DRN-5383449

The complaint

Miss M is unhappy that Wise Payments Limited won't reimburse money she lost to a scam.

What happened

On 20 February 2025 I issued a provisional decision on this complaint. I wanted to give both parties a chance to provide any further evidence and arguments before I issued my final decision. That provisional decision forms part of this final decision and is copied below.

"What happened

In 2022 Miss M came across an advert on social media for a company I'll call 'C', which was offering investments in cryptocurrency and appeared to be endorsed by a well known financial journalist. Miss M contacted C and spoke with a representative.

After agreeing to invest a small amount with C, Miss M was shown a trading platform which appeared to show her money increasing. An "account manager" from C then contacted her and told her that to make her investment she'd need to set up an account with Wise (which she did on 7 October 2022) and an account with a legitimate cryptocurrency provider I'll call 'B'. As she'd not invested before, she agreed that C could use remote access software that they installed on her device to assist her.

After seeing her money increasing on C's online trading platform, Miss M agreed to invest just under £10,000. She transferred money from her primary bank to Wise on 12 October 2022. On the same day, she says C's account manager then remotely took over her device and moved the money to B and on to the trading platform.

The payments were as follows:

Date & Time	*Amount*	*Payment type*
12 October 2022 at 15:20	*£5,000*	*Debit card payment to B*
12 October 2022 at 15:21	*£4,750*	*Debit card payment to B*

Also on 12 October 2022 Miss M agreed with C's recommendation that she make a further payment of just under £10,000. She topped up her Wise account with £9,900 and then C attempted an international transfer of that amount to a new payee but Wise blocked the transaction. Several further transfers to new payees were attempted in quick succession and each was cancelled by Wise. Wise then told Miss M that it had closed her account.

Through a representative, Miss M complained that Wise should have intervened when she attempted to make the first payment of £5,000. She said this was a new account, and the size of payments to a cryptocurrency account made in quick succession should have triggered Wise to give her a fraud warning.

Wise didn't agree. It said it had no reason to intervene in the 12 October 2022 debit card payments, which Miss M had authorised and confirmed by text message. The payments were made to a legitimate payment platform. It said following a review it had closed her account in line with its term and conditions. It said it had not been successful in recovering the money as B had not responded to its requests.

Unhappy with the outcome, Miss M asked us to look into her complaint. Our Investigator didn't uphold it. He wasn't persuaded that for the newly opened account the two transactions on 12 October 2022 were sufficiently unusual as to require Wise to intervene. He noted Wise had intervened in the third (and subsequent) attempted transfers.

Miss M didn't agree and asked for an Ombudsman's review. In summary, she said:

- *Wise should have erred on the side of caution given Miss M's account had been newly opened. The account activity of a relatively high value credit followed immediately by two debits on the same day was consistent with cryptocurrency scams. Wise had a responsibility to provide a warning about cryptocurrency scams, given it was aware this type of scam was increasing in frequency.*
- *Wise's intervention came too late. While she acknowledged Wise couldn't stop and prevent every payment on new accounts, she argued it should be at least partially responsible for the second payment – given the concerning pattern of activity at this point.*
- *Wise didn't offer her support but rather offloaded her account, in line with its poor level of customer care throughout her ordeal.*

What I've provisionally 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.

It's not in dispute here that Miss M fell victim to a cruel scam. She accepts that she authorised the debit card payments made to the cryptocurrency account. The starting point is that banks and Electronic Money Institutions ('EMIs') such as Wise ought to follow the instructions given by their customers in order for their legitimate payments to be made as instructed. So Miss M is presumed to be liable for the loss in the first instance, in circumstances where she authorised the payments.

But I've gone on to consider whether Wise should reasonably have taken any steps to intervene. As a matter of good industry practice, Wise should have taken proactive steps to identify and help prevent transactions – particularly unusual or uncharacteristic transactions – that could involve fraud or be the result of a scam. However, there are many payments made by customers each day and it's not realistic or reasonable to expect Wise to stop and check every payment instruction. There's a balance to be struck between identifying payments that could potentially be fraudulent, and minimising disruption to legitimate payments (allowing customers ready access to their funds).

Overall, 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 it fair and reasonable in October 2022 that Wise should:

have been monitoring accounts and any payments made or received to counter

- *various risks, including preventing fraud and scams;*
- *have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is*

particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;
- *in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – (as in practice banks and EMIs including Wise do).*

Bearing this and Miss M's own comments in mind, I need to decide whether Wise acted fairly and reasonably in its dealings with Miss M when it processed the two debit card payments to B on 12 October 2022.

