

## The complaint

Mr H complains that Metro Bank PLC failed to intervene when he fell victim to a romance scam.

Mr H is represented in this matter, but for ease of reading I will refer to Mr H throughout this decision.

## What happened

The background to this complaint is well known to both parties, so I won't repeat it in detail here.

In summary, Mr H fell victim to a romance scam. Mr H met the scammer on WeChat, Mr H has explained he wanted to learn more about Chinese music, language and culture. The conversation moved to WhatsApp and it appears from the chat transcripts that Mr H developed a romantic interest in the scammer.

The scammer introduced Mr H to a 'business opportunity' that required him to confirm orders through a fake website. To do so he had to make payments to an online account to pay for the items on the understanding he would be reimbursed with a further payment. Mr H was initially able to make small withdrawals from this account. However, when he wanted to make a larger withdrawal the scammers made a number of excuses as to why the withdrawal wasn't possible and asked for further payments before the withdrawal could be made.

The money Mr H transferred from his account with Metro had originated from an account with another provider. It was moved to Mr H's Metro account and then quickly transferred on to another account under Mr H's control, from there I understand Mr H bought cryptocurrency and transferred it on to the scammers. In total Mr H sent £28,979 between 17 and 25 September 2025 from his Metro account.

Mr H complained to Metro. He said it should have intervened before carrying out his instructions. Had it done so, he said it would have prevented him from losing his money to this scam.

Metro did not uphold Mr H's complaint. It said, it didn't think it needed to refund the money Mr H had lost to the scammers because the payments originated from an account under his control, and was transferred to an account he controlled so the transactions were considered 'me2me' (money from and to the same person), in other words, the money was in his control at the time of the transfers.

Our investigator didn't uphold the complaint as they did not consider an intervention by Metro would have been able to prevent Mr H's losses. Mr H did not accept the investigator's view. He said, in summary that the scammer had '*explicitly trained me what to say*' and he felt Metro should have robustly intervened. Had it done so Mr H said it may have uncovered the scam and prevented his losses.

As our investigator couldn't resolve the matter informally the case has been passed to me for a final 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.

Having done so I have reached the same view as our investigator, and for much the same reasons. I'll explain why.

I'm aware that I've summarised this complaint briefly, in less detail than has been provided, and in my own words. No discourtesy is intended by this. Instead, I've focused on what I think is the heart of the matter here. If there's something I've not mentioned, it isn't because I've ignored it. I'm satisfied I don't need to comment on every individual point or argument to be able to reach what I think is the right outcome. Our rules allow me to do this. This simply reflects the informal nature of our service as a free alternative to the courts.

I don't doubt Mr H has been the victim of a scam here – he has lost a large sum of money and has my sympathy for this. However, just because a scam has occurred, it does not mean he is automatically entitled to recompense by Metro. It would only be fair for me to tell Metro to reimburse Mr H for his loss (or a proportion of it) if: I thought Metro reasonably ought to have prevented all (or some of) the payments Mr H made, or Metro hindered the recovery of the payments Mr H made – whilst ultimately being satisfied that such an outcome was fair and reasonable for me to reach.

I have kept in mind that Mr H made the payments himself and the starting position is that Metro should follow its customer's instructions. So, under the Payment Services Regulations 2017 he is presumed liable for the loss in the first instance. I appreciate that Mr H did not intend for his money to ultimately go to a scammer – but he did authorise these payments to take place.

However, there are some situations when a bank should have had a closer look at the wider circumstances surrounding a transaction before allowing it to be made. Considering the relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time - Metro should fairly and reasonably:

- Have been monitoring accounts 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 payment service providers are generally more familiar with than the average customer.
- In some circumstances, take additional steps, or make additional checks, before processing a payment, or in some cases decline it altogether, to help protect customers from the possibility of financial harm from fraud.
- Have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so.

So, I've thought about whether the transactions should have highlighted to Metro that Mr H

might be at a heightened risk of financial harm due to fraud or a scam.

At the time Mr H made the transfers he had only recently opened his account with Metro, so it didn't have an account history to help it establish whether the payments Mr H was making were in-line with his usual account usage. But it did know the value of the payments was increasing significantly. The first payment Mr H made was for £100 on 17 September and the second payment on 21 September was for £5,000. This was followed by three payments on 24 September totalling £20,300 and two more payments the following day totalling £3,579.

I think there was sufficient information for Metro to be concerned that a pattern was forming, payments were made in quick succession— with three on the same day and the value was increasing significantly. Multiple transactions occurring this way can be an indication of a scam.

All the payments went to a known cryptocurrency platform (using a sort code related to crypto.com) — a common feature in investment and romance scams. And the money Mr H was moving from his Metro account had only been deposited in the account very shortly before it was moved on.

In view of this I think Metro should have intervened when Mr H tried to make the second payment on 21 September 2024 of £5,000. A proportionate and appropriate intervention would have been asking Mr H to answer a series of questions and then giving a tailored warning narrowed down to the most likely scam he was potentially falling victim to. Like our investigator I also think Metro should have spoken to him and questioned why he was moving his money so quickly after crediting to his account, before the payment of £12,500 was processed on 24 September 2024.

