DRN-4782990

The complaint

Ms R is complaining that Wise Payments Limited didn't do enough to prevent her from falling victim to an investment scam.

The complaint is brought on her behalf by a professional representative.

What happened

In May 2022 Ms R fell victim to an investment scam. She said she saw an online advert for an investment opportunity endorsed by a public figure, and after researching the company she entered her contact details. Shortly afterwards she was called by someone who I'll refer to as "the scammer." The scammer persuaded Ms R that this would be a good investment for her, and Ms R initially invested £250. The scammer asked Ms R to download a remote access programme and to send her copies of her passport and proof of address, which she did, and then she was given access to a convincing-looking scam platform where she could see her initial investment growing.

Ms R continued to chat with the scammer and felt she'd built up a genuine relationship with her. After a few weeks, the scammer told Ms R she'd need to invest more money to see a substantial return. She told Ms R she should open an account with Wise to avoid delays in making payments and did that for her using her identification documents and remote access. The scammer was able to move Ms R's funds out of the Wise account to what Ms R thought was the genuine investment platform.

The following payments were made from Ms R's account to cryptocurrency exchanges between 30 June 2022 and 25 October 2022 – totalling £55,768.

Payment number	Date	Type	Payee	Amount
1	30 June 2022	Debit card	Cryptocurrency exchange A	£1,000
2	8 July 2022	Debit card	Cryptocurrency exchange A	£3,500
3	8 July 2022	Transfer	Cryptocurrency exchange B	£15
4	19 July 2022	Transfer	Cryptocurrency exchange B	£3,968
5	22 July 2022	Debit card	Cryptocurrency exchange A	£4,975
6	26 July 2022	Debit card	Cryptocurrency exchange A	£4,990
7	3 August 2022	Transfer	Cryptocurrency exchange B	£4,820
8	3 August 2022	Transfer	Cryptocurrency exchange B	£700
9	3 August 2022	Transfer	Cryptocurrency exchange B	£6,300

10	10 August 2022	Debit card	Cryptocurrency exchange A	£4,000
11	20 September 2022	Debit card	Cryptocurrency exchange A	£4,000
12	21 September 2022	Debit card	Cryptocurrency exchange A	£6,000
13	22 September 2022	Debit card	Cryptocurrency exchange A	£6,000
14	28 September 2022	Debit card	Cryptocurrency exchange A	£2,500
15	*13 October 2022*	*Debit card*	*Cryptocurrency exchange A*	*£1,000*
16	*14 October 2022*	*Debit card*	*Cryptocurrency exchange A*	*£6,810*
17	*18 October 2022*	*Debit card*	*Cryptocurrency exchange A*	*£5000*
18	*21 October 2022*	*Debit card*	*Cryptocurrency exchange A*	*£5,000*
19	*24 October 2022*	*Debit card*	*Cryptocurrency exchange A*	*£1,800*
20	24 October 2022	Debit card	Cryptocurrency exchange A	£3,000
21	*25 October 2022*	*Debit card*	*Cryptocurrency exchange A*	*£6,005*

Payments 15 to 19, and 21, were made from Ms R's account after the scammer transferred funds into it from other scam victims and then transferred the funds back out to the cryptocurrency exchange, so I've not included them in Ms R's loss.

Wise has told us that it intervened on Payment 4, Payment 7 and Payment 9 by asking for the payment purpose. For each payment the payment purpose was selected as "*sending money to yourself*" and Wise showed scam warnings based on this payment purpose.

The scam went on for some time but on 26 October 2022 Wise received a report that Ms R's account was being used to receive payments made as part of a scam. So, Wise blocked the account, and it could no longer be used. The scam was subsequently uncovered when Ms R stopped receiving replies from the scammer.

Ms R reported the scam to Wise in July 2023 by raising a complaint through her representative. Wise couldn't complete its investigation in time, so Ms R brought her complaint to the Financial Ombudsman Service.

Our Investigator thought Wise should have intervened further by contacting Ms R directly at the time of Payment 6 on 26 July 2022. But she didn't think a direct intervention from Wise would have uncovered the scam, because Ms R's bank had spoken to her on the phone several times about the payments she was making to her Wise account and Ms R hadn't been open and honest about what was happening.

