DRN-5478391

The complaint

Miss U complains Wise Payments Limited ("Wise") declined to refund payments she says she didn't make.

What happened

On 31 December 2023, Miss U received a call from someone claiming to be from one of her banking providers. In the days prior to the call, she'd responded to a 'missed delivery' email where she provided her card details for her other banking provider, though she later had doubts about the email. In the call she shared her date of birth and was told there had been attempts to use her account so in order to keep her money safe, she would need to transfer money to a temporary account to keep it secure. She was told to open a Wise account and having realised she already held one, she transferred money from her other account into her Wise account.

Not long after, she noticed two payments leave her Wise account, the first for £2,400 and the second for £3,090 to the same cryptocurrency merchant. She then raised a fraud claim with Wise, but it didn't agree to refund her.

Following a complaint made by Miss U, Wise issued its final response letter on 19 February 2024. In summary it said the payments were approved via codes sent to her phone and as it was unsuccessful recovering the funds, it didn't consider it was liable to refund her. Unhappy with its decision, Miss U referred her complaint to our Service.

One of our investigators looked at Miss U's complaint and upheld it. They said they didn't consider Miss U had authorised the payments and as they didn't consider she failed with gross negligence, they recommended Wise refund Miss U her full loss. Wise didn't agree. It considered Miss U authorised the payments by sharing over the codes sent to her phone, and the messages containing the codes explained they were to authorise payments. As Wise didn't agree, the matter was passed to me to decide.

I issued my provisional decision on 28 March 2025 where I upheld this complaint. Miss U agreed but Wise didn't agree. I've summarised its points below:

- The software on Miss U's device at the time only permitted remote viewing, not control, so it wouldn't have been possible for a third-party to have taken full control of her phone.
- Further to that, Miss U would have had to have taken several steps to download the remote software programme that would have required conscious engagement with multiple areas of her device, and so it's unlikely to have been done by accident. And given these technical limitations, it considers the logical conclusion is that Miss U verbally shared her security information.
- There was no clear justification that the third-party could have provided for Miss U to have created a digital card and for Miss U to then share it other than for the purpose of making a payment.
- Based on the one-time passcode ("OTP") messaging, there was no possibility for doubt that a payment was about to be made.

- It maintains that the actions Miss U took meant she authorised these payments.

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 uphold this complaint. I'll explain why.

The dispute here is around whether Wise has acted fairly in treating the disputed payments as authorised. Wise says this is because Miss U shared information which resulted in the payments being made. My role is to decide what's more likely than not to have happened based on the information that is available.

In line with the Payment Services Regulations 2017 ("PSRs"), the relevant legislation here, the starting position is that Wise is liable for unauthorised payments, and Miss U is liable for authorised payments.

I've started by considering what authorisation means under the PSRs. One part is that the payments must have been properly authenticated. The technical data Wise has provided shows the disputed payments were made online using Miss U's card details, and each payment prompted a one-time passcode ("OTP") that needed to be inputted into the merchant's website. So I'm satisfied therefore the payments were authenticated correctly.

Correct authentication isn't enough to deem the payments were authorised. The PSRs say that Miss U must also have given her consent to the execution of the payments. In practical terms, it means Miss U consents to payments by completing the agreed steps as set out in the terms and conditions of the account, or by allowing someone else to complete the steps on her behalf.

Considering how the disputed payments were carried out, Wise's terms and conditions sets out the following on authorising card payments:

> *"19.1 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."*

Wise has provided technical data that shows a digital card was created from Miss U's phone device. This was the same device Miss U used where she was guided to open her Wise account during the scam. And importantly, the card details didn't exist until she created the digital card, which happened during the call with the fraudster. So I don't consider it likely the card details could have been compromised prior to the fraudster's call. But around two minutes after it was created, the digital card details were then viewed on Miss U's device.

Further to that when both payments were made, both required OTPs that were sent to Miss U's phone, and Wise has shown these were required for the payments to have successfully gone through. Miss U has shown she received the codes, and has mentioned she was told by the fraudster she would be given a code that she would need to share verbally.

We can't know for certain what happened here, and I can only decide what I think is more likely than not to have happened. Miss U has described clicking on links she was provided during and before the scam call, one of which was in relation to a phishing email she received days prior to the call. So one possibility is that she may have clicked on malware or given remote access without realising it.

Wise argues that Miss U would have needed to take several steps to download a remote

software programme that would have required conscious engagement with multiple areas of her device. And given these technical limitations, it considers the logical conclusion is that Miss U verbally shared her security information. This may be the case, but without knowing what programme may have been used I don't think it would be fair to speculate as to the process she would have followed. I explained in my provisional decision that it's also possible she shared her card details and I'll address that further below.

I note Wise says that remote software on Miss U's device would have only permitted the fraudster remote viewing, not control. But that would be enough to explain how the fraudster could have seen her secure information.

