recognised that its customers could be at an increased risk of fraud when using its services to purchase cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name.

To be clear, I'm not suggesting Kroo Bank should have more concern about payments being made to a customer's own account than those which are being made to third party payees. As I've set out in some detail above, it is the specific risk associated with cryptocurrency in early 2023 that, in some circumstances, should have caused Kroo Bank to consider transactions to cryptocurrency providers as carrying an increased risk of fraud and the associated harm.

So, in those circumstances, as a matter of what I consider to have been fair and reasonable, good practice and to comply with regulatory requirements, Kroo Bank should have had appropriate systems for making checks and delivering warnings before it processed such payments. And, as I have explained, Kroo Bank was also required by the terms of its contract to refuse or delay payments where regulatory requirements meant it needed to carry out further checks.

So, I've considered, at what point, if any, taking into account what it knew about the payments, Kroo Bank should have identified that Mr W might be at a heightened risk of fraud that warranted its intervention.

Kroo Bank has argued that B and I could not be deemed identifiable cryptocurrency providers, because of the Merchant Category Code (MCC, hereinafter) B was categorised under and because the payments to I appeared on its systems as going to another FCA regulated electronic money institution. I disagree with these arguments, and I think that both payees should have been recognised by Kroo Bank as identifiable cryptocurrency providers from the outset. I say this because the auditing information Kroo Bank provided our service with, shows that the MCC for B was "securities – brokers and dealers" which, along with its name and the information widely available about it online as of July 2024, should have clearly indicated to Kroo Bank that it was a cryptocurrency provider.

With regards to I, I also believe it should be categorised as an identifiable cryptocurrency provider, as the electronic money institutions it appeared as on Kroo Bank's systems is one of the most prominent digital assets payment service providers. So, I think Kroo Bank should have identified from the outset that these payments were going to cryptocurrency providers. I am mindful that Mr W had opened the account for the purpose of the scam and Kroo Bank didn't have any historic information about the account or what Mr W's typical usage was like.

So, at first, it wasn't in a position to know whether Mr W's activity was unusual or out of character – as it had nothing to compare it against. The individual or combined payments' value and their sequence wasn't suspicious enough, so I can't fairly say that Kroo Bank should have suspected that these payments might be part of a scam.

But I'm satisfied that Kroo Bank ought to have recognised that the fourth card payment made on 25 July 2024 carried a heightened risk of financial harm from fraud because:

- It was made only eight minutes after the previous payment, meaning the speed of payments was increasing;
- It was the fourth payment in a row that Mr W had made to a cryptocurrency provider in a week;
- The combined value of the fourth and third payment was over £3,000, which brought the total expenditure towards cryptocurrency since the start of the activity to well above £5,000.
- The pattern of payments indicated both that Mr W was quickly crediting the account before making cryptocurrency transactions and that the daily amounts being sent to cryptocurrency were steadily increasing – which are both very clear features of scams.

To be clear, I do not suggest that Kroo Bank should provide a warning for every payment made to cryptocurrency. Instead, as I've explained, I think it was a combination of the characteristics of this fourth payment (combined with those which came before it, and the fact the payment went to a cryptocurrency provider) which ought to have prompted a warning.

For the reasons I've set out above I'm satisfied that around the time Mr W was making these payments Kroo Bank should have recognised at a general level that its customer could be at increased risk of fraud when using its services to purchase cryptocurrency and, therefore, it should have taken appropriate measures to counter that risk to help protect him from financial harm from fraud.

How should Kroo Bank have intervened?

The evidence before me shows Kroo Bank didn't intervene at all at this point. But I think that proportionate intervention would have taken the form of a warning (whether automated or in

some other form) that was specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022.

The warning Kroo Bank ought fairly and reasonably to have provided should have highlighted, in clear and understandable terms, the key features of common cryptocurrency investment scams, for example referring to: an advertisement on social media, promoted by a celebrity or public figure; an 'account manager', 'broker' or 'trader' acting on their behalf; the use of remote access software and a small initial deposit which quickly increases in value.

