

The complaint

Mrs O complains that Wise Payments Limited didn't do enough to protect her from the financial harm caused by a job scam, or to help her recover the money once she'd reported the scam to it.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

Mrs O received a WhatsApp message from someone I'll refer to as "the scammer" who claimed to work for a recruitment agency. They told her about a part-time job working for a well-known company I'll refer to as "C". The role would require her to rate movies and 'like' social media pages for marketing purposes, and Mrs O could earn £15 to £20 per day.

The scammer also told her about a role for "F", which worked with digital influencers to promote brands. The role would require her to 'like' and follow social media pages and posts to help increase the exposure of the brands. She would also be required to complete tasks which she would have to pay for in advance using cryptocurrency. The scammer explained she would earn a commission on each task and that she could earn £80 per day.

Ms C had been looking for work and was satisfied the opportunities were genuine because she googled the recruitment company and C was very well-known. She was also added to a chat group with others claiming to be doing the same role. She wasn't given any employment documents, but the scammer did provide a written job description.

The scammer told Mrs O to open an account with Wise and showed her how to make a withdrawal on the platform. They instructed her to buy cryptocurrency from P2P sellers and between 28 July 2023 and 29 July 2023, she made eight faster payments to six different recipients totalling £16,784. She also made payments to the scam from a business account she held with Bank B.

Mrs O realised she'd been scammed when the tasks increased in value, and she was unable to make any more withdrawals. She complained to this service with the assistance of a representative who said Ms S didn't recall receiving any warnings when she made the payments and Wise should have intervened because she'd received large payments into the account and before making payments out to multiple new payees, which was unusual for the account and indicative of a scam.

They said that if it had asked her for the purpose of the payments and asked some basic questions, she hadn't been given a cover story, so she'd have explained that she was making payments in cryptocurrency for a job she expected to be paid commission for, that she'd been contacted via WhatsApp, and that she hadn't received any employment documents. With this information Wise would've identified the red flags and uncovered the scam.

Responding to the complaint, Wise said the recipients of the fraudulent transfers were other Wise customers and it had no reason to believe that the accounts would be used for fraudulent purposes. It said it showed warnings for six of the transfers and she chose 'investment' as the purpose of her transfers which meant the warnings it showed weren't relevant. It said that if she'd chosen 'paying to earn money by working online' it would have shown a more relevant scam warning.

It also explained that she chose 'investing' when asked to provide an account purpose, so the selected transfer purposes were in line with the account opening purpose. And as the account was newly created, there was no spending history to compare the payments with, so it couldn't have known her actions were out of character.

Finally, it said Mrs O paid random individuals instead of the company itself, which should have been a red flag. And she didn't carry out any research before accepting the job, trusting what the other group members told her without verifying the information.

Our investigator didn't think the complaint should be upheld. He didn't think the first six payments were unusual or suspicious because even though some of the payments were made on the same day, the values were low value and in line with expected account usage, and the beneficiaries wouldn't have appeared suspicious, so Wise didn't need to intervene. However, by the time Mrs O made payment 7, the cumulative total for the day was £7,124, and as Mrs O had declared the payments were for an investment, Wise should have presented a written warning which was tailored to cryptocurrency investment scams. But as this was a job scam, he didn't think this would have resonated with her, so he couldn't fairly ask it to refund her loss.

Finally, he explained there was no prospect of a successful recovery because Mrs C had sent funds to genuine P2P sellers, so they weren't fraudulent. And she wasn't entitled to any compensation.

Mrs O has asked for her complaint to be reviewed by an Ombudsman. Her representative has argued that Wise should have intervened when she made the fourth payment because this brought to total value of the payments over the £3,000 threshold, and she was making payments to new payees in quick succession from a newly opened account, with the values steadily increasing. They have argued that Wise ought to have been aware that cryptocurrency is acquired from P2P sellers, so there was a high risk that the transfers were made to buy cryptocurrency.

The representative said Wise should have questioned Mrs O about the payments and that a written warning would have been sufficient to stop the scam because there were numerous red flags present. And they don't accept the fact she chose an incorrect payment purpose means Wise didn't need to provide an effective warning because it had a duty to place her answers under a reasonable level of scrutiny, which it didn't do.

