

## The complaint

Mr K complains that Wise Payments Limited (“Wise”) won’t refund money he lost when he was a victim of a scam.

## What happened

The background of this complaint is well known to both parties, so I’ll only refer to the key events here.

In February 2024, Mr K received a telephone call from a person, that we now know to be a scammer, that introduced themselves as being a representative of a genuine cryptocurrency provider, which I will refer to as ‘X’. The scammer said he was calling Mr K to help him recover bitcoin assets he had previously invested.

Mr K said he felt the call was genuine as he did have bitcoin assets in a dormant account with X, which he was unable to access as he had forgotten his login details. The scammer then told Mr K he would receive contact from another firm, which I will refer to as ‘F’, who will help him get his bitcoin investment released. An advisor from F then convinced Mr K to open an account with Wise which would be used to receive the funds once the bitcoin was released. Mr K then said F told him he would need to make a series of payments to release the bitcoin.

Mr K made payments from his Wise account to genuine crypto providers (as shown below before forwarding it on as part of the scam:

| Payment | Date             | Type         | Payee                     | Amount    |
|---------|------------------|--------------|---------------------------|-----------|
| 1       | 26 February 2024 | Card payment | Cryptocurrency provider 1 | £4,296.09 |
| 2       | 1 March 2024     | Card payment | Cryptocurrency provider 1 | £4,215.59 |
| 3       | 1 March 2024     | Card payment | Cryptocurrency provider 1 | £4,386.81 |
| 4       | 1 March 2024     | Card payment | Cryptocurrency provider 1 | £3,354.71 |
| 5       | 1 March 2024     | Card payment | Cryptocurrency provider 2 | £3,296.75 |
| 6       | 7 March 2024     | Card payment | Cryptocurrency provider 1 | £944.18   |
| 7       | 7 March 2024     | Card payment | Cryptocurrency            | £4,206.11 |

|   |              |              |                           |           |
|---|--------------|--------------|---------------------------|-----------|
|   |              |              | provider 2                |           |
| 8 | 7 March 2024 | Card payment | Cryptocurrency provider 1 | £3,433.28 |
| 9 | 7 March 2024 | Card payment | Cryptocurrency provider 1 | £1,712.35 |

Mr K has also raised a complaint against his other banking providers, that I will refer to as 'B' and 'H' that were involved as part of the scam. I will address Mr K complaint about H, which has been brought to the Financial Ombudsman, separately.

Around late April / early May 2024, Mr K said he realised he had been a victim of a scam and reported the incident to Action Fraud and his other banking providers involved. Mr K has confirmed he has received a refund from B for some of the payment she made from that account.

Wise agreed to a partial refund. In summary, they told the Financial Ombudsman:

- They are not Mr K's primary financial provider, so they do not have access to his income or savings information to determine whether the amounts he sent was significant in proportion to funds he holds.
- They deactivated Mr K's account due to concerns regarding him being a potential scam victim, to prevent any further high-risk payments being made and ensure the safety of his funds.
- They completed the card payments as directed and therefore fulfilled their contractual obligations.
- When Mr K set up the first payment to the first crypto exchange, they informed him it could be a scam, and that recovery of funds in case of fraud would be difficult and offered to cancel the transaction. However, Mr K wanted to go ahead with the payment.
- They accepted their safeguarding measures fell short of the standards they uphold, and they recognise more could have been done to prevent the payments. Therefore, they have agreed to partially uphold Mr K's complaint and refund him £8,474.10.

Mr K didn't agree to the partial refund from Wise. Our Investigator thought the partial refund given by Wise was fair and so, she wouldn't be asking Wise to do anything else. She went on to say even though she felt Wise should have provided warnings to Mr K from Payment 1, based on the interactions Mr K had with Wise, B and H, she didn't feel any intervention would have made a difference, which would have resulted in the scam being uncovered. The Investigator also said she wouldn't be asking Wise to provide 8% simple interest on the refunded transactions as she wouldn't have recommended any refund, so the partial refund is more than fair. She also didn't think Wise could've done anything to recover Mr K's money – as chargebacks rules do not cover scams.

Mr K disagreed and so the matter has been passed to me to decide. In short, he's said:

- The warnings issued by B should not cloud/unduly affect the decision with Wise. The Wise complaint should be considered on the actions / inactions of Wise.

- Wise wouldn't have been aware of any warnings provided by B. And any warnings provided by B don't take away from Wise's obligations to their customers.
- The scam warning Wise issued an attempted £100 payment to cryptocurrency provider 1, which was declined, should have been provided for Payment 1. And this could have led to a different outcome.
- By not providing a warning on this, and other payments, Wise facilitated the success of the scammers.
- Wise hasn't provided any rational why Payment 1-3 were excluded from their partial refund.
- Not applying 8% simple interest to the refunded transactions is unfair as Wise didn't provide any scam warnings on any of the transactions.
- Overall, he accepts clear lapses of judgement with respect to dealings with B and H. But Wise didn't provide any warnings, and they didn't protect him as their customer from the scam.