I recognise that a warning of that kind could not have covered off all scenarios. But I think it would have been a proportionate way for Kroo Bank to minimise the risk of financial harm to Mr W by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

I accept that under the relevant card scheme rules Kroo Bank cannot delay a card payment, but in the circumstances of this case, I think it is fair and reasonable to conclude that Kroo Bank ought to have initially declined the fourth payment in order to make further enquiries and with a view to providing a specific scam warning of the type I've described. Only after that scam warning had been given, if Mr W attempted the payment again, should Kroo Bank have made the payment.

Kroo Bank argued that it provided appropriate warnings to Mr W when it told him he couldn't complete cryptocurrency payments from its facilities and when it warned him about social media scams. However, having reviewed those interactions, I'm not persuaded they were either tailored to Mr W's circumstances or proportionate to the scam risks that ought to have been identified at that point.

This is because the warning about using Kroo Bank for cryptocurrency payments wasn't given to protect Mr W from any specific risks but simply to inform him that cryptocurrency payments were outside of the bank's risk appetite; and the social media warning had nothing to do with investment scams, but rather with impromptu request for financial help on social media channels. So, I don't think that Kroo Bank did enough to protect Mr W with those warnings nor do I believe Mr W could have realised he was being scammed thanks to them.

Would Kroo Bank's intervention have made a difference?

The question for me to answer next is whether, on the balance of probabilities, Kroo Bank would have been able to prevent Mr W's further losses, had it intervened at that stage of the scam.

I've considered that point carefully and on the balance of probabilities, I think it would have. I think that a warning of the type I've described would have identified to Mr W that his circumstances aligned with an increasingly common type of scam.

In coming to this conclusion, I've given serious consideration to the fact that Mr W was untruthful in his dealings with Bank A and the five loan providers he borrowed from in order to make payments to the scammer.
However, I don't think those interactions can dictate how Mr W would have reacted to a proportionate warning from Kroo Bank and whether the scam would have been unveiled. I say this because of the following reasons:

- Firstly, our service has received a full copy of the scam chat transcripts and there's no evidence on there that the scammer heavily coached Mr W on what to say if Kroo Bank had intervened on any of the payments. I think this is a crucial consideration

here because Mr W could not have told Kroo Bank that he was making cryptocurrency payments for home improvements, just as he did with the loan providers and Bank A, because that would not have made conceptual sense.

- Even if Mr W had taken steps to disguise the genuine reasons for payment, this would have been a clear red flag indicating to Kroo Bank that something may be amiss. Given Mr W's age, his understanding of cryptocurrency and the fact he wasn't an experienced investor, I think Kroo Bank would have very easily realised Mr W had unfortunately fallen victim to a scam, had it meaningfully engaged with him – which I would have expected it to do, had Mr W's answers not made conceptual sense.
- Kroo Bank argued that Mr W would have taken steps to disguise the genuine reasons for payment and disregard its advice, but I don't agree this would have been the most likely occurrence. The interactions transcripts between Kroo Bank and Mr W show Mr W didn't hide that he was making cryptocurrency transactions, and to date no evidence has been provided by Kroo Bank proving that Mr W took active steps to mislead the bank. On 2 August 2024 Mr W contacted Kroo Bank to understand whether the email he had allegedly received from it prohibiting his cryptocurrency returns from being deposited into Kroo Bank was genuine. Sadly, that email had been spoofed by the scammer to persuade Mr W to pay more fees and taxes to have his dividends paid to him. Kroo Bank didn't identify this and simply referred Mr W back to its policy decision to not facilitate cryptocurrency transactions any longer. I think this interaction demonstrates that Mr W was trying to communicate with Kroo Bank about what was happening and verify whether the emails and requests for payment he was receiving were genuine ones, which persuade me that, more likely than not, he would have been responsive to the bank's intervention.
- This is further supported by the fact that the chat transcripts reveal Mr W was doubtful about the scam from early on, and, whilst the scammer skillfully won his trust back, I think that Mr W would have been receptive to Kroo Bank's warning, had it been tailored to his circumstances.
- Moreover, it's also important to note that it was only towards the end of the scam that Mr W was forced to take out loans and lie to Bank A about the true nature of his transfers, because he'd ran out of money and was desperate to get his investment back. The loan providers would not have lent him money towards a cryptocurrency investment, which forced Mr W to give a different loan purpose due to the predicament he had found himself in. So, I think it was desperation, as opposed to being fully under the scammer's spell, that dictated Mr W's actions at that specific point of the scam, which means it would be unfair to draw the conclusion that Mr W would have definitely lied to Kroo Bank at a much earlier point in the scam where he had not completely exhausted his funds.
- It was ultimately thanks to Mr W's efforts that the scam was unveiled, after he contacted HM Revenue & Customs and his cryptocurrency wallet provider to verify if the requests for payments genuinely came from them, and after he tried to meet the scammer in person at their offices. This makes me believe that Mr W was actively looking for evidence of whether this was a genuine investment or a scam and that he would have taken heed of Kroo Bank's warning, if it had guided him on how to discern a genuine opportunity from a fraudulent one.

