DRN-6248759

The complaint

Mr Y complains that Wise Payment Limited ('Wise') declined to reimburse payments which were debited from his account which he says he did not make or otherwise authorise.

What happened

I wrote to both parties outlining my provisional thoughts on this matter in February 2026. The following is an extract from that provisional decision.

"The circumstances of this complaint are well known to both parties, so I will not go into every detail of what happened here. But in summary, Mr Y disputes making two transfers from his Wise account to a third-party account in March 2024. He said that he had various accounts hacked including email, banking and an electronic money institution ('EMI') he had accounts with. Mr Y explained that the EMI has refunded a disputed transaction to the same payee as the Wise disputed transactions.

Mr Y said when he saw the transactions he raised them with Wise. It initially provided a temporary refund whilst they looked into what had happened. It declined Mr Y's claim on the basis that it did not see how an unknown third party could have made the transactions – so it thought that it was most likely that Mr Y had made or otherwise authorised the transactions. It recalled the temporary refund shortly thereafter.

Unhappy with Wise's response, Mr Y escalated his concerns to our service where one of our investigators looked into what had happened. Our investigator recommended that Mr Y's complaint should be upheld on the basis that they thought he did not make or otherwise authorise the transactions. And they said that Wise should reimburse in full, along with 8% simple interest and £150 in recognition of the distress and inconvenience it had caused Mr Y.

Wise did not agree with our investigators' recommendations, so the case has been passed to me to decide.

What I've provisionally 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 am minded to reach a different conclusion to our investigator. But before reaching any final decision, I wanted to outline my initial thoughts in order to allow both parties to provide any additional comments or evidence. If nothing changes, my final decision would be along the following lines.

Can Wise fairly treat the disputed payments as authorised by Mr Y?

Where evidence is incomplete, inconclusive or contradictory, I reach my decision about the merits of this complaint on the balance of probabilities – in other words, what I consider is most likely to have happened in the light of the available evidence and the wider circumstances.

I also have to take account of law and regulations, regulators' rules, guidance and standards, and codes of practice and good industry practice, when I make my decision. And I want to assure Mr Y that if I don't address every point that's been raised, it's not because I haven't thought about it. I have considered everything that's been said and sent to us. But, I'm going to concentrate in this decision on what I think is relevant and material to reaching a fair and reasonable outcome.

The starting position in line with the relevant legislation – The Payment Services Regulations 2017 – is that Wise would be liable for any unauthorised payments, and Mr Y is liable for any authorised payments.

A common situation in which a payment would be considered authorised is where a customer has made a payment themselves. But there are other circumstances in which a payment can fairly be considered authorised – such as where a customer has given permission for someone else to make a payment on their behalf, or where a customer has told their payment service provider that they want a payment to go ahead.

I've thought carefully about the steps that would need to be taken for the two transfers to take place, and whether these could have been completed by an unknown third party. Having done so, I do not think that it was more likely than not that an unknown third party was able to complete these transactions. In summary, this is because:

- *The phone used to complete the disputed transactions had been linked to Mr Y's Wise account in 2023 – the year prior to the disputed transactions. It was used to login to his Wise app and send two undisputed transactions both in the same year.*

- *Mr Y said that the type of device used in these transactions was the same as a phone he had in the past, but it stopped switching on – so he got a new phone. He said he was not sure what had happened to the old phone. It does appear that a new phone was added to his Wise account the month before the disputed transactions, and both were active around the time of the disputed transactions.*

- *I have considered whether an unknown third party could have somehow got hold of his old, broken device. I do not think this is most likely what happened here. I say this because the correct password was used to login to his Wise account just prior to the transfers. There were no password resets or unsuccessful login attempts – and Wise have provided evidence of this.*

- *So, for an unknown third party to have completed these transactions, they would have had to have physical possession of Mr Y's old phone, have somehow got it to work when he said it would not even turn on, to know the device passcode to get into the phone, then to have known his Wise password – or accessed the phone's password app which requires a password or biometric authentication to get into the app and see the passwords.*

- *Mr Y has not been able to say what happened to the old phone, or how someone could have gotten hold of it. He also did not originally mention this phone when asked about device history, but has since accepted he did have a phone of this make and model. I do appreciate that one might lose track of a broken phone – but this leaves me in a bit of a quandary in trying to establish how an unknown third party could have accessed the phone if he cannot tell me where it was. And if the phone was functioning when it was lost – as it clearly was by the time the disputed transactions took place – it would seem unusual that he would not recall what happened to the phone or where it was kept. It would also seem unusual in those circumstances that the loss of the phone was not reported. No such report was made to Wise.*

