DRN-3794188

The complaint

Mr R is unhappy that Metro Bank PLC won't refund money he lost as a result of a scam.

What happened

In March 2020, Mr R's partner was looking online for investment opportunities. She came across an advert and left her contact details. Soon afterwards she was contacted by someone who claimed to represent a genuine investment company. Unfortunately, they were actually a fraudster.

Mr R's partner made an initial investment of £252.11 using another bank account. She could see this amount added to a 'trading account' provided by the fraudsters. Mr R's partner was given an account manager and kept in regular contact with her and Mr R via instant messages and phone calls.

Mr R's partner was told that if she kept investing, she could make £1,000,000 in a year. To add credibility to their claims, Mr R's partner was allowed to make a small withdrawal from her trading account.

Between August and September 2020, a series of payments were made from Mr R's account at another bank (that I'll call H) to the fraudsters (mostly via several legitimate third parties). I understand that Mr R's partner also sent money to the fraudsters from her own accounts.

From late September 2020, Mr R began to make payments to the fraudsters (via a different legitimate third party) from his Metro account. The first payment was for £20,000 and in total he sent over £115,000.

In late October 2020, H blocked a payment Mr R was trying to make. It had detected that remote access software was being used when the payment was attempted and it was concerned that Mr R was falling victim to a scam. I understand that Mr R was asked to attend a branch of H and spoke to its fraud team from there. He ultimately decided not to go ahead with the payment but is quoted as saying that he was sure that the fraudulent trading platform was not a scam. The notes made by H of that conversation also quote Mr R as saying:

"when you buy bitcoin it goes into your wallet and from there you send it onto another recipient and that's the person who is actually in control of the trading account- I've had the account for about a year and never had a problem with it"

And, when asked about the remote access, he is quoted as saying:

"that's a guy I know on a trading platform who was showing me something-yeah I have an awesome relationship with this person and he is very trustworthy"

Mr R also says that he hadn't been contacted by a third party and had opened the account himself.

After Mr R and his partner were told that they'd need to pay a very substantial sum of money into their trading account in order to withdraw their investment, they realised they'd been the victim of a scam and reported the matter to Metro. Mr R argued that the payments they made were very unusual and out of character and that Metro should have been alert to the possibility he was falling victim to a scam.

Metro said that the payments were not covered under the Lending Standards Board Contingent Reimbursement Model ("CRM Code"), which might have otherwise required it to refund him, and that he should take the matter up with the legitimate intermediary.

The matter was referred to our service but one of our investigators didn't uphold the complaint. They thought that Metro should have questioned the first payment before it left Mr R's account but, had it done so, Mr R would still have gone ahead with the payments.

Mr R, through his representatives, disagreed. He argued that he would have listened to the bank had it intervened and given him a clear warning.

In advance of my final decision, the notes provided by H were put to Mr R. His representatives said that he had generally been honest in his response – acknowledging the use of remote access software and that a third party was operating the trading account. They questioned how well the staff at H had explained the scam risk and thought that Metro should have also been able to identify that remote access software was being used by the fraudster.

As no agreement could be reached, the case was 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.

The starting point for my considerations, under the terms of his account and the relevant regulations, is that Mr R is responsible for payments he's authorised himself. But Metro is a signatory of the CRM Code and also has longstanding obligations to be on the lookout for unusual and out of character transactions to help protect against (among other things) the risk of financial harm from fraud.

The CRM Code does not apply to these payments as it requires a payment to be made to 'another person'. It is undisputed that these payments went to Mr R's own account at the legitimate third party in the first instance.

Like the investigator, I think that the first payment was unusual for Mr R. It was for a significant sum, to a new payee and was much larger than any of the (albeit limited) activity that had come before it. So, given the risk associated with the payment, I think Metro ought to have made enquiries with Mr R before it debited his account.

