DRN-5002218

The complaint

Mrs D complains that Wise Payments Limited (Wise) didn't do enough to protect her from the financial harm caused by an investment scam.

Mrs D has been represented by a claims management company throughout her complaint. I have referred to them as Mrs D's representatives.

What happened

Mrs D said she saw an advert on social media, about an investment opportunity. She made contact through Telegram and began a conversation with someone claiming to be a financial adviser. He told her about investment opportunities in shares.

Mrs D was unfortunately in discussions with a scammer, who was looking to persuade her to set up an account with Wise, transfer her money through it and then onto a cryptocurrency account, and then to their wallet.

Mrs D has, with her husband, complained about her bank, as she transferred money from an account held with it to the account she opened for the scam, with Wise. This complaint has already had issued a final decision from one of my colleagues. Because of this, I won't be deciding any aspect of that, as an ombudsman has already done so.

That said, I will be looking at what happened when Mrs D transferred her money from her Wise account to her cryptocurrency account, and this involved what happened from the beginning of each transfer. So, if anything happened when Mrs D transferred her funds from the bank to Wise, that impacts the merits of Mrs D's complaint here and my decision, I will consider this.

Mrs D through her representatives, made a complaint to Wise and said she had been scammed for £10,900 over 4 payments between 31 May 2023 and 6 June 2023. She made all 4 payments on a debit card to a cryptocurrency exchange and to an account in her name. All 4 payments were then converted to cryptocurrency and sent over to the scammer's wallet. Mrs D's representatives said Wise ought to have intervened from the first payment.

Wise said the payments were made from Mrs D to a cryptocurrency account in her name. It said there was little it could do to recover the funds, and also pointed to a number of terms in its customer agreement that it said were relevant. It said though that it acknowledged it should have done better with regards to the last payment Mrs D made for £3,880. It said it paid half of this payment, being £1,940, back to Mrs D on 16 May 2024, to compensate her for this.

Mrs D's representatives were not in agreement with Wise and so referred her complaint to our service. It said Wise should pay for all of Mrs D's losses plus interest and a payment for distress and inconvenience.

An investigator from our service said she didn't think Wise needed to take any further action. She was persuaded Wise ought to have intervened from the 3rd payment made to the

cryptocurrency provider, but didn't think it would have made a difference anyway. She concluded Mrs D wanted to just get past an earlier intervention with her bank, on the same day, and she was motivated to get the money to the scammer.

Mrs D's representatives didn't accept the investigator's findings. They said Mrs D accepted she misled her bank about the true purpose of the payments but feels if Wise had intervened, then its warnings would have included specific information about common cryptocurrency scams as the payments were going to an identifiable crypto exchange. It said these warnings would have rung true with Mrs D and she would have reconsidered sending the payments.

The parties are still not in agreement, so Mrs D's complaint has been referred to me for 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 first of all looked into the principles of the Contingent Reimbursement Model (CRM) to consider whether it applied here. That said, after doing this, I can see that the code does not cover payments such as the ones made by Mrs D, where she used her debit card. Or where payments are made to a cryptocurrency exchange account in her own name. I've therefore not considered this any further.

Moving on, I'm satisfied Mrs D authorised the relevant payments she made. Mrs D's representatives have explained that the scammer used software to make payments on her behalf. But I've not seen evidence of this, instead after reading an exchange between Mrs D and the scammer, I think she was authorising and making all of the payments herself. This led to her bank contacting Mrs D, intervening and obtaining further authorisation, after discussing the payment. I think, this shows me on balance that Mrs D was authorising the payments on that day, with her bank and then with Wise to her cryptocurrency account.

Under The Payment Services Regulation and the terms and conditions of the account, Mrs D is presumed liable for the loss in the first instance, in circumstances where she authorised the payments. However, this isn't the end of the story. Good industry practice was that Wise ought to have been on the look-out for transactions that were unusual or uncharacteristic to the extent that they might indicate a fraud risk. On spotting such a payment instruction, I would expect Wise to intervene in a manner proportionate to the risk identified.

Wise said it should have done more and identified that there was a risk, when Mrs D made her 4th payment. It said it should have intervened here and provided a warning. It said it has paid Mrs D compensation for this and sent her half of this payment, presumably because it decided it was equally liable with this payment with Mrs D, so decided to pay 50% of it back to her.

Mrs D through her representatives was not happy with this and so the parties are still in dispute. I have gone on to consider whether Wise should have done more here, than it has taken ownership for already.

Should Wise have recognised Mrs D was at risk of financial harm?

The Financial Conduct Authority and Action Fraud published warnings about cryptocurrency scams from 2018 and, by the time this scam occurred in 2023, it was widely understood that there were associated risks in relation to payments made to cryptocurrency exchanges. So, I

think, based on all that I said earlier were Wise's obligations, in addition, it ought to have been on the lookout for this scam occurring, and have an understanding as to what was at stake here.

This was a new account, opened at the suggestion of the scammers. They asked Mrs D to open this account and then transfer money into it from her bank and then on to her cryptocurrency account. I think Wise should have also had a heightened concern about this being a new account too, in addition to what I have already concluded about any payments made to a recognised cryptocurrency payee.

That said, the first payment for £1,000, I don't think I can fairly say reasonably ought to have been enough concern on Wise's part at this stage, yet, that it should have intervened.

