DRN-5939906

The complaint

Mr A is unhappy that Wise Payment Limited won't reimburse money he lost to a scam.

Mr A is represented by a third-party claims firm, but I will refer to Mr A here.

What happened

The background to this complaint is well known to both parties, so I won't repeat everything here. In summary, Mr A has explained that between August and October 2024 he made payments from his Wise account to buy cryptocurrency which he ultimately lost to a romance scam.

Mr A advised he was unexpectedly approached by a company, who I will refer to as "H", offering him an investment opportunity. He was also introduced to one of H's representatives, who I will refer to as the "scammer" and was added to H's group chat. Mr A was told the scammer could help manage his investment funds on H's platform. He advised that he carried out research into H and was happy with the information he found about it. Mr A received contact from the scammer, and they eventually entered a relationship.

Following the advice of the scammer Mr A began investing in H. Mr A was told to transfer funds using a cryptocurrency exchange which I will refer to as "C". He was also given access to H's platform. The scammer advised he could take out 'loans' from H, with the scammer acting as a guarantor, and use the funds to invest in H. He was later told he couldn't use any of his 'profits' to pay back the loans and would need to use his own funds to do this, which he did. Mr A has also confirmed that the scammer helped him to pay back one of the loans.

Mr A realised he had been scammed when he was told he needed to pay additional fees to pay off the loans. H's platform had also stopped working. Mr A also received an email from C which advised that the wallet address he had been using was associated with malicious activity and controlled by scammers. Mr A advised C that he was continuing to speak to the scammers, maintaining the appearance of cooperation, whilst he waited for its guidance on how to track the scammers down. Mr A did further research and found that H may have cloned a genuine firm. He reached out to it by email. It confirmed that it wasn't associated with H in any way and that he should review things to avoid losing his funds.

Mr A has advised he lost £94,600 from his Wise account as a result of the scam, some of which he paid for using credit cards and a loan from a friend.

Mr A raised a complaint with Wise. It didn't think it had done anything wrong by allowing the payments to go through. So, Mr A brought his complaint to our service.

Our Investigator looked into the complaint and upheld it in part. He thought that Wise should have identified that the third payment made towards the scam for £9,250, made on the 29 August 2024 ("Payment 3"), was concerning and it should have questioned Mr A about it before it debited his account. This was because Mr A's payments were sent to an account which offers cryptocurrency services for C, so Wise should have identified the payment was related to cryptocurrency and carried a higher risk. If Wise had provided the relevant

warnings around cryptocurrency scams on this payment, the Investigator thought that the scam would have come to light and Mr A's further losses would have been prevented. Our Investigator however thought that Mr A ought to take some responsibility for his loss too. The Investigator thought that a fair deduction to the amount reimbursed would be 50%.

Both parties didn't agree with the outcome. In summary, Mr A explained that he was vulnerable at the time of the scam and that Wise should have taken this into account. He explained that it prevented him from protecting himself. So, in the circumstances, Mr A didn't agree that a deduction for contributory negligence should be made.

Wise highlighted that the payments were made to Mr A's account at C so it wouldn't have known the payments related to cryptocurrency. It also highlighted that not all cryptocurrency payments were scam related so it thought that blocking or flagging all payments to the same sort code used by Mr A was unreasonable. It also highlighted that Mr A was under the spell of the scammer so it didn't feel a warning would have made a difference in the circumstances.

As both parties remained unhappy, the complaint has been passed to me for review and a final decision.

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, I've come to the same outcome as the Investigator for largely the same reasons. I'll explain why.

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 focussed on what I think is the heart of the matter here. If there's something I have not mentioned, it isn't because I have ignored it. I haven't. I'm satisfied that 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.

In broad terms, the starting position in law is that a firm is expected to process payments and withdrawals that a customer authorises it to make. It isn't disputed that Mr A authorised the payments from his Wise account. Therefore, under the Payment Services Regulations 2017 and the terms of his account, Wise is expected to process Mr A's payments, and he is presumed liable for the loss in the first instance.

But in some circumstances, it might be appropriate for Wise to take a closer look at the circumstances of the payments – for example, if it ought to be alert to a fraud risk, because the transactions were significantly out of character or suspicious. And if so, it should have intervened, for example, by contacting the customer directly, before releasing the payments. This is to help protect customers from the possibility of financial harm from fraud. But I'd expect any intervention to be proportionate to the circumstances of the payment.

Should Wise have identified that Mr A might be at a heightened risk of fraud?

Wise have advised it didn't identify Mr A might be at risk of financial harm from fraud so I have looked to see if it should have been on notice that Mr A may be falling victim to a scam. I'm conscious that the first two payments out of Mr A's account were relatively modest (£750 and £2,000) so I can't see any reason for Wise to have been particularly concerned about

them. Payments of this size are unlikely to have appeared unusual to Wise. So, I don't think these payments would have indicated that Mr A might be at risk of financial harm from fraud.

However, Payment 3 was significantly higher than the previous payments and unusual when compared to Mr A's normal account activity. In my view, the payment was a clear escalation in value and had the potential to cause significant financial harm to Mr A, so Wise should have been on notice that this payment might indicate that Mr A was at risk of financial harm.

Wise has argued it would have only known that Mr A had transferred funds from his account held with it, to another account held with a third party, and that this wasn't identifiable to anything related to cryptocurrency. But I don't think this was the case and I don't agree with it. This is because the sort code Mr A had used to send his funds was for a well-known cryptocurrency provider which operates under the trading name C, meaning any payments to that account were in relation to cryptocurrency. So, it was reasonable to expect Wise to have identified that Payment 3 was linked to cryptocurrency - and therefore higher risk.