If the payments took place under the new APP fraud reimbursement scheme, he would have received a full refund / compensation within 5 days from Wise.

### **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'm sorry Mr K has been the victim of a scam. But while I appreciate this has had a significant impact on him, I think Wise has acted fairly in refunding the amount they have. And so, for the reasons I'll explain, I don't think they need to take any further action.

In broad terms, the starting position in law is that an electronic money institute (EMI) – like Wise - is expected to process payments their customer authorises them to make. Here, it isn't disputed that Mr K knowingly made the payments from his Wise account. I appreciate Mr K was tricked by the scammer as he thought he was paying fees to ultimately get his dormant bitcoins released. Nevertheless, I'm satisfied the payments were authorised by Mr K. So, under the Payment Services Regulations 2017 and the terms of his account, Wise are expected to process the payments and Mr K is presumed liable for the loss in the first instance.

However, taking into account the regulatory rules and guidance, relevant codes of practice and good industry practice, there are circumstances where it might be appropriate for Wise to take additional steps or make additional checks before processing a payment to help protect customers from the possibility of financial harm from fraud.

Here, Wise has already accepted they could've done more to protect Mr K from the scam. Because of this, they decided to partially refund 50% of the transactions from Payment 4 onwards. Given Wise's admission in this respect, I intend to focus on whether Wise should also refund Payments 1-3 and if it is fair and reasonable for the amount refunded to Mr K to be reduced due to contributory negligence on his part.

As a result, I've considered whether Wise should have done more to prevent Mr K from falling victim to the scam, as there are some situations where an EMI should reasonably have had a closer look at the circumstances surrounding a particular transfer. For example,

if it was particularly suspicious or out of character.

Mr K's Wise account had only recently been opened a couple of weeks prior to him making the first scam payment, so I'm mindful that Wise wouldn't have had any transaction history in which to compare Mr K's spending against to determine whether it was unusual. However, Wise have said before Mr K made Payment 1, he attempted to make a £100 payment to the same crypto exchange, which was declined by Wise and he was provided with the following message:

***"Protect yourself from scams***

*This could be a scam. It is hard to get your money back once you send it. If someone is pressuring you to make this payment or giving you investment advice, it is more likely this could be a scam.*

*Do you want to proceed with this transaction?"*

Wise have said Mr K selected 'Yes', *I still want to proceed* which meant the next payment to a crypto exchange would be allowed to go through. Wise have said if he had selected 'No', I don't want to proceed' his card would have been automatically frozen.

I appreciate there is a balance for Wise to find between allowing customers to be able to use their account and questioning transactions to confirm they are legitimate. Here, Payments 1-3 were made to a legitimate crypto exchange, which carries a known fraud risk as crypto scams like this have unfortunately become more prevalent. And although many individuals do invest in crypto legitimately, due to the large credits received on a fairly new account and the large debits being made shortly after to a crypto exchange, I do think Wise should have intervened before processing the payments – particularly because of the associated risks with crypto related transactions (including multi-stage fraud) that are well known to Wise. And so, I think it would've been reasonable for Wise to have taken additional steps before processing these payments.

I've thought carefully about what a proportionate warning in light of the risk presented would be in these circumstances. In doing so, I've taken into account that many payments that look very similar to these payments will be entirely genuine. I've also given due consideration to Wise's duty to make payments promptly, as well as what I consider to have been good industry practice at the time the payments were made. Taking that into account, I think Wise ought, to have provided a warning that was specifically about the risks of crypto investment scams. In doing so, I recognise that it would be difficult for such a warning to cover off every permutation and variation of crypto scams, without significantly losing impact. This would've been an effective way for Wise to limit the harm caused by crypto transactions to their customers. And the warning Wise ought fairly and reasonably to have provided should have highlighted, in clear and understandable terms, the key features of common crypto 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've thought carefully about whether such a warning would've resonated with Mr K, and to the extent whereby he wouldn't have proceeded with making the payments. Having done so, I don't think it would. This is because the most common features of crypto investment scams – which, as per above, I would've expected Wise to have highlighted – wouldn't have been relevant to Mr K's circumstances. Mr K wasn't making the payments for investment purposes, nor did he come across the opportunity through an advertisement on social media. And while there was a third party that had guided him on what he would need to do to

get his bitcoin assets released, they weren't acting on his behalf.

I've also listened to calls Mr K had with both B and H, before, during and after the scam payments he made from his Wise account.

