DRN-5591881

## The complaint

Mrs S complains that Wise Payments Limited ('Wise') won't reimburse the money she lost when she fell victim to a scam.

## What happened

Mrs S says that she saw a celebrity endorsed advert on social media about an investment opportunity. She clicked a link and shortly afterwards she received a call from someone who explained the investment that was with a company I'll call C. Mrs S made a payment of a little over £200 towards this investment using an external account. The following day, Mrs S received a message from someone who said she would be Mrs S' adviser. Mrs S didn't know at the time, but C was a fake company, and the financial adviser was a scammer.

Mrs S said she could quickly see on her account with C that she was making money. The scammer then told her that because she was a new customer, if she invested a further £3,000 C would pay £1,500 into her account. The scammer used a screen-sharing application to help Mrs S set up accounts with Wise and another electronic money institution (EMI), saying the accounts were needed to transfer Mrs S' money through. The £3,000 payment was then made from Mrs S' Wise account on 19 January 2023. Mrs S believed these funds were crediting her account with C.

Mrs S says that the scammer helped her to make further card payments from her Wise account to a cryptocurrency exchange (B) to verify her liquidity. I have set out all the transactions Mrs S made to B in the table below:

| Transaction | Date | Amount |
|---|---|---|
| 1 | 19/01/23 | £3,000 |
| 2 | 23/01/23 | £9,000 |
| 3 | 24/01/23 | £9,500 |
| 4 | 25/01/23 | £8,000 |
| 5 | 01/02/23 | £10,000 |
| 6 | 02/02/23 | £10,000 |
| 7 | 03/02/23 | £10,000 |
| **Total** | | **£59,500** |

Whilst Mrs S was aware of the payments, she says she didn't fully understand the position and thought they were being made to enable her to withdraw funds from B. Mrs S also received fake emails from the other EMI and from B.

Mrs S realised she was the victim of a scam when she was unable to withdraw her funds without making further payments.

Mrs S' appointed representative sent a letter of complaint to Wise at the end of January 2024. They said that Wise should have intervened when she made the first £3,000 payment

to B and, if it had done so, it would have recognised the hallmarks of a cryptocurrency investment scam.

Wise considered Mrs S' claim but didn't agree to reimburse her. It said all card payments were authorised and that as payments were to a legitimate cryptocurrency platform, and the account was newly opened, it had no idea of Mrs S' usual activity so it had no reason to be concerned. Wise also referred to its terms and conditions, which say it isn't responsible for losses that aren't foreseeable.

*Our investigation so far*

The investigator who considered this complaint didn't recommend that it be upheld. He didn't think Wise could have been expected to prevent the loss. This was because Mrs S' bank discussed transfers from her current account to the other EMI account she was supported to open. During these conversations Mrs S misled her bank about the reason for the payments. Mrs S' bank provided scam warnings that were relevant to the scam Mrs S was falling victim to, which she didn't heed. So, the investigator thought that any intervention by Wise wouldn't have made a difference.

Mrs S didn't agree with the investigator's findings and asked for a final decision. The main point made by Mrs S was that Wise should have intervened, asked open and probing questions, and held her answers up to a reasonable level of scrutiny – taking into account that scammers often coach their victims.

Mrs S went on to say that the intervention by her bank (referred to by the investigator) was insufficient and not a reflection of what would have happened if Wise had intervened appropriately. The reason Mrs S gave to her bank for a payment (to buy materials for a property) couldn't be used in any intervention by Wise, as Mrs S was paying a cryptocurrency provider. And Mrs S' representative said the scammer didn't give her a cover story.

The complaint was passed to me to decide. I intended to reach a different outcome to the investigator, so I issued a provisional decision on 8 May 2025 to explain why. In the "What I've provisionally decided – and why" section of my provisional 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.*

*In deciding what's fair and reasonable, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.*

*I'm sorry to hear that Mrs S has been tricked into making these payments. I understand she has lost a significant amount of money.*

*In broad terms, the starting position at law is that an Electronic Money Institution ("EMI") such as Wise is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account.*

*I consider that Wise should in January and February 2023 have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances.*

*Overall, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable that Wise should:*

- *have been monitoring accounts and any payments made or received to counter various risks, including 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 firms are generally more familiar with than the average customer;*
- *in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – (as in practice Wise sometimes does); and*
- *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.*

*Should Wise have recognised that Mrs S was at risk of financial harm from fraud?*

*It isn't in dispute that Mrs S has fallen victim to a cruel scam here, nor that she authorised the payments she made to her cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer).*

