

The complaint

Mr M has complained about Wise Payments Limited not refunding several payments he says he made and lost to an authorised push payment (APP) investment and recovery scam.

What happened

The background to this complaint is well known to both parties, so I won't repeat it in detail here. In summary, Mr M fell victim to an investment scam after he came across an investment platform that he believed to be genuine. After initially completing an enquiry form he was contacted by the scammer who continued to correspond with him throughout. Mr M believed he would be receiving high returns with only minimal risk. Supported by the scammer, during telephone calls and via screensharing software, Mr M proceeded to make payments via a cryptocurrency exchange and peer-to-peer. The funds had the final destination of the scammer, not a legitimate exchange. After an initial deposit the scammer helped Mr M withdraw \$40 to reflect the ease of doing so. However, he realised he had been scammed when he was unable to withdraw his funds.

The scammer then convinced Mr M to join him in an attempt to recover the "lost" funds with a recovery firm. However, Mr M realised this was also part of the scam when he did not obtain his funds and the scammer ceased all contact.

The relevant transaction history of Mr M's completed payments:

Transaction	Date	Type of Transaction	Amount
1	9 November 2022	Card payment to M	£3,450
2	17 November 2022	M Ltd	£4,800
3	21 November 2022	LK	£5,000
4	1 December 2022	M Ltd	£2,150
5	16 December 2022	VU	£5,000
6	16 December 2022	MC	£275
7	16 December 2022	ML	£3,500
8	19 December 2022	VU	£937
9	19 December 2022	VU	£1,747
10	19 December 2022	AT	£875
11	20 December 2022	MWM	£1,050
12	20 December 2022	AAS	£1,170
13	21 December 2022	JYC	£1850
14	21 December 2022	MP	£850
15	22 December 2022	PP	£1,050
16	28 December 2022	CWN	£800
17	17 January 2023	TS	£1810
18	18 January 2023	XRH	£1910
19	9 February 2023	OT	£1,650
20	18 April 2023	VR	£1,725

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.

Our Investigator looked into things but didn't recommend the complaint be upheld. They weren't persuaded, on balance, that Wise could have prevented Mr M from falling victim to the scam. As our Investigator couldn't resolve the matter informally, the case has been passed to me for a final decision.

I issued a provisional decision on 2 May 2025 and said:

"I have considered all the available evidence 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.

I don't doubt Mr M has been the victim of a scam here – he has lost a large sum of money and has my sympathy for this. However, just because a scam has occurred, it does not mean he is automatically entitled to recompense by Wise. It would only be fair for me to tell Wise to reimburse Mr M for his loss (or a proportion of it) if: I thought Wise reasonably ought to have prevented all (or some of) the payments Mr M made, or Wise hindered the recovery of the payments Mr M made – whilst ultimately being satisfied that such an outcome was fair and reasonable for me to reach.

I've thought carefully about whether Wise treated Mr M 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, I've decided to not uphold Mr M's complaint. I know this will come as a disappointment to him and so I will explain below why I've reached the decision I have.

I have kept in mind that Mr M made the payments himself and the starting position is that Wise should follow its customer's instructions. So, under the Payment Services Regulations 2017 (PSR 2017) he is presumed liable for the loss in the first instance. I appreciate that Mr M did not intend for his money to ultimately go to a scammer – but he did authorise these payments to take place. However, there are some situations when an Electronic Money Institution (EMI) should have had a closer look at the wider circumstances surrounding a transaction before allowing it to be made.

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 - Wise 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.*

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

I have kept in mind the initial authorised card payment was to a cryptocurrency provider, but that doesn't mean it would have automatically been treated as suspicious. This is particularly so when there are no other concerning factors about the payment. Buying cryptocurrency is a legitimate activity and wasn't / isn't uncommon for EMI account holders to use their account to do so. The exchange in question is also a legitimate one. Overall, I don't think the payment was sufficiently suspicious that I would have expected Wise to have intervened.

The payments that followed were to a variety of new payees, with no apparent link to the initial payment to the cryptocurrency exchange. So Wise couldn't reasonably have known through its transaction monitoring systems that the final destination for these funds was the same, to the scammer behind the investment. There were also no identifiable patterns with most of Mr M's payments as they were of fluctuating amounts and were generally spread over a few months. Using the account to transfer funds of varying amounts to other individuals would also not appear too unusual as Mr M had used his account this way before; albeit he was doing so on a more frequent basis because of the scam.

Mr M's account activity did cause Wise some concern and it intervened on payments: 2, 4, 7, 10, 13, 14, 15, 16, 17, 18 and 19. It did so by asking Mr M to confirm the reasons for these transfers. In response, Wise presented a warning which broadly covered the potential risks associated with that type of transfer, before allowing the money to be released. I consider these written warnings were generally a reasonable intervention. However, having considered the payments on 16 December 2022, I do think Wise ought to have taken their intervention on payment 7 further than just a written warning. As this was the second large payment made on this day human intervention, such as via its in-app chat, to ask some additional questions would have been more appropriate. But I'm not persuaded that such an intervention from Wise would have prevented Mr M's losses.

