

The complaint

Mrs M has complained that Wise Payments Limited (“Wise”) failed to protect her from falling victim to a scam.

What happened

The background of this complaint is already known to both parties, so I won’t repeat all of it here. But I’ll summarise the key points and then focus on explaining the reason for my decision.

Mrs M has used a professional representative to refer her complaint to this service. For the purposes of my decision, I’ll refer directly to Mrs M, but I’d like to reassure Mrs M and her representative that I’ve considered everything both parties have said.

Mrs M explains that she was introduced to a cryptocurrency investment platform, which I’ll call “C”, via social media. She said the company presented itself as a legitimate investment opportunity, attracting a large number of unsuspecting investors through its website and app, which was publicly available, as well as using fraudulent celebrity endorsements. She says she was persuaded to invest by promises of guaranteed returns, starting with an entry-level rate of 2.5% interest on investments. As a further incentive, investors were told that higher deposits or recruitment of additional investors could increase their guaranteed return to 2.8%. Mrs M says she communicated with the scammers using an messaging application, and they were always knowledgeable and professional. She also says she was added to several group chats where other alleged investors would discuss their investments.

Mrs M says she was convinced by the scam as she checked online reviews of the company, as well as reading online articles, although she now believes these were planted by the scammers.

Mrs M says that the scam reached its peak when C introduced a Thanksgiving bonus, promising to double any deposits made within a 48-hour window. Mrs M was convinced to invest during this period, hoping to capitalise on the bonus. But when Mrs M attempted to withdraw her funds she encountered delays and ultimately discovered that the withdrawals were never processed.

Initially, C claimed the issue was due to a technical problem with the cryptocurrency wallet platform, but that platform confirmed that no legitimate transactions had been made. C then blamed hackers for the loss of funds and began encouraging investors to use another cryptocurrency exchange, initiating what Mrs M says appeared to be a recovery scam.

The payments Mrs M made were as follows:

Date	Amount (£)
30/10/2023	1,255.50
30/10/2023	42.50
30/10/2023	865.85
4/11/2023	254.70

20/11/2023	5,000
20/11/2023	399.26
21/11/2023	211.07
22/11/2023	213.79
1/12/2023	82.48
Total	8,325.15

Mrs M realised she'd been scammed when she wasn't able to make any withdrawals of her profits, so she made a complaint to Wise. She said that the payments in question were out of character compared with her usual account activity. She also said that if Wise had intervened, the scam would've been exposed, and the financial loss would've been prevented. Wise didn't uphold the complaint.

Mrs M remained unhappy so she referred the complaint to this service.

Our investigator considered everything and didn't think the complaint should be upheld. She explained that she thought the warnings Wise had given to Mrs M for five out of the nine payments made were proportionate to the identifiable risks of the payments.

As Mrs M didn't accept the investigator's opinion, the case has been passed to me to make a 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'm sorry to disappoint Mrs M but having considered everything I'm afraid I'm not upholding her complaint, broadly for the same reasons as our investigator, which I've set out below.

In broad terms, the starting position is that a firm is expected to process payments and withdrawals that its customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And in this case it's not in question whether Mrs M authorised these payments from leaving her account. It's accepted by all parties that Mrs M gave the instructions to Wise and Wise made the payments in line with those instructions, and in line with the terms and conditions of Mrs M's account.

But that doesn't always mean that the business should follow every instruction without asking further questions or intervening to ensure requests coming from their customers are firstly genuine, and secondly won't result in harm.

Wise says that each time Mrs M created a new payee and attempted to make one of the payments, it firstly asked her for the purpose of the payment. It says that for some payments Mrs M selected that she was paying for "goods or services" and for others she selected "investment". Wise says that it then showed Mrs M a warning corresponding to the purpose of the payment that she'd chosen for five out of the nine payments and gave her the option to proceed with the payment or cancel it. The payments Wise didn't show a warning for were the ones of £42.50, £399.26, £213.79 and £82.49.

Where Wise showed a warning for the payments Mrs M said were for an investment, I can see the warnings showed two questions that it encouraged Mrs M to consider "did someone reach out to you unexpectedly about this investment?" and "does this investment sound too

good to be true?”. The next screen said “Stop – this sounds like a scam” and at that point Mrs M was given the option to proceed with the payments or cancel them.

For the payments where Mrs M was shown a warning related to “paying for goods or services” Wise again asked two rhetorical questions; “Are you buying from a website like Airbnb or eBay?” and “Do you know and trust the company you’re buying from?”. It again followed these screens with “Stop – this sounds like a scam” and gave Mrs M the option to proceed with the payments or cancel them.

Although Mrs M explains the payments she made were ultimately to buy cryptocurrency, I can see that they were in fact made to individuals, as opposed to cryptocurrency trading platforms. Wise has evidenced through its *Acceptable Use Policy* that it doesn’t allow cryptocurrency-related payments so had Mrs M attempted to do this, the payments would’ve been blocked. But as the payments were made to individuals, Wise didn’t have any way to identify that they were related to the purchase of cryptocurrency, and I therefore wouldn’t have expected it to be able to identify the associated risk.

While I note that Wise didn’t intervene in four of the payments, I don’t think that makes a difference in this case. They were amongst the smallest of the payments, and I also don’t see any reason to believe that Mrs M would’ve reacted differently to any warnings when she sent those payments, so I think she’d still have sent them.

I’ve also considered the previous activity on Mrs M’s account as she says these payments were out of line with that.

I can see that Mrs M’s account had been open for around 16 months at the time these payments were made. Her account hadn’t been used much, but there are five transactions, and I can see that the values of those transactions range between £200 and £1,860. The transactions appear to have been made to a stock broking platform. With this in mind, I can’t say that the transactions that formed part of this scam were out of line with the limited activity Wise had seen previously on Mrs M’s account, in terms of values or type of payments, so I don’t think that Wise should’ve identified the scam based on this.

I do note that Mrs M has highlighted the fact that the two payments made on 20 November 2023 totalled over £5,000, and she therefore believes a different intervention should’ve taken place. Whilst I understand these payments are a cumulatively higher value than the others, this needs to be considered alongside any other risk factors – not the values in isolation. As the payments were made to individuals, and as warnings were shown to Mrs M and acknowledged, I’m satisfied that the interventions were proportionate, despite the higher total value.

Having considered everything, I think Wise’s interventions went far enough to provide Mrs M the opportunity to stop and consider the payments she was making, and the risks they presented, before she made them. I say this because in general the values of the payments were in line with the limited activity Wise had seen on Mrs M’s account before, and they weren’t identifiably being sent to high-risk recipients, such as cryptocurrency platforms. This, and the pattern of the payments, whereby the values fluctuated and they were sent over the time period of a month, means I don’t think Wise missed the opportunity to identify that Mrs M was being scammed, and to intervene more robustly than it did.

Recovery of the funds

Wise says that by the time Mrs M reported the scam to it, all of the funds had been withdrawn from the receiving accounts, so it wasn’t able to recover any of them. Given that the scam was reported several months after it happened, and the fact that funds obtained in

this way are generally withdrawn within hours of receipt, if not sooner, I don't think Wise could've done any more here.

I'm very sorry that Mrs M has fallen victim to this scam and I do understand that my decision will be disappointing. But for the reasons I've set out above, I don't hold Wise responsible for that.

My final decision

I don't uphold Mrs M's complaint against Wise Payments Limited.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs M to accept or reject my decision before 28 October 2024.

Sam Wade
Ombudsman