DRN-6203651

The complaint

X complains that Wise Payments Limited won't refund money he / she lost to an investment scam. X is represented in this complaint, but I'll refer to X as it's X's complaint.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

X is a senior citizen who wanted to invest some of his / her savings so he / she could help his / her family financially.

In mid-2025, X's friend recommended an investment opportunity with (fake) Company Z which involved trading in cryptocurrencies and commodities and promised returns of between 7% and 16%.

After expressing an interest, Person E (a scammer) contacted him / her by phone, and he persuaded X to invest.

X mainly spoke to the scammer by phone and after making an initial investment of £200, which he / she was tricked into believing had made a good profit, Person E persuaded him / her to invest higher amounts.

X was also persuaded to download software to give Person E access to his / her devices.

To credit his / her Company Z investment, in May 2025, X appears to have been told to transfer funds from his / her Bank S account to an international payments company (Firm R). After experiencing difficulties crediting Firm R with £5,000, Bank S intervened. They warned X about Company Z and, due to this and his / her frustration, X decided not to go ahead.

On 16 June 2025, X or Person E then set up an account with Wise.

X knowingly transferred funds to it from his / her Bank S account giving them a different and false reason. From Wise he / she then made the following three payments to an overseas account in his / her name that Person E would've had access to.

Payment Number	Date	Payment type	Payee	Amount
1	19/6/25	International payment	X's account	£5,000
2	28/6/25	International payment	X's account	£5,000
3	14/7/25	International payment	X's account	£15,000
Total				£25,000

X realised they'd been scammed when his / her investment started to reduce, and Person E started to be rude to him / her and then stopped all contact.

X complained to Wise seeking a full refund as he / she thinks their systems should've noticed out of character payments that were indicative of fraud, and interventions would've prevented his / her financial loss.

Wise rejected X's complaint saying:

- They had no reason to believe the transfers weren't legitimate at the time they were set up.
- X had no relevant payment history with Wise, and the reported fraudulent payments were the first transactions set up on X's Wise account.
- They didn't believe the activity on X's account at the time was suspicious enough to mean that further intervention was required and that there was more they could've done to protect his / her account.

X disagreed and escalated his / her complaint to our service. Our investigator considered that Wise should've implemented the following warnings:

- For payments 1 and 2, a general online written warning broadly covering typical scam risks.
- For payment 3, a written tailored warning which asked a series of questions to narrow down the specific scam risk to give a warning based on the risk identified.

However, as our investigator found evidence that X had been untruthful to Bank S (after their initial intervention) he didn't think such fraud prevention action would've stopped X making the payments.

But X disagrees and asks for an ombudsman review. This is because X thinks tailored written warnings should've been implemented on payment 1 and 2, due to a combination of his / her advanced age, the account being new, them knowing about multi-stage fraud and it being an international payment. Also, a human intervention on payment 3 as it was large. And X believes these interventions would've resulted in a different outcome. X also pointed out that the payment reason given to Bank S was extremely superficial and points out that there weren't any probing questions.

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, my decision is not to uphold this complaint and I'll explain why.

I should first say that:

- I'm very sorry to hear that X has been the victim of this very cruel and distressing scam and lost a significant amount of money here.
- In making my findings, I must consider the evidence that is available to me and use it to decide what I consider is more likely than not to have happened, on the balance of probabilities.
- I'm satisfied that the APP Scam Reimbursement Rules, introduced by the Payment Systems Regulator in October 2024, for customers who have fallen victim to an APP scam, don't apply here because the payments were international.
- Regarding recovery attempts, I'm satisfied that Wise made reasonable efforts. Unfortunately, there was a delay in recalling the payments due to the reason given by X followed by a lack of response, and then Wise didn't receive an answer from the beneficiary bank. However, even if Wise had attempted to recall the payment earlier and received a response, I think it likely that the account would've been emptied by the scammer.

- The Payment Services Regulations 2017 (PSR), FCA's Consumer Duty and Banking Protocol are relevant here.

  PSR

  Under the PSR and in accordance with general banking terms and conditions, banks and Electronic Money Institutes (EMI's) should execute an authorised payment instruction without undue delay. The starting position is that liability for an authorised payment rests with the payer, even where they are duped into making that payment.

  There's no dispute that X made the payments here, so they are considered authorised. However, in accordance with the law, regulations and good industry practice, a bank or EMI should be on the look-out for and protect its customers against the risk of fraud and scams so far as is reasonably possible. If it fails to act on information which ought reasonably to alert a prudent banker to potential fraud or financial crime, it might be liable for losses incurred by its customer as a result.

  EMI's and banks do have to strike a balance between the extent to which they intervene in payments to try and prevent fraud and/or financial harm, against the risk of unnecessarily inconveniencing or delaying legitimate transactions. So, I consider Wise should fairly and reasonably:

  - Have been monitoring accounts and any payments made or received to counter various risks such as anti-money laundering and preventing fraud and scams.
  - Have systems in place to look 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 banks 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, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

    Consumer Duty

    Also, from July 2023 Wise had to comply with the Financial Conduct Authority's Consumer Duty which required financial services firms to act to deliver good outcomes for their customers. Whilst the Consumer Duty does not mean that customers will always be protected from bad outcomes, Wise was required to act to avoid foreseeable harm by, for example, operating adequate systems to detect and prevent fraud. Wise was also required to look out for signs of vulnerability.

