

## **The complaint**

Miss C complains that Metro Bank PLC (“Metro”) failed to refund money that Miss C lost as part of a scam.

## **What happened**

Miss C came across a company that purported to be a trading group but was actually a scammer that I will call B.

The scam firm shared “trading signals” with Miss C and it encouraged her to invest more and more.

From her Metro account, Miss C made around 11 payments totalling over £26,000 to a crypto exchange. The funds were then exchanged into crypto and then sent on to B. These transactions took place between September and November 2024.

Miss C realised she had been scammed when she was pressured to invest more.

One of our investigators looked into this matter and they did not uphold this complaint.

Miss C did not agree with this and therefore her complaint was passed to me to issue 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.

In this decision, I’ll concentrate my comments on what I think is relevant. If I don’t comment on a specific point, it’s not because I’ve failed to consider it, but because I don’t think I need to comment in order to reach a fair and reasonable outcome. Our rules allow me to do this and this reflects the nature of our service as a free and informal alternative to the courts.

In broad terms, the starting position at law is banks are expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations 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 it fair and reasonable that Metro 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 Metro sometimes does including in relation to card payments);
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multistage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

I think that Metro should have intervened when Miss C made a payment of £6,000 on 6 November 2024. Prior to this, the payments were not large enough and did not form a pattern sufficiently indicative of a scam to have prompted an intervention from Metro. I think that a proportionate intervention at this point would have been to ask questions about the payments and provide a warning based on the answers provided. I can see that Metro did not intervene during this transaction. But importantly, this does not mean that Metro are liable for the payments made after this point. Metro would only be liable to refund these payments if a proportional and appropriate intervention would have likely stopped the scam.

It is clear that this was a professional and sophisticated scam, not least the detail provided by the scammer in relation to technical analysis of stock and crypto prices. It is also clear that Miss C was convinced, by the time that Metro needed to intervene, that what she was doing was legitimate. She had also built up a relationship with the scammer and she trusted them. Looking at the chats between Miss C and the scammer it is clear that she did not trust financial institutions and she was prepared to obfuscate what she was doing in order to ensure her payments were not stopped and to obtain credit. This is evidenced by her proactively splitting the payments she was making and sending to the crypto exchange via different means in small amounts. I also can see that she stated that she was going to say that she was purchasing a car in order to obtain a personal loan and I can see from her other account providers' notes that she stated that she was taking out a loan to pay off existing debts.

Given the lengths Miss C was going to, to avoid Metro's anti-fraud department from stopping any of the transactions, I think that even if Metro had asked questions about the transactions, Miss C would not have been forthcoming about what she was doing. This means that I think that Metro would have been unable to provide a warning that would have sufficiently resonated with Miss C to have overcome her belief that B was a legitimate trading firm.

So overall, I think that Metro should have intervened more than it did. But I do not think that this would have likely stopped or uncovered the scam.

I've also thought about whether Metro did enough to attempt to recover the money Miss C lost. In this instance the funds were being sent to an account in Miss C's own name. So neither reimbursements scheme applies to the payments in question.

I appreciate this will come as a disappointment to Miss C, and I'm sorry to hear she has been the victim of a scam. However, I'm not persuaded that Metro can fairly or reasonably be held liable for her loss in these circumstances.

**My final decision**

For the reasons given above, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss C to accept or reject my decision before 18 May 2026.

Charlie Newton  
**Ombudsman**