- *I've considered if there could have been some kind of malware of other software used. Whilst I cannot rule out that clever fraudsters could have worked out a way to infiltrate Mr Y's device, I don't think this is most likely because I have seen no explanation as to how this would have happened – and it would be all the more difficult to do to a broken phone that was switched off somewhere. And the technical evidence does not show any sign of malware or device infiltration. Whilst I cannot say with total certainty that clever fraudsters have not found a way to get into this type of phone without leaving a trace – the chances of this would be very low, and with no evidence in support of this being what happened I cannot say this is most likely what happened here.*

- *I appreciate Mr Y has had other accounts hacked into including his email and EMI – but attacks which allow infiltration into these kind of accounts require different routes into the account, which would not create any kind of access into a mobile phone. So, whilst the EMI has decided to reimburse, this does not mean that the transactions with Wise could be considered unauthorised, and I have to consider the merits of this case separately from any conclusion the EMI reached.*

- *The transactions were verified by someone going into the app when push notifications were sent to the phone, in order to tell Wise that they wanted the transactions to take place. I think it is most likely that this happened on Mr Y's genuine device, and for the reasons I outlined above, I do not see how this could have been done by an unknown third party.*

I do accept that there are strange elements that make me think that something else could have happened here – such as an authorised push payment scam or similar. I say this because of the transactions being set up in a language which as far as I am aware, Mr Y does not speak, and the way the account was drained. But Mr Y has said this was not the case, simply that he never authorised these transactions. And for the reasons I have outlined above, I am currently minded to say I do not think this is most likely what happened here.

And so it would follow that I would not be asking Wise to reimburse the disputed transactions."

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.

Wise did not respond to my provisional findings, but Mr Y did – to disagree and ask me to reconsider. In summary, he said:

- The disputed transactions were part of a coordinated multi-platform attack – including logins and attempted logins on his email and EMI account. Email account compromise can facilitate password resets, security verification interception and so is highly relevant here. The EMI independently assessed the transaction made through it and reimbursed him on the basis it was unauthorised. The transaction was concealed within his account history – which was not done by him and is consistent with account takeover.

- The old device was not under his control – it was lost somewhere (possibly in his vehicle or elsewhere) as he had replaced it due to it being unreliable. It was not within his active control at the time of the transfers. There was no SIM card in that device either.

- Wise ought to have recognised the payment was unusual and a risk of fraud, which should have triggered intervention.

- Mr Y reported the matter immediately. The fact that Wise initially froze the funds and temporarily recredited his account indicates that a fraud risk weas recognised at the time. He wanted clarification about the recall of funds.

- Considering all of the elements of the case, he argued that on the balance of probabilities the cumulative factors are far more consistent with coordinated account takeover than with voluntary authorisation.

I will deal with each point briefly in turn.

On the first point, I have already outlined in my provisional decision that the accounts which were hacked required different routes to get in so do not alter my thinking about the plausibility of a hack on his Wise account. Further to this, the technical evidence from Wise would be able to show if there had been any password resets sent to the hacked email account – and there were not. So it does not provide a point of compromise for the relevant security information to access his Wise account. The decision I am reaching is based on the evidence I have before me, and is not altered by the decision the EMI made in that specific case. And I cannot see a plausible explanation as to how someone unknown to him could have accessed his account or made the payments.

Mr Y has said the old device was not under his control, but he has not been able to explain where it was or provide any evidence in support of this.

There are circumstances where Wise ought to intervene in payments which appear to be unusual or out of character for an account. But a failure to do so alone would not be grounds for me to tell it to reimburse Mr Y here - I would need to be satisfied that a proportionate intervention could have prevented the loss. And I do not think that there is enough evidence that these payments were authorised by someone other than Mr Y to conclude that intervention could have prevented a loss here.

Wise did provide a refund in the first instance. This was not from the funds that had left his Wise account and gone to another account. These were provided because the regulations relevant to this complaint – the Payment Services Regulations 2017 – say that where a customer says that they did not authorise payments they must be reimbursed as soon as reasonably practicable and no later than the end of the following business day. So, the reimbursement was in line with their obligations under those regulations. They are entitled to withdraw the reimbursement if their investigations show that it is more likely that their customer authorised the transactions, as took place here.

Once Wise determined that it thought Mr Y made or otherwise authorised the transactions, I would not expect it to continue with any attempts to retrieve the funds from recipient accounts. The only exception to this would be if Mr Y said that he had made the payments as a result of a scam. This is because if payments are authorised without the element of the scam, Wise had no right to attempt recall of the payments.

So considering all of this on the balance of probabilities, I think it is most likely that Mr Y made or otherwise authorised these transactions.

My final decision

I do not uphold this complaint and require Wise Payments Limited to do nothing further.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr Y to accept or reject my decision before 23 April 2026.

Katherine Jones
Ombudsman