DRN-5746944

The complaint

Mr S complains that Metro Bank PLC hasn't refunded him payments made after he fell victim to an investment scam, and he says his account was hacked by the scammers.

What happened

Mr S found an advert on social media for a cryptocurrency investment opportunity. He invested with this company between May and June 2024, when he wasn't able to withdraw funds and realised he'd been scammed.

A short while later, Mr S received contact from another company who claimed to have located his original investment and explained they could help him recover it. They set out this would involve some costs and Mr S agreed to pay these. However, he later realised, in July 2024, that this was also a scam. Mr S says that in early July 2024, his accounts were also hacked by the same scammers, and they stole a large sum of his money.

Mr S complained to Metro about the scams as well as the reported unauthorised payments. Metro didn't look into his full complaint at first and only dealt with the unauthorised payments. It revisited his complaint and awarded him £100 for this, but didn't uphold any of his actual complaint points.

Mr S came to our Service, but our Investigator also didn't uphold his complaint. They concluded all the payments were authorised by Mr S and said that Metro wouldn't have been able to unravel the scams or stop Mr S going ahead. He disagreed and asked for an Ombudsman to reconsider his case.

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.

Initial investment scam and Recovery scam

It isn't in dispute that Mr S authorised the transactions in question. He is therefore presumed liable for the loss in the first instance. However, Metro is aware, taking longstanding regulatory expectations and requirements into account, and what I consider to be good industry practice at the time, that it should have been on the look-out for the possibility of fraud and made additional checks before processing payments in some circumstances.

I'm in agreement with our Investigator that none of the payments to the initial investment scam were so concerning I'd have expected Metro to intervene. They were fairly spaced out and weren't of high enough value or so out of character so that I'd expect Metro to have stopped them. When Mr S got involved in the recovery scam he started sending money to his own EMI account and, for the same reasons, I'm not persuaded the initial payments to this ought to have been concerning either.

However, on 25 June 2024, Mr S then sends six payments to his EMI account in one day.

This is a change in his spending pattern, both in terms of the amount leaving his account and the frequency of payments. So I would've expected Metro to have paused the £2,650 payment he was attempting – as this was the fifth payment attempted and took his total spend to over £7,000 that day – and asked him a series of questions about it. It ought to have used these answers to provide him with a better automated warning on the kind of scams connected with what it was Mr S shared he was doing. But I'm not persuaded that if it had done so, this would've prevented his loss. I'll explain why.

Mr S made payments to this scam from his EMI account. And after these scams, he made payments to a further recovery scam from another bank. Both these parties did intervene on payments he was making. The EMI displayed cryptocurrency scam warnings and brought him into in app chat and questioned him about what he was doing. And, while I accept at a later date, his other bank had him come to branch twice to question him. None of these interactions led to Mr S being fully honest about the actual situation he was in or any of the scams unfolding.

When he was questioned by his EMI about his payments, he looked to mislead it. For example, when the EMI questioned him and provided a relevant warning about cryptocurrency scams, he said he hadn't found the investment on social media, which he had. And he confirmed he'd checked the FCA register for the firm, which doesn't make sense as if he had, he'd have seen it wasn't on there. And he still went ahead. And at another time he set out how he was independently investing and not involved with a third-party – which also wasn't true. And after these scams, in August 2024 when Mr S was involved in another recovery scam for the same funds, he actively misled his bank and told them he was buying household goods. So even after becoming aware of these scams, as Mr S had reported them by then, he still wasn't forthcoming with his bank.

I can only ask Metro to reimburse Mr S if I find that any wrongdoing on its part caused his loss. Mr S has repeatedly said that Metro failed to intervene appropriately and that it should be liable for his losses, but I've not been provided with anything to persuade me that a better intervention would've resulted in a different chain of events here. It's clear Mr S was very under the spells of the scams at the times of the payments and adamant about making them. So I'm not persuaded that better questioning or warnings would've stopped him going ahead.

Payments on 6 July 2024

Mr S has explained that someone hacked his Metro account and made the disputed payments on 6 July 2024 to his EMI account. He's explained they then also hacked his EMI account and made payments to his own cryptocurrency wallet from there.

Metro doesn't hold any evidence which supports Mr S's testimony that his account was accessed by a third-party. And we're aware that the EMI has shown that only one device had access to this account – Mr S's genuine mobile phone. And that some of the disputed payments from here were completed using this device, as they required additional authentication. Mr S hasn't been able to explain how a third-party accessed his actual device to do this, he's told us he didn't share any security information with either of the scammers. And he's also confirmed that no one else had access to his cryptocurrency account and it was within his control at all times.

Mr S has now suggested maybe someone who was updating his computer made these payments, but that doesn't explain how they got access to his EMI account's card and his mobile phone, plus his EMI's security details to then move the money to his cryptocurrency wallet. Or give any insight into how they intended to access the money from here. It's also unclear why an unrelated third-party would process payments in the same way as Mr S had

been for the scams, rather than, for example, just paying an account they could access directly from Metro. So I'm not persuaded this is what happened either.

Considering the above, I'm not persuaded these payments were completed by a third-party without Mr S's consent. The technical evidence I've seen from the EMI indicates Mr S must've been involved in the payments and it's not clear how a third-party would've benefited from moving the funds from Metro to the EMI and then to Mr S's wallet, when he's said his cryptocurrency account was secure and the statements he's shared don't show a loss from there. We also know Mr S did make two further payments to the scam a few days after these, so it's not clear why he would've done this if he believed these same people had just hacked his banking and stolen a large amount of his money. So this again indicates it was Mr S making the payments as part of trying to recover his funds and I don't find these were unauthorised payments.

Recovery of funds

All the funds that left Mr S's Metro account went to other accounts in his own name and under his control. So I'm satisfied there was no reasonable way or need for Metro to act to recover these funds, when Mr S had received them elsewhere as intended and had the benefit of these.

My final decision

For the reasons set out above, I don't uphold Mr S's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 14 October 2025.

Amy Osborne
Ombudsman