However, Mrs D then made two more payments for £3,000 and £3,020 on the same day, to the same cryptocurrency platform. I think at this point Wise should have intervened, especially in light of what I have already said about what it ought to have known at that time about cryptocurrency payments and the fact this was a new account. Mrs D had made 2 payments in succession totalling £6,020. I think it ought to have asked more questions about what these payments were for and what Mrs D was looking to use the cryptocurrency for ultimately. I think if it had done this it would have then needed to provide a warning to Mrs D.

What kind of warning should Wise have provided?

I think by the third payment, for the reasons I have given, Wise ought to have provided at least, a better automated warning. It could have done this in its app, when Mrs D was entering a code, to authorise the payment.

Wise had the opportunity to intervene with a warning that specifically gave some of the key features of cryptocurrency-based investment scams, and informed Mrs D of issues such as how cryptocurrency scams work, whether significant gains were being suggested, whether she had been asked to transfer to another cryptocurrency wallet and how this was not a legitimate reason to make a payment.

If Wise had provided a warning of the type described, would this have prevented the loss Mrs D suffered?

On the direction of the scammers, Mrs D had to authorise several payments on 6 June 2023. First of all, she transferred money on 3 occasions from her bank to Wise, and then shortly afterwards on the same day, she made 3 payments on her debit card from her Wise account to her cryptocurrency exchange account. I have just concluded that on the second of these occasions, when she transferred £3,020 from her Wise account to her cryptocurrency account, that Wise ought to have made an intervention, and I have described the sort of warning it should have given at this point.

I have gone on to consider whether this would have prevented Mrs D from suffering a loss, and whether Wise's warning would have made her change her course of action. I have been able to get some understanding as to Mrs D's actions on that day and whether an intervention would have made a difference here because her bank, did intervene and call her. I think the call her bank made that day does give some indication as to what Mrs D would have said, if Wise had also, not long after on the same day, made an intervention as well.

Mrs D's bank called Mrs D to ask what the purpose of the transfer was, and she replied that she was transferring money from one of her accounts to another, which she opened herself, and the overall purpose was private. The representative from her bank stressed the

importance of being honest and how this could affect her ability to get her money back if it was a scam, and Mrs D confirmed that she'd not been told to lie about what the payment was for. It was clear from the bank's line of enquiries, that although it didn't warn her, the purpose of the call was to make sure she'd not fallen victim to a scam. Mrs D provided answers and reassurances that her payment was for her own private reasons, and she did not give any information about what the purpose of these payments was for.

I have thought carefully about what this meant for any intervention that Wise would have made shortly afterwards. On balance, I think even if Wise had made an intervention when Mrs D made her 3rd payment, I think she would have proceeded and made the payment anyway.

I do appreciate that Wise would have been more explicit with regards to tailoring its warning to a cryptocurrency investment scam, and some of those warnings could have rung true with what Mrs D had involved herself in at that stage. But I think it is clear from the exchanges that I have read between the scammer and Mrs D, that she was motivated to make the payment and would have done so regardless of the type of warning she received from Wise, on this occasion. She fed back to the scammer after she had spoken to her bank that she had been interrogated but the payment went through.

After Mrs D informed the scammer of her interaction with her bank, it offered to call her, but she replied that she was waiting for them [the bank] to call her, and she didn't want to do anything else that would send any red flags. I think the messages sent by Mrs D suggests to me that she was under the spell of the scammers, and would have done what she needed to, to make the payments she made on that day, go through, regardless of the type of warning I think Wise ought to have provided here.

Mrs D messaged the scammers at 1351 on 6 June 2023 about trying not to do anything that would send any red flags, and by 1454, around an hour later, all of the money had got into the hands of the scammers, as they had confirmed this during the same exchange. I think on reading this; I don't think Mrs D's stance would have changed much within this time.

A day later, Mrs D was discussing with the scammers a referral from one of her friends, and her husband potentially investing a much larger sum of money. It wasn't until later on that day, when she tried to withdraw £10,000, and this was not forthcoming that she realised she had most likely been the victim of a scam. She then reported what had happened to Wise and the authorities on 8 June 2023.

Was Wise able to recover the funds once it found out about the scam?

Finally, I've thought about whether Wise could have done more to recover the funds after Mrs D reported the fraud. This is something in certain circumstances it would have been able to look at once it had been notified about the scam from her.

Mrs D didn't make the payments to the scammer, instead she made them initially, to her own account on a cryptocurrency exchange. So, I wouldn't normally expect Wise to attempt to claim back funds in these circumstances where the money was transferred to Mrs D's own account with a business, who were carrying out a service for a legitimate purpose. That said, Wise informed Mrs D that it did try to recover the funds through chargeback, but it was unsuccessful in doing so. I don't think I can conclude it treated Mrs D unfairly here, based on what I have just concluded.

Finally, Wise said it made an offer to pay compensation to Mrs D in relation to the 4th and final payment made. It said it has paid half of this payment back to Mrs D's representatives.

Based on the conclusions I have made; I don't think I can say Wise has been unfair or unreasonable here and I won't be asking it to do anything further.

I'm sorry Mrs D was scammed and lost this money, but in conclusion I can't fairly tell Wise to reimburse her further, in circumstances where I'm not persuaded any intervention would have caused Mrs D to have not gone ahead with the payments. I also don't think it had an opportunity to recover her funds on this occasion.

My final decision

My final decision is that I do not uphold Mrs D's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs D to accept or reject my decision before 7 August 2025.

Mark Richardson
Ombudsman