Based on the above findings, I believe that, on the balance of probabilities, a proportionate intervention would have successfully broken the scammer's spell on Mr W and prevented his further losses.

Should Mr W bear part of the responsibility for his loss?

I've thought about whether Mr W should bear any responsibility for his losses from the fourth payment onwards. 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, including taking into account Mr W's own actions and responsibility for the losses he has suffered.

I recognise that, as a layman who claims to have little investment experience, there were aspects to the scam that would have appeared convincing. Mr W has recalled that the scammer and their company came across as very professional, with a genuine online presence and what appeared to be a genuine trading platform. I can see why the look and feel of a platform to access and manage profits could add further validation to the scam.

However, whilst I accept that Mr W conducted some very basic research on reliable online verification platforms very early on in the scam, he then proceeded to take the scammer's advice and overall situation at face value. Had he delved deeper in his online research he would have found out that some one-star reviews about one of the cryptocurrency providers he was asked to use were widely available, suggesting that the cryptocurrency provider had been amply exploited by scammers in other instances.

Although I accept it is possible to make significant profits when investing in cryptocurrency, I also think Mr W should have questioned the plausibility of the developing situation, especially when he faced difficulties withdrawing the alleged profits and the scammer hadn't advised him about needing to meet those costs beforehand.

The returns Mr W thought he had made after having made a very small initial investment were wholly unrealistic and Mr W didn't take any independent steps to verify whether those numbers could amount to a legitimate return in the circumstances. I would have expected Mr W to conduct such checks, especially as he told us he was very inexperienced about investments and cryptocurrency.

Moreover, I would have expected Mr W to attempt to withdraw his returns before committing to much larger payments, to prove that the investment was a genuine one.

Finally, I believe that Mr W should have realised that no genuine account manager would have advised him to lie to his bank and to loan providers in order to continue making payments to the investment.

Looking at the circumstances, I think Mr W should have, on the balance of probabilities, realised there was a possibility the situation was not genuine and acted accordingly, much earlier than he did. As such, it would not be fair to require Kroo Bank to compensate him for the full amount of his losses.

I've concluded, on balance, that it would be fair to reduce the amount Kroo Bank pays Mr W in relation to the payments he made from the fourth payment onwards because of his role in what happened. Weighing the fault that I've found on both sides, I think a fair deduction is 50%.

Recovery

The payments were made by debit card and faster payment to two separate cryptocurrency providers.

Mr W sent that cryptocurrency to the fraudsters from both wallets. So, Kroo Bank would not have been able to recover the funds as none would have remained in the wallets.

In addition, with regards to the debit card payments, I don't consider that a chargeback would have had any prospect of success given there's no dispute that B provided cryptocurrency to Mr W, which he subsequently sent to the fraudsters.

So, I don't think it would be fair and reasonable to conclude that Kroo Bank should have done anything more to try and recover Mr W's funds.

Putting things right

To put things right, Kroo Bank Ltd should now:

- Pay Mr W 50% of the payments he made from the fourth payment onwards – a total of £64,711.41.
- Pay 8% simple interest per annum on £64,711.41 from the date of each payment to the date of settlement*

I consider that 8% simple interest per year fairly reflects the fact that Mr W has been deprived of this money and that he might have used it in a variety of ways.

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

My final decision

For the reasons given above, I uphold this complaint in part and require Kroo Bank Ltd to pay Mr W as I have set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr W to accept or reject my decision before 4 February 2026.

Daria Ermini
Ombudsman