

The complaint

Miss V complains that Wise Payments Limited won't refund the money she lost after she was the victim of a scam.

What happened

In early 2023, Miss V saw an advert for a cryptocurrency investment company on a social media platform. She says she checked online reviews of the company, as well as its profiles on other social media websites, but didn't see anything negative and so filled in an application form. She was then contacted by an account manager from the investment company who guided her through opening electronic wallets, purchasing cryptocurrency through a cryptocurrency exchange, and then sending this cryptocurrency to the company's trading platform.

Miss V made two payments from her Wise account to a cryptocurrency exchange to purchase cryptocurrency, as set out below:

Date	Amount
15 March 2023	£2,499
28 March 2023	£1,999

She then says she was speaking to the cryptocurrency investment company and gave the person she was speaking to remote access to her device so they could show her documents about her investment. But the person then accessed her bank account and made another payment to the cryptocurrency exchange she hadn't agreed to, as set out below:

Date	Amount
30 March 2023	£3,700

The company said it would call her back shortly afterwards to complete a withdrawal but, when it didn't call her back, Miss V realised she'd been the victim of a scam.

Wise investigated but said it thought all the payments were approved by Miss V, with notifications sent to her phone. It also said it didn't think the payments were unusual and so wasn't responsible for the money Miss V lost. Miss V wasn't satisfied with Wise's response, so referred a complaint to our service.

I sent Miss V and Wise a provisional decision on 19 April 2024, setting out why I was intending to uphold this complaint in part. An extract from my provisional decision is set out below:

"Did Miss V authorise the payments?"

Miss V accepts she made the first two payments here, on 15 March and 28 March 2023. But she says the third payment, on 30 March 2023, was made by the investment company and she didn't agree to it.

Generally a business can hold a customer liable for disputed transactions on their account if the evidence suggests it's more likely than not that the customer authorised the payments – for example, by making them themselves or telling someone else they could make them.

Deciding whether a customer has authorised payments is a two-part test. Firstly the payments must be authenticated, and secondly, the customer must have consented to the payments being made. And this doesn't necessarily require proving that the customer made the payments themselves, as it is possible for a customer to consent to someone else making payments on their account.

Wise has sent us evidence which shows all three payments were made using Miss V's card details. This means the payments were all correctly authenticated, and so I must also think about whether the evidence suggests it's more likely than not that Miss V consented to all of the payments.

I've thought very carefully about this and I think it's a finely balanced matter in this case. But where the evidence available is unclear or inconclusive, I must make my decision on what I think is likely to have happened, based on the evidence I do have.

Miss V says she didn't agree to the third payment but Wise's evidence shows that, for all of the three payments, a message was sent to Miss V's mobile phone saying she was making a payment and asking her to tap to confirm it was her – and that the payment was confirmed each time. It also shows that the message for the third payment was sent to the same phone number as both of the first two payments.

Wise's evidence also shows that the IP address used when the third payment was being set up was the same as the IP address used when setting up the second payment, which Miss V accepts she did. And that the device used to log in to Miss V's online banking when the third payment was being set up was the same device used to log in when the first two payments were made.

So in order for the scammers to have made the payments without Miss V's knowledge or consent, they would have had to have access to and control over both her phone and the device used to log in to her online banking – which I think is unlikely. And even if the scammers did have control over the phone and the device, they were both still in Miss V's possession and she would have been able to see the activity on them. But she doesn't appear to have disputed the payment with Wise until after the scammers failed to complete her withdrawal, and so appears to have accepted it being made.

Based on the evidence I have, and in the absence of any other likely explanation, I think it's likely Miss V was aware of the third payment here and did consent to it – either by making it herself or allowing someone else to make it. And so I think Wise has acted reasonably in treating this third payment as authorised.

Did Wise do enough to protect Miss V?

While I think Miss V authorised all the payments, where a customer makes a payment as a consequence of the actions of a fraudster, it may sometimes be fair and reasonable for the account provider to reimburse the customer – even though they authorised the payments.

Account providers are expected to make payments in line with their customers' instructions. And, for the reasons I've explained above, I think Miss V did authorise the payments here. So while she may not have intended for the money to go to scammers, the starting position in law is that she is liable for them and Wise doesn't have to refund the money she lost.

However, the regulatory landscape, along with good industry practice, sets out requirements for account providers to protect their customers from fraud and financial harm. So, in line with this, I think Wise should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and 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 banks 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, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

So I've also considered whether Wise should have identified that Miss V was potentially at risk of fraud as a result of these payments.

The first two payments made as a result of the scam weren't for what I'd consider to be particularly large amounts. And the account had only been opened relatively recently and so there wasn't a significant period of account history for Wise to compare the payments to when assessing whether they were out of character. So I wouldn't have expected Wise to identify that Miss V could be at risk of financial harm as a result of these payments, and I don't think it's unreasonable that it didn't take any further steps before allowing them to go through.

