

The complaint

Ms A is complaining that Wise Payments Limited hasn't refunded payments she says she didn't make.

What happened

The circumstances of the complaint are known to both parties, so I'll only summarise them here.

In August 2024 Ms A was contacted by someone (the scammer) who said they worked for her bank. They had some information about her other accounts which made them seem genuine. They explained her accounts had been compromised and she needed to move her money to keep it safe.

Following the scammer's instructions, Ms A opened a new account with Wise and transferred four separate payments of £500 into it. Following this, debit card payments of £500 and £1,400 were made to a money transfer service.

Ms A has told us she wasn't aware of these payments being made and they just disappeared from her account. She says she didn't give the scammer any of her Wise card or account details; they knew them already. After the payments had been made the call to the scammer dropped out, and Ms A called her bank. Her bank told her that it hadn't called her, and she realised she'd been scammed.

Ms A contacted Wise immediately to report what had happened, while the payments were still showing as pending. But Wise told her it couldn't stop the payments. Ms A complained to Wise, and it issued its final response letter on 6 November 2024. It explained that it wouldn't be refunding the disputed payments.

Ms A brought her complaint to the Financial Ombudsman Service, and it was looked into by one of our Investigators. Our Investigator thought Ms A's complaint should be upheld, in part. She concluded that Ms A had authorised the disputed payments, but she thought Wise ought to have identified Ms A was at risk of a scam and contacted her directly before allowing the payments to be made. The Investigator thought that if it had done so, the payments would have been prevented. However, she also thought Ms A's actions meant she should share responsibility equally with Wise. She asked Wise to refund 50% of the disputed payments, with 8% simple interest.

Wise disagreed with the Investigator's view. It said, in summary, that it was unreasonable to have expected it to have intervened directly due to a scam risk, given that this was a new account and the transactions were not high in value. It said it had initially declined the payments attempted to the money transfer service due to a fraud risk and had frozen Ms A's card, but Ms A had unfrozen the card and confirmed that she wanted to complete this sort of transaction in future. It also said Ms A had completed its stronger authentication process to confirm the disputed payments. It felt it had done enough to establish the payments were genuine.

Ms A feels strongly that Wise's systems must have been hacked, or that an employee was involved, which resulted in the scammer knowing her secure details.

Ms A's complaint was passed to me for review and a decision.

I issued my provisional decision on 4 December 2025. I told both parties that I had provisionally decided not to uphold Ms A's complaint. This is what I said.

"Did Ms A authorise the payments?"

The relevant law here is the Payment Services Regulations 2017 (PSRs) – 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. Ms A disputes authorising the payments, so I'll address this point first.

The PSRs specify that authorisation depends on whether the payment transactions were authenticated correctly – and whether Ms A, or someone acting on her behalf, consented to them.

The PSRs go on to specify consent must be given in the form, and in accordance with the procedure, agreed between Ms A and Wise. I've reviewed the terms of Ms A's account with Wise and in relation to making debit card payments they say the following:

"You authorise every transaction. You agree that any use by you of your Card, card number or PIN constitutes your authorisation and consent to the transaction."

So, they don't specify exactly how Ms A gives consent to card payments. But broadly speaking, this is usually through entering the long card number, the card expiry date and CVV into the merchant's website (in this case, the website of the money transfer service).

Ms A says she didn't share her card details and it's not clear how the scammer gained access to them, as this was a brand-new account. However, from what she says it seems it was the scammer who gave the payment instructions using Ms A's card details. If this was the case, then Ms A didn't agree to the payment instructions. But Wise says the payments were authorised because Ms A confirmed the payments using its stronger authentication process.

Wise has sent us some screenshots to show that the process flow here has steps which involve receiving a notification showing a payment is waiting to be reviewed, which then opens a screen asking for the payment to be reviewed. The payment amount and who it's being made to is shown on the screen with an option to approve or deny the payment.

I've seen evidence that the disputed payments were approved on the same mobile device used to open the account with Wise (which Ms A says she did) and the same device was used to access Ms A's account until 24 October 2024. I must conclude that this is Ms A's device, which remained in her possession throughout. This was the only device that accessed Ms A's account on the day the account was opened and the disputed payments were made, and the IP address is also the same throughout.