Wise have advised that cryptocurrency transactions are not inherently illegal. And although I agree with this, by August 2024, when these payments started, Wise should 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. It should also have been aware of the increase in multi-stage fraud (including those involving cryptocurrency) when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years and it's a trend Wise ought fairly and reasonably to have been aware of at the time of the scam. So, taking all this into account I think Wise ought to have provided warnings on the risks associated with cryptocurrency payments before the payment went ahead.

I consider that a proportionate intervention from Wise here would have been for it to ask Mr A a series of questions to narrow down the specific scam risk and provide a tailored warning which covered off the key features of the scam risk it had identified. Of course, any such warning relies on the customer answering questions honestly and openly, but I think Mr A would have been open and honest about the circumstances of this payment had Wise intervened. He hasn't told us that he'd been coached in how to mislead Wise had it intervened with questions, and I have found no evidence of this in the correspondence I have reviewed.

It's also clear from the messages with the scammer that Mr A was very worried about H's platform not being available. He raised this with the scammer several times. When he received an email highlighting that the wallet address he had used was linked to scammers Mr A discussed this with the scammer, highlighting he may have been scammed. He explained to the scammer that he wanted to continue looking into H's trading platform based on this information. This was despite the scammer's reassurances that the issues he was experiencing with the platform were normal and that he shouldn't be worried. He tried to open the website using his laptop and using a different browser. He referred to his attempts a number of times in the messages, sharing screenshots with the scammer. So, on balance, I think he would have taken any warnings from Wise into account before proceeding with further payments.

Mr A also carried out further research on H following the above concerns. He contacted H using different details and found out that it may have been cloned. He highlighted this with the scammer. And although he told the scammer he was looking to open another account with a different cryptocurrency provider, he has shared with C that he was continuing to message the scammer whilst he sought advice from it in the hope that he wouldn't lose his

funds. He didn't make any further payments from this point. All this suggests that a warning provided by Wise, alerting him to the key features of the type of scam he was falling victim to, would have resonated with Mr A – because so much of what he'd experienced was typical of similar scams, which would have been highlighted to him in a warning.

Although it could be argued that Mr A was under the scammer's spell. Having reviewed the messages with the scammer it's clear Mr A thought H's actions were separate to those of the scammer. It's also clear that Mr A was willing to question the scammer when he had concerns based on what I have said above. I also agree with the Investigator that an earlier intervention in August 2024, rather than in October 2024, when Mr A found out about the concerns with H, was more likely to have resonated with Mr A.

Taking into account this and given his ongoing concerns, I think, Mr A would have decided not to go ahead with any further payments, had a warning been given. I'm therefore satisfied Wise can be fairly and reasonably held responsible for Mr A's loss from Payment 3 onwards (subject to a deduction for Mr A's own contribution which I will consider below).

Should Mr A bear any responsibility for his 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, as a layperson, there were aspects to the scam that would have appeared convincing. I have taken into account the provision of the trading platform (which, I understand, would have used genuine, albeit manipulated, software to demonstrate the apparent success of trades). The scammer also built a relationship with Mr A which he thought was genuine at the time. So, I've taken all of that into account when deciding whether it would be fair for the reimbursement due to Mr A to be reduced. I think it should be.

Mr A was unexpectedly contacted about an investment. This should have appeared unusual as it's not something a legitimate business would usually do. He's also invested significant sums without any returns after speaking to someone he never met face to face.

Mr A explained he had carried out checks online before investing in H and that all reviews were positive. Having carried out my own historical internet search however, I found a significant number of negative reviews on a well-known review website that appeared as a top search result. These reviews highlighted the company was fraudulent. And when searching for H using a common search engine, one of the first results highlights a warning on the Financial Conduct Authority website advising customers to avoid dealing with it, so I don't think this information was difficult to find had Mr A carried out the checks he mentions.

I understand that Mr A was experiencing some difficult circumstances at the time he fell victim to the scam. He's also shared information on his ongoing health problems. I would like to thank Mr A for sharing this information with us. But I can't say that Wise was or should have been aware that he was vulnerable or made any special adjustments for him at the time the transactions were made. I also don't think the information Mr A has highlighted means he was less able to protect himself. When he noticed concerns with regards to the investment, he was able to deal with these appropriately, contacting different companies to help resolve his issues.

Overall, I'm not satisfied that it was reasonable for Mr A to proceed without better independent checks and based on the red flags he should have taken into account. Taking all of the above into account I think that Wise can fairly reduce the amount it pays to Mr A because of his role in what happened. Weighing the fault that I've found on both sides, I think a fair deduction is 50%.

Could Wise have done anything to recover Mr A's money?

I've considered whether Wise could have done anything to recover Mr A's payments once the scam was uncovered. However, the payments were converted into cryptocurrency and paid to the scammer. Therefore, I don't think there was any realistic possibility of recovery.

Interest

Mr A has used various different sources to fund the scam. He has paid interest on some of these funds and incurred fees. He is also continuing to pay some charges on the loss he has incurred. Although neither party has raised concerns on awarding interest on the refund, I have given this some thought as part of my decision. On the whole, given that most of the payments have been funded from different sources and are being repaid across different dates, I believe the fairest way to resolve the simple interest calculation is to award 8% interest in the circumstances.

My final decision

For the reasons given above, I uphold this complaint in part and require Wise Payments Limited to pay Mr A:

- 50% of all payments made towards the scam from 29 August 2024 – a total of £45,925.
- 8% simple interest per year on that amount from the date of each payment to the date of settlement (less any tax lawfully deductible)

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr A to accept or reject my decision before 12 January 2026.

Aleya Khanom
Ombudsman