Ms R's representative didn't agree with our Investigator. It said, in summary, that Wise failed Ms R by not providing an effective intervention. It said Wise should have provided effective scam warnings and asked probing questions about the circumstances of the payments, with a view to the possibility that Ms R was being coached by the scammer.

Ms R's complaint has now been passed to me for review and a 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.

I'm very sorry to disappoint Ms R but I'm not upholding her complaint. I'll explain why.

Were the payments authorised?

The relevant law here is the Payment Services Regulations 2017 – these set out what is needed for a payment to be authorised and who has liability for disputed payments in different situations. With some exceptions, the starting point is that the consumer is responsible for authorised payments and the business is responsible for unauthorised payments.

The PSRs go on to specify how consent is given. It must be in the form, and in accordance with the procedure, agreed between Ms R and Wise, which according to Wise's terms and conditions at the time of the payments was as follows (for card payments):

"*You agree that any use of your Card, card number or PIN constitutes your authorisation and consent to a transaction."*

For transfers, the terms said (broadly) that a customer must provide details of the recipient account name, account number and the amount of the payment to set up a payment.

In practical terms, that means Ms R consents to a payment if she completes the agreed payment steps. Or if someone else acts on her behalf and uses those agreed steps. If Ms R allowed someone else to use the payment steps, that individual would be treated as her agent and any payments they made would be considered authorised.

Ms R says she didn't make the payments in dispute here herself, but she knew the payments were being made – she was aware that she'd shared her card details with the scammer in order to make the payments, and from what she told her bank about the scam it seems she also shared the one time passcodes Wise sent to her via text message with the scammer so the card payments could be authenticated. And for the transfers, Ms R had allowed the scammer to access her Wise account and to use the agreed payments steps to make payments on her behalf.

Here, Ms R was aware someone else had access to her account and was making payments that she believed were for her benefit. Therefore, I think it's fair and reasonable for Wise to treat the payments as authorised.

Could Wise reasonably have prevented Ms R's loss?

I've concluded that the payments were authorised, so I've gone on to consider if Wise should have done anything else to prevent the payments Ms R made to the scam.

When a payment is authorised, Wise has a duty to act on the payment instruction. But in some circumstances, it should take a closer look at the circumstances of the payment – for example, if it ought to be alert to a fraud risk, because the transaction is unusual, or looks

out of character or suspicious. And if so, it should intervene, for example, by contacting the customer directly, before releasing the payments. I'd expect any intervention to be proportionate to the circumstances of the payment.

But I've also kept in mind that Wise processes high volumes of transactions each day. There is a balance for it to find between allowing customers to be able to use their account and questioning transactions to confirm they're legitimate.

The account with Wise was opened as part of the scam and so there was no usual account activity for Wise to compare these transactions to. Wise would have been relying on generic indicators to decide if the payments looked suspicious.

The Investigator concluded that Wise didn't show Ms R any scam warnings – but I can see it did provide scam warnings based on the payment purpose of *"sending money to yourself"* selected for the payments, although these were not particularly relevant to the scam Ms R was experiencing due to this payment purpose being selected. We know that Ms R was unlikely to have seen these warnings because the scammer was carrying out the process to make the payments, but Wise wouldn't have been aware of this.

The Investigator decided Wise should have intervened directly at the time of Payment 6, but with the above in mind I think a more reasonable point for a direct intervention from Wise would have been around Payment 9 on 3 August 2022, when over £10,000 had been sent to a cryptocurrency exchange in one day. I'm also keeping in mind that while it was clear the card payments were to buy cryptocurrency, in 2022 I wouldn't have expected Wise to have considered there was a significantly heightened risk of fraud due to this.

But this doesn't make a difference to the overall outcome of Ms R's complaint because notwithstanding the exact point at which Wise should have intervened directly, I don't think the scam would have been uncovered if Wise had intervened in this way.

I say this because Ms R had another complaint with us relating to payments made to the scam from her account with her bank. And I can see that Ms R's bank did intervene during the progression of the scam, and they had several conversations with Ms R about the circumstances of the payments (including on 3 August 2022). But in these conversations Ms R wasn't open about the circumstances of the payments she was making and gave her bank inaccurate information about the purpose of the payments.