*I'm aware that 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. So Wise likely thought the transactions I have set out in the table above would be credited to a cryptocurrency account in Mrs S' own name.*

*But by the time these payments were made, firms like Wise had been aware of the risk of multi-stage scams involving cryptocurrency for some time. 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.*

*So, taking into account all of the above, I am satisfied that by the end of 2022, prior to the payments Mrs S made, Wise 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.*

*In those circumstances, as a matter of what I consider to have been fair and reasonable and good practice, Wise should have had appropriate systems for making checks and delivering warnings before it processed such payments. I don't think that the fact payments were going to an account held in Mrs S' own name should have led Wise to believe there wasn't a risk of fraud.*

*What did Wise do to warn Mrs S?*

*Wise say that it provided Mrs S with a warning that said:*

*"**Protect yourself from scams***

*This could be a scam. It's hard to get your money back once you send it – so first tell us what this transfer's for to get advice."*

*Mrs S chose the 'Sending money to myself' option and was given short warnings about safe account scams and being pressured to make a payment.*

*I'm not persuaded Wise's very generalised warnings went far enough to protect Mrs S.*

*What kind of warning should Wise have provided to Mrs S?*

*I've gone on to consider, taking into account what Wise knew about the payments, at what point, if any, it ought to have identified that Mrs S might be at a heightened risk of fraud. I've 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.*

*When Mrs S attempted to make payment one, I think Wise ought fairly and reasonably to have recognised there was a heightened possibility that the transaction was linked to a scam. Whilst Mrs S used the sending money to myself payment option, it was to an identifiable provider of cryptocurrency and was for a relatively large amount. In line with the good industry practice that I've set out above, I think a proportionate response to that risk would have been for Wise to have provided a tailored written warning.*

*I think that such a warning should have addressed the key risks and features of the most common cryptocurrency scams – cryptocurrency investment scams. The warning should have highlighted, in clear and understandable terms, the key features of these scams, for example referring to: an advertisement on social media, possibly 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.*

*By payment five I think a proportionate response to the risk presented would have been for Wise to have attempted to establish the circumstances surrounding the payment before allowing it to debit Mrs S' account. Mrs S had made a series of higher value payments that were going to an identifiable provider of cryptocurrency. I think it should have done this by, for example, discussing the payment further rather than providing an on-screen warning.*

*If Wise had provided warnings of the type described, would that have prevented the losses Mrs S suffered?*

*On balance, I'm satisfied that a written warning of the type described would have resonated with Mrs S and prevented her further loss. The key features of an investment scam were all present when she made the payment. The investment opportunity was supposedly celebrity endorsed and was advertised on social media, she had a broker or financial advisor acting on her behalf, remote access software was involved, and a small initial deposit quickly increased in value.*

*I appreciate that Mrs S later misled her bank about the reason for transferring funds to another EMI (on 2 February and 6 February 2023). But I'm not persuaded this means that Mrs S wouldn't have heeded an appropriate warning from Wise on 19 January. I say this because when Mrs S made payment one it was very early in the scam and related to the investment itself rather than to withdrawing her funds. So, the scammer hadn't had the opportunity to build trust and wasn't telling her she'd lose all her money if she didn't follow their instructions. The payment was also made before Mrs S received fake emails from the other EMI and from B.*

*I haven't seen any evidence that Mrs S was given a cover story to share with Wise and don't think she would have risked losing her money.*

*As I think that a written warning when payment one was made would have prevented Mrs S' loss I see no merit in considering the impact of further intervention at a later point.*

*Is it fair and reasonable for Wise to be held responsible for Mrs S' loss?*

*In reaching my decision about what is fair and reasonable, I have taken into account that Mrs S purchased cryptocurrency which credited a wallet in her own name, rather than making a payment directly to the fraudsters. So, she remained in control of her money after she made the payments from her Wise account, and it took further steps before the money was lost to the fraudsters.*

*But as I've set out in some detail above, I think that Wise still should have recognised that Mrs S might have been at risk of financial harm from fraud when she made payment one, and in those circumstances it should have declined the payment and made further enquiries. If it had taken those steps, I am satisfied it would have prevented the losses Mrs S suffered. The fact that the money used to fund the scam came from elsewhere and wasn't lost at the point it was transferred to Mrs S' own account does not alter that fact and I think Wise can fairly be held responsible for Mrs S' loss in such circumstances.*

*Should Mrs S bear any responsibility for her losses?*

*In considering this point, I've taken into account what the law says about contributory negligence as well as what's fair and reasonable in the circumstances of this complaint.*

