DRN-5001036

The complaint

Ms A complains Wise Payments Limited didn't do enough to protect her when she fell victim to an investment scam and that it won't refund the money she lost as a result.

What happened

The background to this complaint is well-known to both parties and so I'll only refer to some key events here.

In February 2024, Ms A was tricked into sending money to what turned out to be a crypto investment scam. Ms A has explained she was introduced to the investment opportunity by a friend who had been investing for several months. Having expressed her interest in the investment, Ms A was contacted by an account manager who provided her with daily updates on market trends, advised on trades and shared purported earnings through screenshots of the trading dashboard. Ms A has said she was guided to purchase crypto using a legitimate crypto exchange platform's peer-to-peer marketplace - which appeared to Wise as if she was making payments to individuals. Having successfully purchased crypto, Ms A was instructed to transfer it to wallet addresses provided by the scammer.

In total Ms A made the following payments from her Wise account:

Transaction	Date and time	Payment type and payee	Amount
1	5 March 2024	Transfer to Payee 1	£50
2	14 March 2024	Transfer to payee 2	£400
3	16 March 2024	Transfer to Payee 3	£1,000
4	17 March 2024	Transfer to Payee 4	£2,000
5	17 March 2024	Transfer to Payee 5	£2,000
6	18 March 2024	Transfer to Payee 6	£51
		Total loss	**£5,501**

Ms A also purchased crypto via other accounts she held with another bank and e-money institution ('EMI').

Ms A said she realised she'd been scammed when she faced undue pressure to invest additional funds and was told she needed to invest further funds to "unlock" her profits.

Ms A notified Wise of the scam and asked for help recovering her losses. Wise was able to recover £2,400, in relation to two of the transactions, but explained it had been unable to recover any other funds. It refused to reimburse Ms A for the remainder of the loss as it had properly carried out her instructions. It also noted that it had intervened on two of Ms A's

payments but that she had said the payments related to “goods and services”, rather than “investments”, which prevented it from providing her with a more accurate scam warning.

Unhappy with Wise’s response, Ms A referred her complaint to the Financial Ombudsman. Our Investigator didn’t uphold the complaint. While she accepted that Ms A had been the victim of a scam, given what Wise knew about the payments at the time, our Investigator didn’t think it ought to have been unduly concerned about the risk of fraud. So, she did not expect it to intervene before processing the payments. But she noted that despite this, Wise had intervened on two of the payments, but that Ms A had selected an incorrect payment option, which prevented Wise from providing a more accurate scam warning which could have prevented Ms A’s loss.

Ms A disagreed and asked for an Ombudsman’s final decision. She said Wise’s decision to partly refund her loss demonstrated its recognition and acceptance that her payments had been made as part of scam, and that it was partially responsible. She also noted that while Wise had intervened on two of her payments, the warnings provided were not sufficiently impactful to prevent her further loss to the scam. She also suggested that her payments ought to be covered under the Contingent Reimbursement Model Code (the CRM Code). Ms A also explained why she considered the scammers actions were covered by the Fraud Act 2006.

The case has now been passed to me to decide.

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 should start by saying there is no doubt Ms A has been the victim of a sophisticated scam, which caused her to lose a significant amount of money. I don’t underestimate the impact the scam has had on her, or her financial security, particularly given her personal circumstances at this time. But I should explain, for the purposes of this decision, I am not considering the actions of the scammer, beyond establishing that Ms A has suffered a loss due to a scam. So, I will not be commenting on the application of the Fraud Act 2006.

Instead, I must consider Wise’s role in Ms A’s transactions, and whether there is any reason it should be fairly held responsible for her losses - either because it ought reasonably to have prevented her losses or because it was required to reimburse them. I know this won’t be the outcome Ms A is hoping for, but for similar reasons to our Investigator, I don’t think Wise is responsible for her losses. So, I don’t think it has acted unfairly by not refunding her remaining losses. I’ll explain why.

Should Wise be held liable for Ms A’s loss?

In line with the Payment Services Regulations 2017 (PSRs), the starting position is that Ms A is liable for payments she authorises – and Wise generally would be liable for unauthorised payments taken from her account.

Here, there isn’t any dispute Ms A authorised the payments. So, although Ms A didn’t intend the money to go to the scammers, and was clearly under their instruction when making the payments, under the PSRs she is presumed liable for her loss in the first instance.