Should Wise have recognised that Miss M was at risk of financial harm from fraud and, if so, should it have intervened?

The key question here is whether the payments were sufficiently unusual or suspicious for Miss M's newly opened Wise account such that intervention from Wise ought reasonably to have been warranted.

As I've said, there's a balance banks and EMIs need to strike between identifying payments that could potentially be fraudulent and allowing customers ready access to their funds. Not all crypto-related payments are made as a result of a fraud or a scam.

Miss M had opened her Wise account on 7 October 2022 and on that day had paid in four small amounts totalling £30. This meant that Wise did not have any meaningful account history to refer to when deciding whether the disputed payments were unusual or out of character for Miss M's account.

On 12 October 2022 Miss M transferred £9,750 to her Wise account and then made two card payments in quick succession – just one minute apart –for £5,000 and £4,750 respectively to B.

I've not seen any evidence to suggest that Wise knew Miss M's intended payment purpose. But Wise says that it did not give any warnings to Miss M when she made the payments, which were made by 3D secure and authorised by her by text messages.

There's no doubt the payments were made rapidly to a new payee. They followed a credit to the account and drained its balance. Wise didn't have any account history to refer to in order to determine whether the payments were unusual as compared with Miss M's normal spending pattern.

The first two payments were for just under £10,000 and were made in quick succession. I think the payments should really have been flagged by Wise as being unusual account activity. But given the lack of account history, the size of the payments that were made and that Wise is an EMI I think that any intervention at this point should have been limited to an online written warning that broadly covered scam risks.

Would an online written warning have prevented Miss M's losses?

I'm currently minded to conclude that an online written warning at the time of Miss M's debit card payments to B would not have prevented her losses. I'll explain why.

Miss M has told us that the scammer made the payments from Wise to B on her behalf using remote access software installed on her device. This has led me to conclude that Miss M would likely not have seen any warning that was provided. Given the fraud that was happening, I don't think the scammer would have heeded any warning either.

I appreciate Wise did then intervene when the scammer attempted to make the international transfer of £9,900 and stopped that transfer (and several later ones) from proceeding. I don't think this, of itself, means Wise should also have stopped the debit card transactions earlier that same day. The pattern of transactions had changed by the time the scammer tried to make the transfers, using the remote access software.

But I do consider the fact the scammer was able to attempt to make several international transfers, that were each being cancelled by Wise, meant it's likely Miss M didn't see any intervention by Wise in those transactions. I think this means that sadly Miss M wouldn't have seen – or acted on - an online written warning about scam risks even if Wise had issued one at the point of her debit card payments.

Overall then, I think that Wise should have intervened and given an online written warning. But for the reasons I've explained, I don't think this would have stopped the scam at the point of the debit card payments. As such, I currently don't think that Wise is responsible – in full or in part – for Miss M's losses.

Could Wise have done anything to recover Miss M's money?

I've considered whether the debit card payments could have been recovered by any other means. But given the payments were made to an account with B in Miss M's name, and the funds were quickly moved from that account to the scammer (as shown to Miss M in the false trading account) I don't think it's likely the funds could be recovered.

Was Wise entitled to close Miss M's account?

Miss M says Wise failed to offer her support and instead it "offloaded" her account.

But I don't think Wise acted unreasonably. It's not in dispute that Miss M's account had been subject to fraud, with the scammer having remote access to control her account. Wise's account terms and conditions (section 8.4) allow it to suspend and/or restrict Miss M's account in these circumstances.

I am sorry that Miss M fell victim to a cruel scam. I don't underestimate the impact on her, as she's described in her complaint. But for the reasons I've given, I don't think I can fairly hold Wise responsible for her losses. So I don't intend to uphold this complaint.

My provisional decision

For the reasons I've given, I don't intend to uphold this complaint."

Responses to my provisional decision

Wise didn't respond to my provisional decision.

Miss M responded through her representative to say she didn't agree with my provisional findings. In summary, she said she didn't believe Wise had adequately protected her and that its lack of protective measures had directly led to her losing her money. She believed Wise should have identified the warning signs of the scam and at the very least have temporarily stopped the activity. The scammers were relying on the ease and speed of transferring funds from Wise to themselves. In support of this, she said:

- The activity on her account warranted robust, human intervention from Wise because: the account was newly opened with no prior activity to draw from; the payments were going to a high risk recipient; her account had activity consistent with

cryptocurrency scams; there were high-value credits followed by immediate withdrawals.

