

The complaint

Ms S complains that Wise Payments Limited didn't do enough to protect her from the financial harm caused by an investment 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.

Ms S joined an online dating site where she met someone I'll refer to as "the scammer". They communicated via WhatsApp, email, calls, and video calls, but never met in person. The scammer said he was divorced, he had one son, and had moved to the UK after the divorce. They exchanged information about their background and seemed to have a lot of the same interests. He sent photographs of himself and his son and claimed to run a family business which was registered overseas.

Ms S believed the scammer was genuine and that they were developing a relationship. After five weeks, her asked her to send him some money because he was working overseas, and his bank account had been blocked. He then contacted her on his return to the UK stating he needed money to pay solicitor's fees.

Ms S sent funds to the scammer from Bank B until 26 May 2022 when she was warned by Bank B that she might be the victim of a scam. A few days later, she began to send funds from Bank S, and in December 2022 she stated sending funds from Wise. Variously, she sent funds via faster payment and debit card to cryptocurrency exchange companies and via money remittance services. Between 31 May 2022 to 15 December 2022, she made 187 payments from Bank S to eight different beneficiaries totalling £198,187.76. And, from 16 December 2022 and 22 May 2023, she made twelve faster payments from Wise totalling \$72,591.93.

Unfortunately, she realised she'd been scammed when she found a person on social media that had the same photographs that the scammer had sent to her. Ms S complained to this service with the assistance of a representative who said Wise should have intervened when she made the first payment of £7,675 because it was a large payment which exceeded the previous spending on the account. They said that if it had intervened, it would have identified that Ms S had met someone through an online dating site, and she'd been asked to make payments in cryptocurrency for solicitors fees, having never met him before. This would have been prevented.

Wise said there was no previous spending history on the account, and the payments happened infrequently over a long period of time, which isn't indicative of fraud. It explained it is an EMI, it's not unusual for its customers to make larger, infrequent payments, and there was currency conversion involved, which is the main selling point of its services. It said that when Ms S was asked to provide a payment purpose, she said she was paying friends and family. For three payments sent to an overseas account, she said "other" once, and twice she said it was for "goods and services".

Our investigator didn't think the complaint should be upheld. She thought Wise should have intervened when Ms S made the first payment due to the high value of the payment. And she thought there should have been a human intervention for the second payment because it was the second high value transaction to the same recipient in two consecutive days. But she didn't think this would have made a difference because Ms S had been making payments to the scam from multiple accounts with different providers for close to a year and by the time she started to use her Wise account, she was already under the spell of the scammer and determined to make the payments.

She explained that Bank B had carried out a security check in branch on 26 May 2022. While she was on a call with the Fraud Team, Ms S was warned that she was falling victim to a romance scam, and she agreed for the payment to be cancelled. But in subsequent messages she had with the scammer, Ms S told him what Bank B had said and he told her it wasn't a scam and she started to send payments from Starling and, later from Wise.

Our investigator also noted that Bank B had intervened in July 2022 and that during the calls, Ms S was dishonest about the circumstances of the payment, advising that she was investing in Bitcoin and that she'd been doing so since 2017. She also confirmed that no one had asked her to make the payments.

She commented that Wise asked Ms S asked to provide a payment purpose when she made payments two, three, ten, eleven and twelve, but each time she gave an inaccurate response which likely prevented Wise from providing a relevant warning.

Overall, she accepted Wise should have intervened sooner, but she didn't think this would have prevented Ms S from going ahead with the payments because she continued to make payments having received relevant warnings from Bank B and she misled Wise when it did intervene, so she thought it was unlikely that an earlier intervention or a better warning would've prevented her loss.

Finally, our investigator was satisfied that Wise did what it could to recover Ms S's money once it was aware of the fraud, but most of the funds had already been removed from the receiving accounts.

Ms S's representative has asked for the complaint to be reviewed by an Ombudsman. They've argued that the intervention from Bank M on 26 May 2025 uncovered the scam and Ms S chose not to go ahead with the payment, so there's no reason Wise couldn't have stopped the scam if it had intervened appropriately.

They've commented that Bank B didn't do enough during the call because it didn't confirm she'd fallen victim to a scam, so she continued to make payments to the scam.

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. I'm sorry to hear that Ms S has been the victim of a cruel scam. I know she feels strongly about this complaint, and this will come as a disappointment to her, so I'll explain why.

I'm satisfied Ms S '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, Ms S is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Ms S 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 was an emoney/money remittance provider and at the time these events took place it wasn't subject to all of the same rules, regulations and best practice that applied to banks and building societies. But it was 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. It 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 Ms S 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 Ms S from financial harm due to fraud.