But when Miss V tried to make the third payment here, for £3,700 on 30 March 2023, I think Wise should have identified that she could be at risk of financial harm. This payment was for a significantly larger amount than the two previous payments made out of her account. It was also made to an account that was identifiably related to cryptocurrency, as it was made to a company whose main business is operating a cryptocurrency exchange. And by early 2023 I think Wise ought to have recognised that cryptocurrency related transactions carried an elevated risk of fraud, as there had been widespread coverage in the media about increased losses to cryptocurrency scams and many firms had placed blocks or restrictions on cryptocurrency related transactions.

So I think the combination of the amount of these payment and the fact it was identifiably related to cryptocurrency should have caused Wise concern that Miss V was at risk of financial harm from fraud. And, in line with good industry practice at the time, I would have expected it to provide her with a written warning about cryptocurrency investment scams and some of their typical features.

What difference would a warning have made?

Given the size of this payment and the risk I think it should have identified, I think it would be reasonable to expect Wise to have provided Miss V with a tailored written warning relevant to cryptocurrency investment scams, tackling some of the key features of the scam.

I've not seen anything to suggest Miss V was coached by the scammers to ignore any warnings her account provider gave her, so I think it's likely she would have read and considered any warning Wise gave. And as Miss V was not an experienced investor and

Wise was the expert in financial matters in this situation, I think any warning or concerns it raised would have carried significant weight with her.

If Wise's warning had mentioned cryptocurrency investment scams offering returns that were too good to be true, being endorsed by celebrities or well-known personalities, using fake trading platforms or being managed by an account manager – which are all common features of cryptocurrency investment scams – I think it would have resonated with Miss V, as these features were all present in her case. I think she would likely have recognised that the cryptocurrency investment company was a scam and wouldn't have continued to make the payment.

And so if Wise had done more to protect Miss V before she made the third payment, as I think it should have, I don't think she would have lost the money from this payment. And so I think it would be reasonable for Wise to bear some responsibility for the loss Miss V suffered from this payment.

Should Miss V bear some responsibility for her loss?

I've also thought about whether it would be fair for Miss V to bear some responsibility for her loss. And while I appreciate that this was a sophisticated scam where she was given access to a trading platform which appeared to show trades being made and profits she was making, I do think there were a number of things about what was happening that should have caused her significant concern.

After seeing the advert on social media, she doesn't appear to have done significant checks into who the investment company were or seen any independent evidence of the returns they had been able to get for other investors. And given the amount of money she was sending them, I don't think it was reasonable for her to rely solely on the advert and lack of negative information online and I think it's reasonable to expect her to have done more checks than she did.

Miss V doesn't appear to have been sent any documents or paperwork relating to the investments she was making. And given the amount of money she was investing and that she thought she was investing through a professional company, I think this lack of documentation should have caused her concern. Miss V also doesn't appear to have been given a particularly clear explanation, or have had a particularly clear understanding, of what she was investing in or how the profit was generated. And I think it would be reasonable to expect her to have a clearer understanding of these things before investing the amount of money she did.

Miss V also appears to have been told she had made very significant returns on the money she had invested. From what she's told us and the copies of communication between her and the company she's sent us, she was told she was earning profit of between 30 – 50% of the amount she invested in just a few days. She also doesn't appear to have tried to withdraw any of her investment, or seen any evidence she could access the profit she was told she had made. And I think being told she had achieved such high returns in such a short period of time should have caused her significant concern that what she was being told was too good to be true.

I sympathise with the position Miss V has found herself in. She has been the victim of a cruel and sophisticated scam. But I think there were a number of things here which should have caused her significant concern. And I don't think she did enough, or that the seemingly genuine information she received from the company should have been enough, to overcome those concerns. So I think it would be fair for her to also bear some responsibility for the loss she suffered.

As I think both Miss V and Wise should bear some responsibility for the loss she suffered, I think it would be fair for Wise to refund 50% of the money Miss V lost from the third payment she made.”

I said I'd consider anything further Miss V and Wise sent in following the provisional decision, provided it was received by the deadline given.

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.

Miss V responded to the provisional decision saying she was happy to accept it. And Wise didn't respond to the provisional decision.

So as neither Miss V nor Wise submitted any further evidence or arguments following it, I still think the conclusions I set out in the provisional decision are correct – and for the same reasons.

I still think both Miss V and Wise should bear some responsibility for the loss she suffered, and that it would be fair for Wise to refund 50% of the money Miss V lost from the third payment she made onwards.

My final decision

For the reasons set out above, I uphold this complaint in part, and require Wise Payments Limited to:

- Refund Miss V 50% of the money she lost from the third payment – for a total of £1,850
- Pay Miss V 8% simple interest on this refund, from the date of the payments until the date of settlement

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss V to accept or reject my decision before 20 June 2024.

Alan Millward
Ombudsman