Ms R hasn't given much detail about how she was guided by the scammer, although she's told us that she was told not to tell her bank about investing in cryptocurrency and she was worried she wouldn't get back what she'd already invested if she didn't do as they instructed. But judging by the conversations she had with her bank it seems she must have been guided quite closely about what to say to bypass the interventions her bank carried out.

In a conversation with her bank on 3 August 2022 when she was making a payment to Wise, Ms R said the following:

- The purpose of the transfer was for personal reasons.
- She was transferring the money to Wise because the interest rates were better.
- Someone told her this and she did research too.
- She wasn't told to open an account with Wise by anyone.
- The payments into her account with the bank were expected and were from her family.

- Nobody had told her how to answer her bank's questions or to mislead them in any way.
- She was the only one who had access to her internet banking or device.
- Nobody had asked her to share information from her secure device and she wasn't planning on sending the funds to anyone else.

In later conversations Ms R gave her bank a detailed cover story, explaining that she was transferring funds to buy furniture for a property she owned abroad. Ms R was also asked to visit the branch before her bank released the payments and had a conversation there in which she also misled the bank about the circumstances of the payments.

I'm also taking into account that on 16 August 2022 Ms R spoke to her bank and told them she'd been the victim of a scam. She said she was asked to make another payment to withdraw her funds and she realised then this was unlikely to be a genuine investment. It's unclear how Ms R was then persuaded to continue to make payments to the scam from her bank and subsequently from Wise, but it's clear that she was, as she continued to invest in the scam despite further detailed interventions from her bank about the later payments.

This scam was very sophisticated and involved Ms R being groomed by the scammer over some time before she was asked to invest larger sums of money. So, a relationship had been built up by the time she started to make more significant payments. Ms R obviously placed a lot of trust in the scammer as she allowed her to move money between her accounts and authenticated the transactions, and she's said she thought of the scammer as a friend.

Businesses should ask probing questions and be mindful that scammers can provide cover stories or guide their victims in what to say to avoid the scam being detected. But the effectiveness of an intervention in uncovering a scam does also somewhat rely on their customer being open and honest about what they're doing. It's clear that Ms R's bank had strong suspicions that she was continuing to be scammed after its conversation with her on 16 August 2022 but ultimately Ms R insisted that she was making the payments to buy furniture for her house abroad and wanted to make the payments. Although Wise would have been aware that Ms R was making payments to a cryptocurrency exchange so that particular cover story may not have rung true, I do think it's likely that Ms R would have been guided by the scammer on how to effectively bypass any intervention from Wise. And I don't think any intervention or warning from Wise would have broken the scammer's the spell given the evidence that Ms R apparently realised she'd been scammed on 16 August 2022 but continued to allow the scammer to make these payments anyway.

Overall, the weight of the evidence suggests that Ms R was under the spell of the scammer, and was determined to continue to make the payments to the scam despite the interventions from her bank and her own suspicions that she was being scammed. From what I've seen I'm not persuaded that her payments to the scam would have been prevented, had Wise intervened directly as I would have expected.

Could Wise have recovered the funds once the scam was reported?

When the scam was reported Wise did attempt to recover the funds Ms R transferred to the cryptocurrency exchange, but perhaps unsurprisingly it appears to have been unsuccessful in doing so – because the funds were transferred to an account held in Ms R's name and were used to buy cryptocurrency, which was then lost to the scam.

Some of the payments were made using Ms R's debit card. Debit card transactions can sometimes be disputed through a process called chargeback, subject to the relevant card scheme's rules. But there was little prospect of chargeback being successful here, because the cryptocurrency exchange provided the service it had been paid for in facilitating the purchase of the cryptocurrency which was then lost to the scam.

Other considerations

I'm really sorry to learn that Ms R was diagnosed with a serious illness during the scam. But because I don't think Wise were, or ought to have been aware of this I can't say that it didn't fairly take this into account when the payments were made.

I'm sorry to disappoint Ms R. It's not in dispute that she's been the victim of a cruel scam, and I can see just how effectively the scammer manipulated her into making these payments. I can understand why, as a victim of a scam, she'd think the payments she made should be refunded. But because I don't think an intervention from Wise would have prevented her loss, it wouldn't be fair or reasonable to ask it to refund the payments she made.

My final decision

My final decision is that I'm not upholding Ms R's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms R to accept or reject my decision before 19 August 2025.

Helen Sutcliffe
Ombudsman