However, I also accept the possibility that Miss U shared over her card details and OTPs but hasn't otherwise recalled doing so because of the pressure she was being put under by this individual where she was falsely led to believe her money was at risk. And that she needed to take steps to keep her money safe in her Wise account. It's common for scammers to use sophisticated techniques to manipulate their victims, and so I'm mindful that Miss U may well have been following the scammers instructions without appreciating the full context or impact of her actions.

Given the overall circumstances of how the scam was unfolding, and as Miss U hasn't said she was guided at any stage to the cryptocurrency merchant's website, I consider it most likely it was the fraudster that input Miss U's card details and the OTPs into the merchant's website.

Miss U accepts she moved funds from another bank account she held into her Wise account but has been consistent in saying that she didn't make or give someone consent to make these payments. She said the fraudster explained that to keep her money safe she would need to transfer money to a temporary account to keep it secure, which was the Wise account.

Wise argues that there was no clear justification that the fraudster could have given Miss U as to why she needed to create a digital card, and for it to have then been shared over other than for the purpose of making a payment. But I don't think that's a reasonable conclusion to draw in the circumstances - there could be several possible scenarios as to why she was directed to create a digital card that didn't involve understanding payments would be made. We know that Miss U believed she was creating a temporary account, and so I think it's more likely that this was simply part of setting up the Wise account. Unfortunately, we don't know why Miss U shared the card details (if that's what happened), there are several false reasons the scammer could have provided to persuade her of this.

Wise explains that the OTP message was clear a payment was being made. But that alone doesn't therefore mean Miss U authorised these payments. Given what Miss U has explained, I do consider it more likely than not that she believed her money would stay in her Wise account and that she wasn't of the understanding that money would be moving out of her Wise account during her call with the fraudster. It's common in scams, like the one Miss U fell victim to here, for the victim to be told to set-up a new account and move money from a 'compromised' account into a new account, that the victim opens, where their money would remain and be safe. And if Miss U did share the OTPs I think it's more likely than not, based on what she's told us she understood was happening, that she didn't read the content of the messages or understood that by sharing the information, she would be enabling the fraudster to make payments on her behalf given the pressure she said she was being put under.

I've considered Wise's points about why it thinks Miss U authorised these payments. As I consider it most likely it was the fraudster that carried out the agreed steps, and Miss U

didn't give consent for the payments to be made on her behalf, I'm persuaded the two disputed payments were unauthorised.

Did Miss U fail in her obligations with gross negligence?

The PSRs set out Wise can hold Miss U liable for unauthorised payments in certain circumstances. Of most relevance here is if she failed with gross negligence in her obligation to take all reasonable steps to keep safe personalised security credentials and to use the payment instrument in accordance with the account terms and conditions.

When I'm considering if Miss U has failed in her obligations with gross negligence, I need to consider that the test isn't simply whether someone was careless. For someone to fail with gross negligence they would need to have seriously disregarded an obvious risk, falling significantly below the standards expected of a reasonable person.

Miss U received a call from someone claiming to be from one of her banking providers. In the days prior to the call, she'd responded to a 'missed delivery' phishing email where she provided her card details for her other banking provider. She was asked to confirm her date of birth and she was told there had been attempts to use her account fraudulently. I can appreciate, given her doubts after responding to the email she received where she shared her card details for the account provider who the fraudster claimed to be calling from, why she believed the call was genuine.

Miss U has explained she doesn't recall sharing card details with the fraudster but mentioned sharing a code, and has explained that she was put under pressure by the fraudster. It's common in scams like these for fraudsters to pressure people into taking steps they believe is to keep their money safe and often don't realise what they've shared at the time. Or see the full content of messages sent because of the pressure they're put under to act quickly. And fraudsters often create doubt through sophisticated techniques to persuade the victim their money is at risk by claiming to be a provider they have a relationship with. Here, Miss U was told someone had attempted to use her account and that an investigation needed to be carried out whilst they resolved the issue with her account which meant moving her money into another account of hers. And as she had doubts about the phishing email she received, she was ultimately tricked into believing her account was at risk.

I consider the actions Miss U took was to protect her money, and under pressure from the fraudster. And given the circumstances of the scam here I don't think she seriously disregarded an obvious risk at the time in the steps she took to safeguard her money. It follows that I don't think Miss U's actions were grossly negligent.

Taking everything into account, I'm not persuaded Wise has shown Miss U failed in her obligations with gross negligence and I don't think there's any other reason Wise can fairly hold her liable for her loss. So in line with the PSRs, it needs to put things right by refunding the two unauthorised payments along with paying interest to compensate her for the time she's been without her money.

My final decision

My final decision is that Wise Payments Limited should:

- Refund Miss U the unauthorised payments in full, less any funds that have since been refunded or recovered.

- Pay 8% simple interest per year on these amounts from the date of loss to the date of settlement (if Wise Payments Limited considers that it is required by HM Revenue

& Customs to withhold income tax from that interest it should tell Miss U how much it's taken off. It should also give Miss U a tax deduction certificate if she asks for one so she can reclaim the tax from HM Revenue & Customs if appropriate).

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss U to accept or reject my decision before 15 May 2025.

Timothy Doe
Ombudsman