With the above in mind, I first considered:

Whether Wise should've recognised that X was at risk of financial harm from fraud and put in place effective interventions?

Payments 1 and 2

I don't think the payments being international and the funds coming from one of X's accounts to go to another overseas ('me to me' payments in X's name) would've been seen as unusual or high risk.

This is because:

- Wise is an EMI and not a bank, and its primary purpose is to send payments worldwide.

- The payments Wise make are typically for transfers to accounts in another currency or for payments to friends and family members and payments can range from one-off low amounts to larger amounts.
- Wise would've had some level of comfort that the payments were going to another account in X's name that would be under X's control.

Also, these two payments weren't particularly high and, with a gap between them, there wasn't a fraud pattern.

However, considering Wise didn't have any information on X's spending pattern and would've had information on X's advanced age, which could be a potential vulnerability, I also would've expected proportionate action to have been the issuing of general fraud and scam warnings. And Wise have confirmed that this didn't occur.

Payment 3

This payment was almost one month after payment 1, so again there wasn't a fraud and scam pattern, and it was now an established 'me to me' payment' rather than a first-time payment going to a third party or a company.

Although the above would've reduced the level of risk, £15,000 should've been seen as a large amount and, as Wise had a lack of payment information and could see a potential vulnerability, I would've expected them to have identified some risks factors and implemented their dynamic automated fraud prevention system to give education and warnings.

This would've asked X to confirm the payment reason and then answer a series of questions to narrow down the specific scam risk to enable them to give strong fraud and scam education, warnings and advice. Wise have also confirmed that this didn't occur.

Having established that Wise should've recognised a level of risk and put in place written warnings and implemented their dynamic warning system, I then considered:

Whether implementation of such fraud and scam prevention methods would've prevented X's financial loss.

On Bank S's first 27 May 2025 intervention, X was open about what he / she was doing (when first attempting a £5,000 payment) and seemed cautious, fully aware of scam risks and assured. However, Person E appears to have subsequently persuaded X to have changed his / her mind and to be untruthful to his / her banks in order to pay more money into the fake investment.

Having seen evidence of Person E giving X clear instructions to lie to his / her bank or EMI, I noted that, after she had received warnings about Bank X and some scam education from Bank S, the following questions were asked and answers given:

- A Bank S agent said *'Criminals can be very convincing and ask a customer to mislead the bank to avoid detection. If anyone has asked you to lie or mislead the bank as part of this payment request, it will be a scam. This includes giving us a different payment reason to the one that's true'* and they asked X if anyone had told him / her to lie to them? X wasn't truthful and said '*no*' and made a point of repeating the same answer.
- When the Bank S agent asked X for the reason that he / she was transferring funds to Wise, again X wasn't truthful and said he / she was *'going abroad a lot'.*

Although I in no way blame X for her actions, as Person E would've convinced her she was making a high profit and persuaded him / her to give answers to circumvent bank checks, based on the above interactions with Bank S and strong coaching evidence, I'm not persuaded she would've taken note of written warnings if they had occurred on payment 1 and 2.

If implemented on payment 3, Wise's dynamic automated system would've given X the following choice of payment reasons:

1. *'Sending money to yourself*
2. *Sending money to friends and family*
3. *Paying for goods or services*
4. *Paying a bill (like utilities or tax)*
5. *Making an investment*
6. *Paying to earn money by working online*
7. *Something else'*

And, upon selection of one of the above reasons, further questions would appear followed by relevant education and warnings.

As Person E had control of X's devices, he would've probably deliberately selected the wrong reason or, if X was controlling her device for the Wise payments, told her what to select. So, as X was trusting Person E and under their spell, I think it more likely than not that:

- Wise wouldn't have received the correct payment reason.
- The effectiveness of their fraud prevention system would've been negated, and X wouldn't have received the correct education, warnings and advice.
- X would've gone ahead with the payment.

Even if X saw the correct warnings and education or a human intervention was implemented, on balance, I'm not persuaded this would've made a difference. I say this because X had already received warnings, was aware of the risk and was willing to trust Person E over his / her bank. And with initial human intervention likely being electronic (as Wise are an EMI and the payment was 'me to me') and Person E coaching X and having control of his / her devices, I think it more likely than not that a Wise agent would've been given a plausible 'me to me' transfer explanation that would've likely limited questions and avoided suspicion.

So, having considered the above and all the information on file, whilst I think Wise should've implemented warnings and I'm genuinely very sorry to hear about X's large financial loss and significant distress, I don't think it would be fair or reasonable to hold Wise responsible for X's financial loss.

My final decision

For the reasons mentioned above, my final decision is that I'm not upholding this complaint against Wise Payments Limited.

Under the rules of the Financial Ombudsman Service, I'm required to ask X to accept or reject my decision before 7 April 2026.

Paul Douglas
Ombudsman