

The complaint

M, a limited company, complains that Wise Payments Limited (“Wise”) won’t refund the money it lost to a scam.

The complaint has been brought by M’s director (I’ll refer to as “Miss N”) and through a representative. For simplicity, I’ll generally refer to M and Miss N throughout this decision.

What happened

The background is known to both parties, so I won’t repeat all the details. In summary, Miss N explains that M is a small business she had recently established and had registered to sell goods on a well-known online marketplace (“E”). On 16 June 2025, she received an email that appeared to be from E, advising that an order had been received.

The email directed her to a portal that looked identical to E’s platform – but was actually a clone of the genuine site – and explained that, as a new seller, Miss N needed to complete a “verification process” by following “support agent” instructions she was given through the spoofed portal’s chat function. Believing the contact was genuine and that she was completing a routine verification process, Miss N followed the instructions.

This led to Miss N providing M’s card details and then approving a payment in her Wise app which she was told would be refunded immediately. Miss N was then instructed to repeat the process because the “verification” had supposedly failed. It was only after the third attempt, when more money was being requested, that she realised she had been scammed. By that point, a total of £1,848.87 had been taken across three card payments. These were made to a merchant (“G”) which Miss N didn’t recognise. Within minutes, she froze the card and tried to cancel the payments within the Wise app, but this was unsuccessful.

Miss N reported the scam to Wise. A complaint was raised and referred to our Service. Our Investigator didn’t uphold it. In short, she was satisfied the payments should be treated as authorised. She wasn’t persuaded Wise had missed an opportunity to prevent the scam given, for example, the amounts involved. And she didn’t think there were significant failings by Wise in terms of recovery or the service provided such that a compensation award is warranted. As the matter couldn’t be resolved informally, it’s been passed to me to decide.

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, I’ve decided not to uphold it for similar reasons as the Investigator. Miss N will understandably be disappointed but these are the key reasons for my decision.

Can Wise fairly treat the payments as authorised?

The starting point – under the Payment Services Regulations 2017 (PSRs) – is that M is liable for authorised payments. With some exceptions, Wise is liable for unauthorised

ones. A payment is usually considered authorised when a customer makes it themselves. But it can also be treated as authorised if the customer allows someone else to make it on their behalf or if they tell their payment service provider they want a payment to proceed.

In this case, Miss N appears to have interacted with only E's spoofed portal and provided M's card details believing she was following genuine instructions from the chat. It seems the scammer likely used those details to initiate payments on G's website. But Miss N has also explained, for example, that she was told she had to "verify her account by making a payment, which would be immediately refunded".

Even though I appreciate Miss N didn't complete all the steps to make the payments, was under the influence of a convincing scam, and was tricked about the wider context, it's accepted she provided the card details on the understanding that this information would be used to complete a "test" transaction from the account and money would be taken and refunded. It is also on this basis that she approved the in-app notification that followed.

Miss N also accepts that she approved further notifications in the app. This is supported by Wise's technical evidence. And I think it matters that all the payments were approved using strong customer authentication (3DS). The approval screens asked "*Authorise your online purchases?*". They displayed key information, including merchant and amount, and offered options to approve or decline. As Wise clearly asked Miss N if she wanted each payment to proceed, and the prompts were unambiguous, I think it was reasonable for Wise to rely on the steps Miss N took as her consenting to the payments. And so, for the payments to be treated as authorised. As noted by the Investigator, under the PSRs, the validity of a payer's consent doesn't depend on whether the full context of the payment was explained to them.

Should Wise have done more to prevent the scam?

In general, the starting point at law is that Wise is expected to process payments and withdrawals that a customer authorises it to make. However, taking account of relevant law, regulatory rules and guidance, industry codes of practice, and what I consider to have been good industry practice at the time, Wise should also have taken additional steps or made additional checks, before processing a payment in some circumstances.

Looking at the account, the payment amounts and merchant involved, I'm not persuaded Wise failed to intervene at a point when it should have suspected that M was at a heightened risk of fraud. The payments, while not insignificant, would not have appeared as particularly concerning in value. And although they were made in quick succession, I'm not persuaded such a suspicious spending pattern developed to the extent that Wise ought to have stepped in. In reaching this view, I'm mindful that all payments were made to what appears to be a genuine merchant, with no official warnings, and 3DS approved. I'm also mindful that M's is a business account where fluctuations in spending can reasonably be expected at times.

Could Wise have done more to recover M's money?

As the disputed transactions were card payments, a potential recovery route for Wise was the chargeback scheme. Chargeback is operated by the card scheme provider to resolve disputes between customers and merchants, subject to the scheme rules.

Participation is voluntary and the scope limited. Wise wouldn't be expected to raise a claim it believed had no realistic prospect of success. As the Investigator explained, a chargeback on fraud grounds was unlikely to succeed because the payments were 3DS approved. Since the payments were made to what appears to be a legitimate merchant, it's also unlikely a claim would have succeeded as the merchant likely provided the goods or services, albeit to

a scammer. Here Wise has shown it did submit an automated recall request to the merchant through Visa but received no response. I note Miss N also contacted the merchant and some of her questions remain unanswered. However, for the reasons above, it wasn't a failing on Wise's part not to raise a chargeback when there was no realistic prospect of success.

Other matters

Miss N says that when she realised she had been scammed, she went into the app to try to cancel the card payments and clicked an option to do so, but it didn't work. She believes this was either a technical error or misleading. I understand her point but I don't agree that Wise should be held responsible because of this. Once the card payments were approved, Wise wouldn't have been able to stop the funds from leaving the account. And I'm not persuaded Miss N made the payments because of, or in reliance on, any 'cancel' button in-app or any public posts providing general information on cancelling transactions after the event.

Miss N also says she was distressed because it took her over five minutes, in a state of panic, to find a contact number. She noted other firms offer 24/7 fraud support with clearly displayed contact numbers. I don't underestimate the amount of stress these scams can cause and I recognise Miss N did all she could once she realised what had happened. As I've explained, the payments couldn't have been stopped once approved and I don't think Wise acted unfairly in not pursuing a chargeback. Although Wise doesn't have a 24/7 phone line, that's a business decision it's entitled to take. Its site had information on how to report fraud and Miss N was able to do so within minutes of the last transaction, even though I can appreciate why she would have liked to have spoken to someone at the time it happened.

Wise acknowledged Miss N's scam report and she did speak to Wise the following day. I can understand why Miss N wanted a quick response and to speak to a manager. But I don't think it was unreasonable of Wise to explain that she needed to wait for the relevant team to complete its investigation. It was explained an update would be provided once there was progress. Wise then issued its dispute outcome on 18 June 2025. It recommended that Miss N contact G to report the fraud. I don't think that was unreasonable. In the meantime, Miss N had raised a complaint. On 23 June 2025, Wise acknowledged it, setting out the next steps and signposting her to support organisations. It then issued its response on 27 June 2025.

I don't consider there to be any significant failings or breaches on Wise's part that would justify a compensation award. I would add that while I'm mindful of everything Miss N has shared with us about her personal circumstances and I'm sorry the whole experience has affected her deeply, I can't reasonably hold Wise responsible for any distress caused by the actions of a fraudster. It's also relevant to note that we can only make awards for distress and inconvenience suffered by the complainant. M, as the account holder, is the eligible complainant here. As a limited company, M cannot suffer distress.

My final decision

For the reasons I've given, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask M to accept or reject my decision before 29 April 2026.

Thomas Cardia
Ombudsman