Metro didn't intervene then (or at any other point), so it's not possible for me to know whether such an intervention would have made a difference to Mr R's decision to continue with the payments. So, I've had to reach a decision on the balance of probabilities. Clearly the best evidence of what might have happened are the notes provided by H. It's unfortunate that H was not able to provide a call recording and it's apparent that some of the observations H made, were made in hindsight, after the scam had been reported to it. For example, although the name of the investment company is mentioned in the notes, it doesn't appear that Mr R disclosed (or was necessarily asked for) the name of the fraudulent

investment company at the time he made the payments (a warning about the fraudsters not being authorised existed on the Financial Conduct Authority website prior to Mr R making the payments in dispute).

We do know that H detected the use of remote access and, taking the quotes at face value, although Mr R denied having been contacted by a third party and was adamant that he was not falling victim to a scam, he does seem to describe a hallmark of this kind of scam: moving money first to a legitimate provider and then on to a trading account. He also acknowledges that someone on, or related to, a trading platform is the person who has had remote access to his computer.

So, I've thought carefully about both the position that Metro was in and the comments Mr R made to H to decide what I think might have happened had it intervened.

Metro's position was slightly different to that of H. Metro says if it had detected remote access being used, it would have blocked Mr R's account. The fact it didn't suggests that it didn't detect such activity (neither is it clear that Mr R has actually suggested that remote access was active when he made the payments from Metro). The notes provided by H suggest that its comments around remote access are, at least in part, what prompted Mr R to reveal the involvement of a third party. Given Mr R's confidence that he was not falling victim to a scam, I think, on balance, that he wouldn't have volunteered this information if he didn't have to explain why remote access was being used.

The payments from H also went straight to a cryptocurrency provider. The payments from Metro went to a foreign exchange firm. While the latter still carries risk, the former, in conjunction with the fact that the cryptocurrency was being moved to a broker bear all the hallmarks of a cryptocurrency scam. So, had Metro intervened, I don't think it would reasonably have been as concerned about the activity as H was, and ought to have been.

I've also thought about Mr R's reported comments about the broker – how highly he thought of this person. I know that Mr R has mentioned that he and his partner had contact over a messaging service with this person, but he hasn't produced any evidence of those conversations. That leaves me concerned that those conversations would only reinforce the impression I have of a strong bond between Mr R and the fraudster, one that Metro might have found it difficult to break down.

It's notable that Mr R voluntarily decided not to proceed with the payment that H blocked. H's notes show that he was asked to attend a branch, but when he arrived he'd already decided not to proceed. But it doesn't appear that the scrutiny of, and concern about, the payment was what deterred him – as he went on to make a payment of the same amount the following day from his account at Metro. And, while it's difficult to know exactly what was said during those interactions or how well the risk was explained, it seems likely that the possibility that Mr R was being scammed was raised (as it was necessary for Mr R to deny that was happening). The fact Mr R went on to make a payment of the same size from another bank, may suggest that he was trying to avoid any further scrutiny by H.

Like the investigator I'm also conscious that Mr R had already invested a significant sum of money and had been promised life changing returns. I have to take into account that he would be reluctant to give up such an opportunity. I further note that he had some experience of trading and much of what the fraudsters said resonated with him – he believed he understood the terminology and methods they employed. I think he would have appeared to bank staff as someone who was confident about what he was doing. Again, these factors make it difficult to see how an intervention by Metro would have made a difference.

Overall, the evidence from H suggests that Mr R was very confident about the investment he was making, he placed a significant amount of trust in the fraudulent broker and was confident that he was not falling victim to a scam. And, though Mr R did reveal concerning aspects of his investment to H, it was in a better position to identify the potential scam risk, given it had identified remote access and that the payments were being made to a cryptocurrency provider (both hallmarks of a cryptocurrency investment scam). Metro was not in such a position and I'm not persuaded that it would have been able to elicit the same level of detail from Mr R had it intervened and provided a warning to him. And, I don't think it would have been able to dissuade him from making the first payment (or any payment after that) and prevented his loss.

Finally, as the payments were sent to an account in Mr R's name, before being sent to the fraudsters overseas, it wouldn't have been possible for Metro to recover them.

I'm sorry that Mr R has lost money to such a cruel and cynical scam. I understand that this decision will be extremely disappointing for him, but I don't find that Metro are responsible for his loss.

My final decision

For the reasons I've explained, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr R to accept or reject my decision before 28 July 2023.

Rich Drury
Ombudsman