Did Wise need to intervene before it processed the payments?

In broad terms, the starting position at law is that an EMI, such as Wise is expected to

process payments and withdrawals that a customer authorises it to make, in accordance with the PSRs and the terms and conditions of the customer's account.

But, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Wise ought to have been on the look-out for the possibility of fraud and made additional checks before processing payments in some circumstances.

But there is also a balance to be struck between identifying payments that could potentially be fraudulent and minimising disruption to legitimate payments.

I have reviewed Ms A's account and the payments she made to the scam. Having considered when they were made, their value and who they were made to, I'm not persuaded Wise ought to have found the first three payments suspicious, such that it ought to have made enquires of Ms A before processing them. They were all low value payments and there was nothing to indicate the payments were connected as they were made to different payees over several days.

Wise has demonstrated that it did intervene before processing Ms A's fourth and fifth payments. As part of the payment journey, it presented Ms A with an onscreen warning stating, *"Protect yourself from scams. This could be a scam. Tell us what this transfer's for, and we can give you advice."* Ms A then selected that the transfer was for *"Paying for goods or services"*; *"Making an investment"* was also an available option. Wise then presented Ms A with a number of other questions related to her selected payment purpose and presented her with scam warnings relevant to the answers she provided. Ms A was then presented with an option to cancel the transfer or continue to with the payment. Ms A chose to continue with the payment.

I appreciate Ms A has said she did not intentionally provide an inaccurate payment reason to Wise. She has explained that as her transfer was an intermediate step to purchase crypto via a peer-to-peer seller, which was later transferred on to an investment, she felt *"Paying for goods or services"* was the most appropriate answer. I have no reason to doubt what Ms A has said. But my focus here is not whether Ms A acted appropriately, but whether Wise's response to the perceived fraud risk was proportionate in the circumstances, and overall, I think it was.

Given the value of the payments and their destinations, I think it was proportionate in the circumstances for Wise to respond to the risk identified through its automated system, where it asked a series of questions about the transaction, to narrow down the potential scam risk, and then provided a warning tailored to that specific risk.

Unfortunately, this type of intervention will never be fail-safe, and the accuracy and/or relevance of the warnings is somewhat reliant on the options selected by the consumer. I think the payments options Wise presented to Ms A were clear and concise, and provided a reasonable articulation of the general types of transactions it would expect to see. While I can understand why Ms A did not think her payment related specifically to *"Making an investment",* I'm satisfied that this was nevertheless an option available to her. I'm also satisfied that by selecting this option she would have been provided with a more appropriate warning, which may or may not have prevented her further losses. But in any event, I consider Wise's intervention was proportionate in the circumstances. It is unfortunate that it did not successfully uncover the scam, but I cannot reasonably conclude that was due to any failing on Wise's part.

I note Ms A has also asked for us to consider whether Wise was required to reimburse her under the CRM code, which provides increased protection to consumers who are the victims

of Authorised Push Payment ('APP') scams. But the CRM Code is a voluntary code and Wise is not a signatory. But even if it were, the CRM Code would still not apply in these circumstances. While there is no doubt Ms A lost money to a scam, the evidence supports that the payments from her Wise account went to legitimate peer-to-peer crypto sellers. Having received Ms A's funds those sellers transferred Ms A the relevant crypto in return. Ms A later transferred that crypto away into the control of the scammers. So, the transaction that took place from Ms A's Wise account was not itself part of the scam and so would not be covered under the CRM Code.

I have also considered whether Wise could have done any more to recover Ms A's losses, but I don't think it could. Given the relationship between Ms A and the beneficiaries, as outlined above, it's surprising that Wise was able to recover some of the funds Ms A lost. But while Wise was able to recover some funds, I would not have expected it to do anything more than it did to attempt to recover her remaining funds.

Taking everything into account, while Wise recognised Ms A was potentially at risk of financial harm from fraud, it responded proportionately to that risk. Unfortunately, despite Wise's efforts to provide a relevant warning, it was unable to identify the payments were related to an investment. And despite the broader scam warnings provided, Ms A chose to go ahead with her payments. So, while I know this will be disappointing for Ms A, I don't find that Wise is responsible for her loss. It follows that I will not be asking it to take any further action.

My final decision

For the reasons given above, my final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms A to accept or reject my decision before 23 July 2025.

Lisa De Noronha
Ombudsman