

The complaint

Mr N is unhappy that Wise Payments Limited decided not to refund him after he was the victim of an authorised push payment (APP) scam.

What happened

Mr N fell for a job scam using his Wise account. He purchased tasks to complete, which would earn him commission and payment. He was also encouraged to use a crypto wallet provider and use a trading platform.

From June and August 2022 Mr N made 14 payments totalling £16,729.82. Mr N says the scammers said they were from reputable and well-known companies, so he had no reason to doubt this wasn't a legitimate job opportunity. Mr N said he'd used job websites previously and that's why didn't think contact about this job, although out of the blue, was out of the ordinary or suspicious. He set up accounts, as instructed to by the scammers, and was provided a login, so that he could utilise their training tools, trading platforms and website. The portal was professional, and Mr N says he assumed only legitimate companies would have access to such sophisticated software.

When Mr N realised, he'd been the victim of a scam he raised a claim with Wise, seeking a full refund, plus 8% simple interest and a £250 compensation payment.

Mr N held his account with Wise for some time but used it rarely. Wise highlighted that he'd used the account for five transfers between 2015 and 2021. It went on to say because the account had a limited history of activity it didn't have anything to compare the fraudulent payments to.

Many of Mr N's payments were made to other accounts held at Wise. These were peer to peer crypto purchases. Wise confirmed no funds remained in the recipient accounts it held. One of our investigators looked into things. They didn't uphold Mr N's complaint as they didn't think Wise needed to have intervened or prevented the payments when Mr N made them. He didn't think the payments were particularly suspicious or unusual as they weren't of significant value.

He also said Wise couldn't recover the funds as the recipients provided the crypto currency Mr N purchased from them.

He did not recommend any compensation needed to be paid by Wise.

Mr N's representatives disagreed, it said Wise as an EMI had a duty to have systems in place to detect and prevent scams. The pattern of payments here was suspicious because:

- Mr N set up 13 new payees, which was unusual.
- In the previous six months he hadn't processed a payment for more than £5, so the value of the payments here was unusual for Mr N.
- The first payment Mr N made, for £4,976 ought to have triggered a warning in and of

itself.

- Although the payments were identifiable being made to or in regard of cryptocurrency, Wise ought to have been aware that victims transfer money to new payees before going on to purchase crypto currency
- The request for compensation was to reflect the mental and emotional stress suffered by Mr N.

The investigator didn't consider the payments made by Mr N to represent a scam risk. He went on to say the payments made on 29 June 2022, are not of high value and are not made in quick succession, and they were made to four different payees. He added, the one-off payment of £4,976, whilst larger than Mr N's usual payments, wasn't significant in value. And the payments were made to individuals so Wise wouldn't have been able to identify these were related to cryptocurrency. He also said the distress here was caused by the scammers and not by Wise, so he wasn't minded to change his finding regarding compensation. Mr N's representative did not agree and asked for an ombudsman to review the complaint. I have set out the table of transactions below.

Date	Payee	amount
29 June 2022	Payee 1	£4,976.28
29 June 2022	Payee 2	£418.14
29 June 2022	Payee 3	£1,328
29 June 2022	Payee 4	£994.71
27 July 2022	Payee 5	£20
28 July 2022	Payee 6	£192.55
1 August 2022	Payee 7	£156.08
5 August 2022	Payee 8	£149
10 August 2022	Payee 9	£220
19 August 2022	Payee 10	£348.89
19 August 2022	Payee 11	£2,000
19 August 2022	Payee 12	£3,056.11
19 August 2022	Payee 11	£2,000
19 August 2022	Payee 13	£870.06
		Total £16,729.82

The complaint was passed to me and below I've set out below my provisional decision – the findings and recommendations of which I've adopted as forming part of this final decision.

My provisional 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.

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.

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.

But, 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 including in relation to card payments);
- 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.

I'm satisfied that Wise ought to have recognised that the fourth payment Mr N made on 29 June 2022 carried a heightened risk of financial harm from fraud. I say this because, by this time Mr N had made payments totalling over £7,700 in one day, to four new payees. Which was out of character for Mr N and represented a scam risk.

Wise hasn't provided a detail file, so I haven't seen the account opening reason or any evidence of the payments as they were processed. I don't know if Wise asked any questions of Mr N at the time of making the payments – i.e. if Mr N gave a payment reason for any of the payments made. Or if that prompted Wise to provide any warnings.

But even if it did ask questions or provide warnings, I don't think this changes the overall outcome here. I'll explain why.

The payment reason options that would have been made available to Mr N when making these payments would have been – sending money to yourself; sending money to friends and family; paying for goods or services; paying a bill; making an investment; or something else. Wise didn't offer an option of "paying to earn money by working online" until around March 2023.

If Mr N had selected one of the existing options, then I think a proportionate response to that risk would've been for Wise to have provided the associated warning for the payment reason Mr N gave. At best, the closest payment option to the scenario Mr N fell victim to was making an investment so if he'd selected that payment reason he would have received an online written warning which said

"did someone reach out to you unexpectedly about this investment?