They've further suggested Mrs O wasn't lying because she was sending money to get returns, and it's possible she pressed the wrong button. They've argued that she shouldn't be punished for not providing the wrong payment purpose, this type of intervention shouldn't be regarded as sufficient when many high-risk factors were present and if she'd been asked probing questions the scam would have been exposed.

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 reached the same conclusion as our investigator. And for largely the same reasons. I'm sorry to hear that Mrs O has been the victim of a cruel scam. I know she feels strongly about this complaint, and this will come as a disappointment to him, so I'll explain why.

I'm satisfied Mrs O 'authorised' the payments for the purposes of the of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although she didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of her bank account, she is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mrs O didn't intend her money to go to scammers, she did authorise the disputed payments. Wise is expected to process payments and withdrawals that a customer authorises it to make, but where the customer has been the victim of a scam, it may sometimes be fair and reasonable for the bank to reimburse them even though they authorised the payment.

Prevention

Wise is an emoney/money remittance provider and isn't subject to all of the same rules, regulations and best practice that applied to banks and building societies. But it is subject to the FCA's Principles for Businesses and BCOBS 2 and owed a duty of care to protect its customers against the risk of fraud and scams so far as reasonably possible.

I've thought about whether Wise could have done more to prevent the scam from occurring altogether. Buying cryptocurrency is a legitimate activity and from the evidence I've seen, the payments were made to a genuine cryptocurrency sellers. However, Wise ought to fairly and reasonably be alert to fraud and scams and these payments were part of a wider scam, so I need to consider whether it ought to have intervened to warn Mrs O when she tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect Wise to intervene with a view to protecting Mrs O from financial harm due to fraud.

The payments did flag as suspicious on Wise's systems and so I've considered whether it intervened when it should have done and if the intervention was proportionate. Because she was buying cryptocurrency through P2P sellers, it wouldn't have been obvious that she was buying cryptocurrency and there was nothing else suspicious about the payees, and there was no spending history on the account to compare the payments with. So I wouldn't expect it to have intervened in the first six payments. Mrs O's representative has suggested it should have intervened when she made payment four because the cumulative total of the four payments exceeded £3,000, but in the absence of any concerning factors, we wouldn't expect it to have intervened because it wouldn't have been apparent that she was buying cryptocurrency, and the payments were consistent with the account opening reason.

I agree with our investigator that Wise should have intervened when Mrs O made payment seven because by this time, the cumulative total for the day was £7,124. In July 2023, a proportionate response would have been for Wise to have given Mrs O a 'better automated warning' which would involve asking her to provide a payment purpose followed by a tailored written warning relevant to the purpose she chose.

Wise has confirmed that it did this for six of the payments and that she was shown a written warning tailored to cryptocurrency investment scams because she said the payments were for 'an investment'. Because this was consistent with the account opening purpose, I'm satisfied that this was plausible and that the warning was relevant to the information it had. I'm also satisfied that Wise was prevented from identifying the scam because Mrs O gave an incorrect response.

Mrs O's representative has argued that Mrs O shouldn't be punished for having given an incorrect response, particularly as this could have been a mistake and I agree there are circumstances where that would be unfair. However, whether or not she intentionally misled Wise, I don't think it ought reasonably to have questioned the information Mrs O gave it in circumstances where the response was plausible.

Mrs O's representative has also argued that Wise should have asked questions about the payment which would have uncovered the scam, but I'm satisfied the intervention was proportionate to the risk presented by the payments and I don't accept that it needed to do anything else.

Overall, I'm satisfied Wise took the correct steps prior to the funds being released – as well as the steps it took after being notified of the potential fraud. I'm sorry to hear Mrs O has lost money and the effect this has had on her. But for the reasons I've explained, I don't think Wise is to blame for this and so I can't fairly tell it to do anything further to resolve this complaint.

Recovery

I don't think there was a realistic prospect of a successful recovery because Mrs O received the cryptocurrency she paid for.

Compensation

The main cause for the upset was the scammer who persuaded Mrs O to part with her funds. I haven't found any errors or delays to Wise's investigation, so I don't think she is entitled to any compensation.

My final decision

For the reasons I've outlined above, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms C to accept or reject my decision before 21 April 2025.

Carolyn Bonnell
Ombudsman