- In 2022 losses to cryptocurrency fraud had reached record levels and by the end of 2022 many high street banks had placed restrictions or additional friction on cryptocurrency purchases owing to elevated risk. So when Miss M's payments took place, she thought Wise should have recognised that payments to cryptocurrency carried a higher risk of being associated with fraud.

- She referred me to two of my ombudsman colleagues' decisions. She said the first decision supported her view that Wise should have monitored her account and identified suspicious activity that appeared unusual or out of character. Without any transaction history Wise should have erred on the side of caution. She said the second decision supported her view that newly opened accounts present a greater risk of misuse compared to established accounts. By October 2022, Wise should have been aware its accounts were being used by scammers to extract money from their victims due to *"their lax approach to payment verification and account security"*.

- Wise should have had systems in place to detect the use of remote access technology that is standard across the industry. She referred to the FCA's published warnings regarding screen-sharing scams in the months before the scam: https://www.fca.org.uk/consumers/screen-sharing-scams
  Wise should have been aware of this and taken steps to protect its customers. Quoting from an ombudsman colleague's decision *"the broad legal position that a bank is expected to process payments that a customer authorises is not absolute."* Once Wise had detected remote access technology it should have temporarily stopped the account. This vital breathing room would have enabled Miss M to catch up with the scammers *"who were able to navigate Wise's system so quickly that she was unable to follow their actions".*

- The scammers were so quick and efficient whilst using Wise's system that she was unable to fully understand what was going on and act on any warnings provided. The lack of friction within Wise's payment journey meant she was unable to fully understand and consider the information given to her. Whilst recognising the fine line between normal account use and stopping fraud, she thought the payments were so suspicious that they warranted a more robust challenge.

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've carefully considered all Miss M's comments. But I'm not persuaded to change the findings I reached in my provisional decision for the reasons set out in that decision and below. I'll focus on what I consider are the central issues.

Miss M says that Wise should have recognised from the payment amount and pattern that she was at risk of financial harm. I've read the decisions to which she's referred in support of her position. I reach my decisions based on the individual facts and circumstances of each complaint. And in any event the decisions don't lead me to change my opinion in this case. I say this because I accept that the two payments made in quick succession for just under £10,000 should really have been flagged by Wise as being unusual account activity.

I've carefully considered Miss M's reasons for arguing that robust, human intervention would have been proportionate in all the circumstances.

Wise is an EMI and generally its accounts are used differently from traditional current accounts. I've taken into account the lack of account history and the combined amount of the two disputed payments. I accept the issue of a proportionate intervention is quite finely balanced in this case. But I don't think this changes the outcome because even a human intervention wouldn't necessarily have been over the phone.

I say this because at the time of the disputed payments (October 2022) I think it would have been reasonable for Wise to contact its customer to discuss the payments through a number of channels, including an online chat conversation. It would have been for Wise to decide how to do this and I can't say that it must have called its customer. And, if Wise had intervened by online chat conversation I don't think it's likely it would have made a difference. As Miss M accepts, the fraudsters had control of her computer using remote access software. Unfortunately, she says they were acting quickly and efficiently such that she was unable fully to understand what was going on or act on any warnings given. I think the fraudsters would have been able to mask or quickly navigate through any online intervention including a text-based conversation.

Miss M says that Wise should have detected that the fraudsters were using remote access software. I've read the FCA's warning (first published in May 2022) to consumers about screen sharing scams, which describes the risk of scams where the consumer is contacted out of the blue and asked to download software to share the screen.

But I don't think the FCA's warning to consumers in 2022 means that Wise had to have systems in place to detect the use of remote access software. I don't know of any rules or regulations that specify that Wise should have had remote access detection systems. So I can't fairly find it did anything wrong in not having this type of system in place.

Miss M says this type of remote access detection system was "standard across the industry" in October 2022. She's not provided any additional evidence about that. I'm aware of another EMI that had decided to include this system as a security measure to protect itself and its customers. But I don't think this, of itself, means that this type of software was good industry practice in 2022. It follows that I don't consider the fact Wise did not use this type of software in October 2022 means that it is responsible for Miss M's loss.

Despite my natural sympathy for Miss M, for the reasons I've explained in my provisional decision and above, I don't consider I can fairly require Wise to compensate her for the loss she suffered.

My final decision

For the reasons I've given, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss M to accept or reject my decision before 18 April 2025.

Amanda Maycock
Ombudsman