Scammers might call or message you with an opportunity, and can be very pushy. Check the company with your local regulator if this happens.

Does the investment sound too good to be true?

If returns sound very high risk, or risks are downplayed, it could be a scam. Check the company with your local regulator first."

But here, Mr N was falling victim to a job scam, not an investment scam. So, while the content of the warning would've related to common investment scams at the time, it wasn't relevant to him. Overall Mr M has said he thought he was dealing with well-known reputable firms, the people he dealt with were professional, with high quality websites and platforms. He wasn't suspicious about what he was being asked to do until much later on when he was asked to deposit a much higher amount, two months after the first payment and having already made 14 payments in total. And none of the scam warnings that would or could have been presented would have provided enough specifics or detail

about the particular scam that he fell victim to, that they would have had any impact on his decision making at the time.

The warning therefore wouldn't have deterred him from going ahead. But I consider this was what was proportionate to the risk at the time.

Alternatively, Mr N might have selected one of the other payment reasons, none of which speak to the specific of the job scam he was falling victim to and again wouldn't have had any impact in deterring him from making these payments.

And importantly based on the risk profile, presented by the payments Mr N was making; individually low value, to new payees spread across a period of time, I'm not persuaded that Wise needed to do more than provide an online written warning.

And I'm not persuaded that Wise ought to have had a job scam specific warning by June 2022. It wasn't required to ask questions of Mr N so it was expected to display a warning based on the payment information it held and the most common scam/s associated with this. While job scams were increasing in prevalence, cryptocurrency investment scams were more prevalent and a warning attempting covering both situations was unlikely to be effective to either scam.

I think there was a second point at which Wise ought to have provided a warning. That's on 19 August 2022, when Mr N made payments of over £8,000, to three new payees. But again, I think an online written warning here would have been proportionate. And I have set out why I think a warning here wouldn't have made a difference.

I don't think intervention beyond a warning was required. At this point Mr N has increased spending on his account over a period of two months, he'd not reported any issues with those payments and although there is an increase on that day, there's nothing else about the payments that means they warrant more than an online warning. I don't think the pattern of the payments made on 29 June 2022 when combined with these on 19 August 2022 are significant enough, given the length of time between them, that Wise ought to have considered human intervention was needed at this point either.

So, in summary I'm satisfied that an appropriate intervention would've been to show a scam warning to Mr N. But that this wouldn't have unravelled the scam for the reasons above. And I don't consider there was any reason for Wise to do more than this and speak to Mr N in this case.

I agree with investigator that whilst the impact of the scam has been a distressing one for Mr N this wasn't the fault of Wise and I can't see that it made an error in deciding not to refund him or otherwise that would warrant a compensation payment made awarded here.

So I'm not minded uphold this complaint.

Following my provisional decision Wise responded to say it had nothing further to add.

Mr N's representative was in touch to say Mr N rejected my provisional decision and does not believe Wise should escape liability.

The representative went on to say it understood Mr N selected the wrong payment purpose but it is well known that scam victims are rigorously coached by scammers on what to say,

The representative referenced a decision on a different case which covered the issue of customers being coached by scammers and the bank having ought to have been aware of that at the time. The representative said Wise has not given this point of view any consideration., despite the clear signs of unusual account activity.

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 have considered the additional points raised by Mr N's representatives. I'll start by saying I think Mr N's representatives have missed the point made in my provisional decision that Wise has not provided evidence to show if it asked Mr N any questions at the time he made the payment. To clarify I haven't made a finding that Mr N picked the wrong payment reason. What I have concluded is that a proportionate response by Wise – in light of the value, pattern and nature of the payments would have been to provide a warning, potentially an investment scam warning, if Mr N had indicated that's what the payments were for.

I acknowledge that consumers are often coached by scammers to select specific payment reasons or to give specific answers if questioned. And banks and payment institutions should be aware of this and take that into account when weighing up any proportionate intervention. But I also have to take into account what would have been a proportionate response to the payments Mr N was specifically making. And, as I've said here the only intervention, I consider to have been proportionate, would have been an online warning. And given that Mr N was making these payments for what he thought was an online job I'm not satisfied any type of warning, that would have been presented to Mr N would have had any material impact on what he was doing.

The fraud and scam landscape is ever-evolving, and it's important that firms continuously update their fraud detection systems to keep up to date with common scams. However, with so many variations of scams out there, we also have to be reasonable about what scams firms can reasonably be expected to build into their warnings systems. And at the time Mr N made these payments, I wouldn't have expected Wise to have questions and warnings tailored towards the key risks of job scams.

So, whilst I'm sorry that Mr N has been the victim of a cruel scam, I can't reasonably conclude that Wise is liable to refund his losses in this instance.

My final decision

I don't uphold Mr N's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr N to accept or reject my decision before 9 April 2025.

Sophia Smith
Ombudsman