Ms S was asked to provide a payment purpose for five of the payments and was shown warnings relevant to the purpose she selected before she proceeded with the payments. The first payment was for \$9,289.95 on 16 December 2022, and as this was a new payee and the amount was higher than previous spending on the account, I think Wise should have intervened and provided a written warning that broadly covered general scam risks.

I've thought about whether this would have made any difference to Ms S's decision to make the payment and based on her response to the warnings she received from Bank B and Bank S, I don't think a written warning would have made any difference, especially as we wouldn't expect a generic warning to contain enough detail to have resonated with her. I would expect Wise to have intervened again the following day when Ms S paid \$8,313 to the same payee. This is because the cumulative total for payments one and, two which were made over two consecutive days, was \$17,602 which was a significant amount and unusual when compared to the previous spending on the account. I think a proportionate intervention would have been for Wise to contact Ms S and ask her questions including why she was making the payments, whether there was a third party involved and, if so, how she met them, and whether she'd been coached to lie. But I don't think this would have made any difference because I don't think she'd have been honest in her responses and so I don't think Wise would have detected the scam.

On 26 May 2022 she was required by Bank B to attend a branch because of doubts about a payment she was attempting to make to a cryptocurrency exchange. During the call she had while she was at the branch, she explained she was sending funds to a gentleman overseas who she'd met four weeks prior because he needed to get into his UK bank accounts. She said he'd been working there for a week, and she planned to send a total of £16,000. The call handler told Ms S that she thought she was the victim of a romance scam and Ms S was happy for the payment to be cancelled, but she didn't believe she'd been scammed. In response to this the call handler arranged for the account to be blocked to prevent her from making any further scam payments.

Significantly, she started to make payments from Bank S after she was told by Bank B that she was the victim of a romance scam, and the messages she sent to the scammer when she left the bank show she didn't believe what she'd been told and still trusted him.

Bank S asked Ms S for a payment purpose before three of the payments she made from that account. On those occasions she said she was sending gifts to friends and family, she'd met them face to face, she hadn't been asked to send money unexpectedly, and she hadn't been asked to make the payment due to some form of problem or emergency. She was then warned: *'Fraudsters will tell you how to answer these questions to scam you. A genuine organisation will never do this. A bank or any other organisation will never tell you to move money to a new, 'safe' bank account. Fraudsters can make phone calls appear to come from a different number. Are you speaking with who you think you are'? I'm satisfied Ms S's responses to the questions she was asked prevented Bank S from identifying that she was the victim of a scam.*

I've also listened to the calls Ms S had with Bank B about a payment she was making to a cryptocurrency exchange on 15 July 2022 and its clear she misled the agent throughout. She was open about the fact she was buying cryptocurrency, but she said there was no third party or friend involved and that she wasn't being forced to make the payment. I'm satisfied that Bank B did ask probing questions – it asked which cryptocurrency she was buying, whether she been asked to download remote access software, whether she'd invested before, whether she was aware of the risks and whether she'd done any due diligence – and I don't think there was anything else it could have asked to either uncover the scam or to prompt Ms S to disclose any more information. It's clear from her messages with the scammer after the calls that Ms S was frustrated at having to spend time on the phone to the bank and she even suggested sending funds via a third party who could then forward the funds to a cryptocurrency merchant to avoid further calls with the bank.

She was also asked to provide a payment purpose when she made payments from Wise, but each time she gave an inaccurate response which likely prevented it from providing a relevant warning.

Based what happened during the various interventions, I don't think there was anything that Wise could have detected the scam. I accept that she did disclose the existence of the scammer in the May call with Bank B, but she later lied to Bank S and Wise about the purpose of the payments she was making from those accounts. And by the time I think Wise should have intervened, she'd been coached by the scammer not to tell the truth.

The fact she made payments from Bank S after being told by Bank B that she was being scammed shows she chose to believe what she was told by the scammer over what she'd been told by Bank B. And the fact she tried to think of alternative ways to send the funds when it became increasingly difficult in July 2022 shows she was determined to make the payments and, significantly, she maintained this attitude until May 2023.

So, while I think Wise should have contacted her when Ms S made the second payment, I don't think it could have uncovered the scam.

I've thought about whether there were any further opportunities to intervene, and I think it should have intervened again when Ms S sent \$9,442.49 to a new beneficiary. But as the amount was no longer unusual for the account and there weren't any other concerning factors, I would only expect it to have given a written warning that broadly covered the general scam risk and for the reasons I've already outlined, I don't think this could have made any difference.

Recovery

I'm satisfied that Wise did what it could to recover the funds but most of the funds had already been removed from the account.

Compensation

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

I'm sorry to hear Ms S 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.

My final decision

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 S to accept or reject my decision before 16 April 2025.

Carolyn Bonnell **Ombudsman**