The responses Mr M gave to these warnings, especially to those early in the scam, highlight how quickly the scammer had built influence with Mr M and was coaching him. This, when considered alongside the scam chat history logs, likely explains why Mr M felt comfortable selecting the payment reasons he did on the transactions Wise blocked. Ultimately, he was most likely being guided to do so by the scammer. There was no other reason, given Mr M no doubt believed this was a genuine investment, to have mislead Wise with his answers. As Mr M did not provide accurate reasons for the purpose of each payment, it denied Wise the opportunity to display a more appropriate warning. The warning given for each of these payments was dependent upon what Mr M selected the reason for the transfer to be. Had Mr M selected 'Making an investment', rather than 'Paying for goods or services' or 'Sending money to friends and family', he would have been shown an investment scam warning. Such a warning would have broadly covered the risks of an investment scam. However,

instead, Mr M was shown less applicable warnings about potential scams linked with paying for goods or services or sending money to friends or family.

Alongside the inaccurate information Mr M had already supplied to Wise for payments 2, 4 and 7, in response to the interventions it did complete, I've also noted he was also screensharing with the scammer at various points and speaking with them via the telephone whilst completing transactions. The scam chat shows Mr M was speaking with the scammer directly before payment 7, and perhaps even during the payment as well, which as above, likely explains why he felt comfortable misleading Wise as to the payment reason. Therefore, I think it highly probable the scammer would have guided Mr M on how to respond during a human intervention. Additionally, in November 2022 Mr M's other bank ("bank 1") flagged a transfer he was making to Wise as potential fraud, yet he was not forthcoming with any details during that call. Although there was no substantive questioning, I have kept in mind Mr M only confirmed enough detail for bank 1 to be aware he was transferring the funds to his own Wise account and did not volunteer anything else. So, as well as being persuaded Mr M would have been coached through how to respond to any questions from Wise, I do not think he would have been readily forthcoming with any additional information which may have alerted Wise to the scam he was involved in. Ultimately, nor do I think any subsequent additional intervention, taking into account all those that did occur as the payments progressed, would have prevented Mr M's losses occurring.

I have noted a substantial number of Mr M's transactions did not complete from 16 January 2023 onwards, with some flagged for further review by Wise. During this time Mr M also telephoned Wise to ask what was preventing him making payments, but I've noted no formal intervention occurred in these calls. Wise has confirmed a review of Mr M's account began on 22 January 2023, but decided the payments resembled peer-to-peer cryptocurrency transactions and took no further action. However, it accepts it could have done more to question Mr M at this point. On 24 January 2023 Wise also accepts this failed payment should have triggered a request for confirmation as to the payment reason and relationship to the recipient. Similarly, on 25 January 2023 another fraud agent reviewed Mr M's account but took no action after seeing Mr M subsequently just sent his funds to another of his own accounts. Wise is correct to conclude it could have questioned Mr M more here, but I do not think it would have prevented Mr M's losses.

I say this because I am not persuaded that even had there been further human intervention it would not have made any difference. The scam chat history makes it clear that as the scam progressed, Mr M's trust in the scammer increased and with it the influence the scammer had over him. When these later payments failed Mr M reverted to the scammer to seek assistance for alternative ways to make his payments. They agreed that with the 'fraud squad' watching Mr M it would make it harder for him to complete transactions, before screensharing and reviewing the terms and conditions of alternative EMI together. The scammer also instructed Mr M on how to respond if questioned, to receive funds in another currency to bypass higher regulatory expectations and that he should split transfers into smaller amounts to increase the possibility of transfers being successful. Even when a professional recovery agent informed him of the scam, the scammer was able to dissuade him from listening to them. Mr M was unquestionably under the influence of the scammer, trusting that he had not only helped him make legitimate investments but was also helping him recover his funds.

It's most likely whatever the obstacle, or information Mr M was presented with from other parties, Mr M would have sought guidance from the scammer as he had done

at all other times. Therefore, I'm not persuaded Wise would have been able to prevent Mr M's losses from either the investment or recovery scam.

Recovery

The only method of recovery Wise has for the payment made by card is to request a chargeback. However, Mr M didn't make the initial card payment to the scammer directly, he paid a cryptocurrency exchange. The service provided by the cryptocurrency exchange would have been to convert or facilitate the conversion of Mr M's payments into cryptocurrency. The fact that the cryptocurrency was later transferred elsewhere, to the scammer, doesn't give rise to a valid chargeback claim against the merchant Mr M paid. Ultimately, the cryptocurrency exchange provided the requested service to Mr M.

It's not clear if Wise took any action to try and recover the funds Mr M transferred directly to other accounts after he reported the fraud. But given the length of time that had passed between Mr M making the payments and reporting the scam, I think it's more likely than not that the funds would have already been removed from these accounts. From what we know of these types of scams, scammers usually move the funds elsewhere shortly after the transfer to seemingly to try and hinder any type of successful recovery. Or, where the funds were used to purchase cryptocurrency, peer-to-peer, which Mr M then transferred to the scammer, any attempt by Wise would have also unlikely been successful. Mr M would have received the cryptocurrency and it would have remained in his control until he decided to send it to the scammer. Because of this, I'm not persuaded Wise could've successfully recovered Mr M's funds.

So, in light of all of the above findings, there's no fair and reasonable basis under which I can ask Wise Payments Limited to reimburse Mr M's loss."

Wise Payments Limited responded and accepted my provisional decision. However, Mr M did not reply.

As there are no additional points for me to consider, I see no reason to depart from the provisional decision I issued.

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 M to accept or reject my decision before 25 June 2025.

Lawrence Keath
Ombudsman