*I recognise that there were some sophisticated elements of this scam which involved a fake celebrity endorsed advert and platform, and faked emails from the other EMI and B which would have given the investment legitimacy.*

*But I consider there were red flags that should have concerned Mrs S. Mrs S hasn't suggested that she completed research in respect of C before investing and I'm unable to find any reviews at the time Mrs S made the payments, which is unusual. Mrs S then received messages from someone who said they were a financial adviser but made no mention of C. Before Mrs S made the final payments this adviser told Mrs S to lie to her bank about the reason for transfers to her EMI account. I can't see that a legitimate investment company would ask a customer to do this. The scammer also advised Mrs S to download a screen sharing app. When Mrs S spoke to her bank about a transfer on 2 February 2023, she was told that legitimate companies wouldn't ask her to download anything.*

*The fake emails Mrs S received contained errors in terms of content and grammar. I also consider that Mrs S ought reasonably to have had concerns about being asked to pay such large amounts of money to verify accounts and withdraw her funds. She had invested a small initial amount and an additional £3,000 and then was asked to pay increasing amounts of money before she could withdraw her profits. And the profits Mrs S was told she had received were unrealistic. On 20 January 2023 (after investing £3,000 the day before) Mrs S was told she had a profit and bonus of £1,240.*

*Overall, I'm provisionally persuaded that Wise should reimburse 50% of Mrs S' loss from and*

*including payment one together with interest as set out below, as Mrs S has been deprived of the funds.*

*Responses to my provisional decision*

Mrs S accepted my provisional findings. but Wise did not. It agreed that it should be held partly responsible for Mrs S' loss but didn't think it should have provided a written warning in respect of payment one. Wise noted that internal figures demonstrated that only a very small proportion of payments to B at the time were reported as fraud so it's unlikely Wise would have had any concerns.

Wise noted that the £900 payment (payment two in the table in my provisional decision) was made to an account in Mrs S' name and should not form part of her loss. But by payment three, when Mrs S was making a second payment to B for a significantly greater amount, Wise accepted there was a new and concerning pattern of payments. Wise offered to refund 50% of payment three onwards, plus interest. Mrs S didn't accept Wise's offer.

**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.

After reviewing Wise's response to my provisional decision, my decision remains broadly the same. I set out my full reasoning in my provisional decision (and reproduced it above) so I won't repeat it in full here.

Wise has provided evidence which shows that payment two in my provisional decision (for £990 on 21 January 2023) was to an account in Mrs S' own name at another bank. Given this, I agree with Wise that this payment doesn't form part of Mrs S' loss from her Wise account. Before issuing this decision, I put this point to Mrs S' representative, who said that the payment formed part of the scam. I still don't agree that Wise is responsible for this payment though. I can see that £990 was sent from Mrs S' Wise account to her bank and that on the same day Mrs S credited her Wise account with £1,000. She later made payments to the scammer from her Wise account which I have considered in the table above.

I have considered the point made by Wise about payments to B of less than £5,000. But, as I set out in my provisional decision, by the end of 2022 I consider Wise 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. As a result, Wise should have had appropriate systems for making checks and delivering warnings before it processed such payments. I consider that a proportionate response to the risk posed by a £3,000 payment to an identifiable cryptocurrency exchange would be to provide a written warning tailored to cryptocurrency investment scams. I have no reason to believe that a warning of this kind would not have prevented Mrs S' loss. All the classic hallmarks of this type of scam were present and I think an appropriate warning would have resonated with her.

I consider Mrs S should share responsibility for her loss for the reasons set out in my provisional decision. Neither party has raised any objections to what I said. Briefly, Mrs S hasn't suggested that she completed research before investing, there are no reviews in respect of C, and the messages Mrs S received were from someone who claimed to be a financial adviser but made no reference to C. Mrs S was also advised to use a screen-sharing application and to lie to her bank. I don't think a legitimate company would ask her to take these steps. I also think Mrs S ought reasonably to have had concerns about the fake emails she received, and about being asked to pay such large amounts to withdraw funds.

Overall, I'm satisfied Mrs S should share responsibility for her loss as set out below.

## My final decision

For the reasons stated, I uphold this complaint and require Wise Payments Limited to:

- Pay Mrs S £29,750; and
- Pay interest on the above amount at the rate of 8% simple per year from the date of each payment to the date of settlement.

If Wise Payments Limited is legally required to deduct tax from the interest it should send Mrs S a tax deduction certificate so she can claim it back from HMRC if appropriate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs S to accept or reject my decision before 26 June 2025.

Jay Hadfield
**Ombudsman**