Mr K had two phone calls with B on 30 January 2024, and 26 February 2024 before he made Payment 1. Call one (on 30 January 2024) lasted around 25 minutes, which involved B calling Mr K regarding a recent scam he had fallen victim to. The advisor went on to explain that it is very likely he would be targeted again and by the same scammers. So, B was keen to explain what kind of tactics the scammers use. And they mentioned the scammers would call him pretending to be from recovery companies, that specialise in helping customers recover lost crypto. The advisor went on to explain the whole process the scammers generally tend to use, which was very similar to the scam Mr K fell victim to.

On the second call, which took place shortly before Payment 1 was made, Mr K called B and said a payment he was trying to make to his Wise account had been blocked. The advisor explained the payment was blocked due to its high value. Mr K informed the advisor *"he was making payments in stocks and shares which are regulated, so he doesn't want to keep calling the banks to verify payments"*. B went on to explain the checks were only being done to protect customers.

Mr K also had four calls with H several weeks after the payments he made from his Wise account. These payments were also going to fund the scam and were made to a different crypto provider than the ones Mr K used from his Wise account. H asked Mr K various questions before the payments were released including the following:

Halifax: *"Have you opened the wallet yourself? Or has anyone else helped you open it?"*

Mr K: *"No, no, it's my wallet and I have passwords for it and everything else"*.

Halifax: *"And no-one's helped you open it, no other third parties and no one else has access to it?"*

Mr K: *"No, no"*.

Halifax: *"What's happening with some of these is, the fraudster is claiming to be from the likes of these places and they'll take remote access to your computer and set up a digital wallet, you move the money into it and they pinch it"*.

Halifax: *"Have you received any calls from anyone pretending to be from another company? Did someone contact you about this opportunity?"*

Mr K: *"No"*.

Halifax: *"Why are you making the payment?"*

Mr K: *"sending money to my own crypto account and [I]wasn't being instructed to make the payments by anyone else"*

Across the calls Mr K was provided with various crypto investment scam warnings, as well as scam warnings about other types of scams that are common, such as impersonation scams, job scams etc.

I'm aware that Mr K doesn't think his interactions with B and H should absolve Wise's responsibilities – including protecting their customers from scams. But while I understand his

views on this, for me to find it fair and reasonable that Wise should refund Mr K requires more than a finding that Wise ought to have intervened. I would need to find not only that Wise failed to intervene where it ought reasonably to have done so — but crucially, I'd need to find that but for this failure, the subsequent loss would've been avoided.

That latter element concerns causation. A proportionate intervention will not always result in the prevention of a payment. And if I find it more likely than not that such a proportionate intervention by Wise wouldn't have revealed the payments were part of a fraud or scam, then I couldn't fairly hold it liable for not having prevented them from being made.

When considering this, I think it is fair and reasonable for me to take Mr K's interactions with B and H into account. This is because it gives me an idea of what would've most likely have happened if Wise had carried out the additional steps I would've reasonable expected.

In Mr K's case, while I think Wise should've taken additional steps before processing Payments 1-3, I'm not persuaded that even if they'd done this – whether in the form of a tailored written warning or reached out to discuss the payment further -it would've deterred Mr K from making the payments. I think the conversations Mr K had with B and Halifax demonstrate that he wasn't willing to disclose the true circumstances of why he was making the payments – specifically that a third-party recovery firm was directing him to make payments to release crypto held in a dormant account. So, even if Wise had contacted Mr K, I think it's he would've acted similarly – thereby preventing them from being able to uncover the scam and providing relevant warnings to his situation. I also don't think any scam warnings provided by Wise would've resonated with Mr K - particularly as Mr K received such a warning the day prior to the scam occurring from B. So, it should've been at the forefront of his mind and resonated enough with him to have realised the contact he received from X and F wasn't genuine.

Because of this, I don't think Wise's failure to provide such warnings led to Mr K suffering his loss.

I've considered Mr K's argument that he should receive 8% simple interest on the transactions Wise have refunded. However, as I don't agree the scam would have been uncovered, even if Wise had asked further questions about the payments, he has already been refunded more than I would've awarded. So, it wouldn't be fair for me to direct Wise to pay 8% interest in these circumstances.

I've also considered whether, on being alerted to the scam, Wise could reasonably have done anything to recover Mr K's losses, but I don't think they could. The only possible option for recovery here, given the payments were made by debit card, would have been for Wise to have attempted a chargeback against the payee – that being the crypto exchanges. But I don't think there would've been any prospect of success given there's no dispute that the crypto exchanges provided crypto to Mr K, which he – unfortunately - sent to the fraudsters.

I appreciate Mr K feels strongly that my decision is heavily influenced by warnings issued by B and H. However, I've considered all the interactions Mr K had with his banking providers to reach a fair outcome – which I think this is fair for the reasons I've explained. And although, I have a great deal of sympathy for Mr K and the loss he's suffered, it would only be fair for me to direct Wise to refund his loss if I thought they were responsible – and I'm not persuaded this was the case.

**My final decision**

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr K to accept or reject my decision before 28 August 2025.

Israr Ahmed  
**Ombudsman**