However, I am not persuaded such interventions would have prevented Mr H's losses from occurring. This scam was clearly a sophisticated one – with Mr H believing he was working for a legitimate company he had been introduced to by the person he had become close to.

In reaching this view I have taken into account that the information provided to this service shows that Mr H was coached by the scammer on what to say if his bank queried the payments and encouraged to give untruthful answers. In particular, I note that on 17 September 2024, Mr H asked the scammer which payment purpose he should select when moving the first payment of £100 to his Metro account. The scammer instructed Mr H to select either paying friends and family or buying cryptocurrency. Mr H then asked the scammer what he should say in response to a question about whether the account was under his control and whether the company was FCA registered. The scammer told Mr H to confirm the account was under his control.

On 23 September 2024 the bank Mr H was using to transfer money to his account with Metro queried a £3,500 payment he wanted to make. Mr H told the bank he had '*... not made any investments, I am trading BTC with my own funds in a Crypto account and I know exactly what I'm doing.*'

This wording had been provided to Mr H by the scammer.

The scammer also gave Mr H very clear instructions so that he could convince his bank he understood what he was doing. The scammer said;

*Anyway, no matter what they tell you, you just need to tell them that you know what you are doing, you are just trying to do some transactions in the Crypto account, because of the US dollar interest rate cuts and you think the cryptocurrency market is now profitable, tell them*

*very clearly you are not engaged in other investments. This way you can save a lot of trouble*

Mr H knew this explanation was completely untrue, but it appears he did not question why he was being instructed to lie to his bank or given such an elaborate cover story.

I am also mindful that the scammer also told Mr H not to show his bank screen shots of the exchange and told him to say he was sending money to family overseas in cryptocurrency. Mr H repeated back to the scammer what he had been instructed to say to check he had followed the scammers instructions correctly. As our investigator noted, Mr H followed the scammers instructions. In the chat he had with the scammer on 26 September 2024 Mr H said:

*Hi baby, I'm on the phone with my other bank. I'm telling them the things you told me to say.*

I am also mindful that on 21 September 2024, Metro blocked an incoming payment to Mr H's account and queried it with him. Mr H told Metro:

*You have blocked me from transferring funds from my [name of bank] account into my Metro Bank account. Please unblock it as I am transferring between my own accounts...I have not made any investments, I am trading BTC with my own funds in a Crypto account and I know exactly what I'm doing.*

He went on to say:

*I appreciate that you are trying to protect me and crack crime... but I need to know I can use Metro Bank as easily as my other banks.*

In view of this willingness to repeat what the scammers had told him to say when Mr H knew it to be untrue, I cannot reasonably find that even if Metro had intervened before Mr H made the payments from his Metro account it would have been able to uncover the scam Mr H had fallen victim to.

Mr H no doubt, considering the feelings he seems to have developed, was being manipulated in order to override his thoughts that payments he was making seemed dubious. It seems the scammers were suggesting that these payments were a standard procedure, with the scammer he met on WeChat endorsing this to be the case.

I do not think an intervention by Metro would have been successful at breaking the scammer's influence. Additionally, whilst I've not seen everything that Mr H saw, such as all the messages with the scammer he believed he had a romantic interest with, the apparent explanation for how the scheme worked is implausible and I think Mr H ought reasonably to have questioned whether the payments he was tasked with making could really be capable of leading to the result he wanted. The requirement to send funds to acquire funds should have been a red flag.

I also think Mr H ought reasonably to have recognised the scammers could essentially have continued saying more deposits would be required to get his refund – whilst continuing to leave the hope of him meeting the person he met on WeChat a possibility. This too highlights the level of influence the scammer clearly held over him. I do not say this to be critical of Mr H, I am simply highlighting that due to this I am not persuaded Metro could have broken such a level of influence with such an intervention. Therefore, I do not think Metro could have prevented his losses.

I don't intend any comments or findings I've made in this decision to downplay or diminish the impact this scam has had on Mr H. I have a great deal of sympathy for Mr H being the

victim of what was clearly a cruel scam that has had a significant impact on him. But I can only compel Metro to refund Mr H if it is responsible for the loss incurred. For the reasons explained, having carefully considered the circumstances of this complaint, I can see no basis on which I can fairly say that Metro should be held liable for the loss Mr H has sadly suffered.

### Recovery

I've also looked at whether Metro Bank took the steps I would have expected it to take once it was aware that the payments were the result of fraud.

I'm satisfied that had Metro Bank contacted the receiving bank as soon as it was aware of the fraud this wouldn't have made a difference in the circumstances. This is because, unfortunately, when Mr H reported the fraud, he had already sent the money from the receiving account to the scammers.

### **My final decision**

For the reasons I have set out 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 Mr H to accept or reject my decision before 17 December 2025.

Suzannah Stuart  
**Ombudsman**