I appreciate that Ms A says she didn't approve the payments, but this wouldn't explain how Wise's records show the payments being approved on her own device. I know Ms A thinks either her account was hacked or a Wise employee was involved in making the payments, but the technical evidence doesn't support this. Overall, I think it's likely Ms A did approve the payments using the stronger authentication process Wise has outlined.

Although Ms A says she didn't enter her card details or approve the payments, I'm satisfied that the payments were correctly authenticated using her card information and stronger authentication. I do appreciate how frustrating this must be for her when she feels strongly that this isn't what happened - but I must make my decision based on the available evidence I have, and from that evidence it does appear that she authenticated the payments. So, I think it was reasonable for Wise to consider the payment instructions to be genuine and to process the payments. As such, it's reasonable for Wise to treat the payments as having been authorised and it's not obliged to provide a refund.

Should Wise have recognised the scam and intervened?

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

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 payment. 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.

I've thought about this point carefully. But I don't think Wise ought to have done any more than it did here to prevent the disputed payments.

Ms A's account was newly-opened so there wasn't any account activity for Wise to compare the payments to, to decide if they appeared to be unusual – it would have been relying on generic indicators to identify if Ms A was at risk of a scam. But the payments here weren't of a value where I'd generally expect Wise to have been concerned that Ms A was at risk of financial harm through a scam.

I appreciate that the Investigator has identified the payments Ms A made into the account as suspicious because the movement of the funds in four lower amounts rather than a single, higher value payment was characteristic of the type of scam she was experiencing. But there are other reasons why Ms A could have made the payments into the account in the way she did, and in any case I wouldn't expect Wise to have picked up on this unless it had a reason to take a closer look at the activity on Ms A's account as part of a scam intervention, and I don't think it did here.

It's clear that Wise did identify some risk in the account activity, because it froze Ms A's card and declined payments to the money transfer service until the card was unfrozen and Ms A had confirmed she'd seen a screen which said "This transaction could be a scam. Confirm if you want to allow this type of transaction in the future." It was only after Ms A unfroze her card and pressed confirm on this screen that it allowed the disputed payments to be made. I understand that Ms A says she didn't take these steps, but the technical evidence does show that her mobile device was the only device that accessed her account when this was done.

So, Wise did take some steps to satisfy itself that it was Ms A completing the transactions and was reassured by the response it received. I think this was proportionate in all the circumstances here, and I wouldn't have expected Wise to have intervened by contacting Ms A directly.

Could Wise have done more to recover the payments?

When a payment has been made by debit card it can't be recalled or cancelled, even in a pending state.

It's possible to dispute a debit card payment through a process called chargeback, which can sometimes be attempted if something has gone wrong with a debit card purchase, subject to the relevant card scheme's rules.

Wise doesn't appear to have raised chargebacks when Ms A disputed the payments, but I'm satisfied that there would have been little prospect of chargebacks being successful here. I say this because I've concluded the payments were authorised by Ms A, and also because the payments were made to a legitimate money transfer service which would have provided the service in transferring the funds.

Like the Investigator, I don't think Wise made any errors or gave Ms A a poor service when she reported what had happened, or in the way it dealt with her complaint.

Once again, I'm really sorry to disappoint Ms A. She's been the victim of a cruel scam and I can understand why she'd think she should get her money back. But from what I've seen so far, I've not found that Wise ought to have done anything else here. So, I don't think it would be fair or reasonable to ask it to refund the disputed payments.

Ms A replied to my provisional decision to make it clear she didn't agree. She said I'd not taken into account that the scammer had her Wise account details so Wise must have been hacked – and she said she didn't authorise anything, the scammer did.

Wise didn't reply to 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.

I appreciate that Ms A is unhappy with the findings in my provisional decision and feels strongly that Wise was hacked and that she didn't authorise any of the payments. But as I've explained, the technical evidence doesn't support this.

Although I'm sorry to disappoint Ms A, I see no reason to depart from my provisional decision that I'm not upholding her complaint.

My final decision

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

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms A to accept or reject my decision before 16 January 2026.

Helen Sutcliffe
Ombudsman