

## The complaint

Mr F complains that Metro Bank Plc didn't do enough to protect him from the financial harm caused by an investment scam, or to help him recover the money once he'd reported the scam to it.

## What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

In May 2024, Mr F saw an advertisement on Google promoting an opportunity to invest in cryptocurrency using a company I'll refer to as "I". The advert featured a celebrity endorsement and claimed that "I" used expert brokers to train beginners on the trading process.

Mr F clicked on a link in the advert and was redirected to I's website which included an 'about us' section, FAQs, and a 24/7 live chat option and full details of the various company directors. He completed an online enquiry form and was contacted by someone I'll refer to as "the scammer" who seemed professional and articulate and who explained "I" would provide an online trading account and a broker who would instruct him on what to invest in.

The scammer told him to open an account on I's trading platform and to download AnyDesk, which would allow him to make trades on his behalf and to guide him through the process. He also told him to open accounts with a cryptocurrency exchange I'll refer to as "O", and Metro Bank.

The broker asked Mr F to first purchase cryptocurrency through a cryptocurrency exchange company and then load the cryptocurrency onto an online wallet. Between 7 May 2024 and 31 May 2024, he made twelve transfers to the cryptocurrency exchange totalling £64,500 from Metro Bank. He also made payments to the scam from "R" and Bank H.

The scammer encouraged Mr F to borrow money and during the scam period he used £8,000 from a credit card, a £10,000 loan in his own name, and a £25,000 loan in his mother's name to fund the investment. He also borrowed £7,000 from his mother. But when he tried to make a withdrawal, the scammer said he'd need to pay liquidity fees, and when he did so, he was chased for further funds.

Mr F complained to Metro Bank with the assistance of his representative who said it should have intervened because he was transferring funds to a cryptocurrency merchant from a newly opened account immediately after receiving high-value credits into the account. They said that Metro Bank's interventions were insufficient because it failed to ask probing questions and the warnings weren't effective.

But Metro Bank refused to refund any of the payments because Mr F transferred funds to his own account to purchase cryptocurrency and then transferred it to a third-party wallet, where he lost control of the funds.

Mr F wasn't satisfied and so he complained to this service with the assistance of his representative who argued that he made the payments believing the investment was genuine and if he'd been given an effective warning he wouldn't have gone through with the payments.

Responding to the complaint, Metro Bank said it contacted Mr F on 17 May 2024 regarding payments he'd made on 16 May 2024. It said Mr F asserted that he was investing on his own and so if it had intervened again or asked further questions, he would have given the same incorrect information.

Our investigator didn't think the complaint should be upheld. He thought Metro Bank should have recognised that the payments Mr F made on 31 May 2024 carried a heightened risk of financial harm from fraud because he made two payments of £10,000 in one day in quick succession. He thought it should have shown Mr F an investment scam warning, having already made sufficient enquiries on 17 May 2024 when he paid £2,300 payment to the same merchant. But, based on his conduct when he was questioned about the payments, he didn't think this would have made any difference.

Our investigator explained that on 17 May 2024, Mr F told Metro Bank that he wasn't being assisted by a third party, and on 6 June, he told Bank H he was transferring the funds because he was going on holiday. He also said no one had directed him to make the payment and he'd had the account R for months, when in fact he'd opened it the day before. He also explained that R intervened on 6 June 2024 and asked Mr F whether anyone had recently contacted him and encouraged him to purchase cryptocurrency, which he denied. It also asked where he planned to send the cryptocurrency once purchased, and he said 'nowhere'.

Our investigator further commented that Mr F had received payments into his Metro Bank account from third parties and transferred the funds to his own cryptocurrency account (At the request of the scammer), before transferring them to the scammer's wallet. He felt Mr F ought to have asked why the third parties couldn't have set up cryptocurrency accounts and done it themselves and he noted that Mr F had queried why the bank had told him the payments from third parties were fraudulent, but he didn't receive a response.

Our investigator felt this showed Mr F was ignoring obvious signs that something was not right and it was clear from the messages between Mr F and the scammer that he trusted her and was willing to follow her instructions, so he was unlikely to heed a written warning from Metro Bank on 31 May 2024.

Mr F has asked for his complaint to be reviewed by an Ombudsman. His representative has argued that Metro Bank should have asked Mr F why he was making the payments, how he found out about the investment, whether he'd had a second opinion, whether he had access to an online portal, and whether he'd downloaded AnyDesk, and had it done so it would have uncovered the scam. They've argued that Mr F told Metro Bank he was buying cryptocurrency and as this was a newly opened account, it should have asked more probing questions and provided effective scam warnings. It should also have enacted banking protocol due to the high value of the payments.

### **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've reached the same conclusion as our investigator. And for largely the same reasons. I'm sorry to hear that Mr F has been the victim of a cruel scam. I know he

feels strongly about this complaint, and this will come as a disappointment to him, so I'll explain why.

I'm satisfied Mr F 'authorised' the payments for the purposes of the of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although he didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of his bank account, he is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mr F didn't intend his money to go to scammers, he did authorise the disputed payments. Metro Bank is expected to process payments and withdrawals that a customer authorises it to make, but where the customer has been the victim of a scam, it may sometimes be fair and reasonable for the bank to reimburse them even though they authorised the payment.

### *Prevention*

I've thought about whether Metro Bank could have done more to prevent the scam from occurring altogether. Buying cryptocurrency is a legitimate activity and from the evidence I've seen, the payments were made to a genuine cryptocurrency exchange company. However, Metro Bank ought to fairly and reasonably be alert to fraud and scams and these payments were part of a wider scam, so I need to consider whether it did enough to warn Mr F when he tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect it to intervene with a view to protecting him from financial harm due to fraud.

Metro Bank intervened on 17 May 2024, when Mr F made the fourth payment. Arguably, it should have done so before the third payment because the cumulative value of the first two payments that day was £5,200, but I don't think an earlier intervention would have played out any differently.

I've considered what happened during the intervention, and I'm satisfied Mr F was asked relevant and probing questions and his answers prevented Metro Bank from detecting the scam. He wasn't given an effective warning but, based on the fact he trusted the scammer to the extent he was prepared to mislead his bank and borrow funds to fund the investment, I don't think a tailored warning would have made any difference.

I've considered whether there were any further opportunities to intervene, and I agree with our investigator that Metro Bank ought to have intervened again on 31 May 2024. I accept he made a payment for £12,500 on 17 May 2024, and this was higher than the previous payments, but Metro Bank had intervened earlier the same day in respect of payments to the same beneficiary and in those circumstances, I don't think it's unreasonable that it didn't intervene again.

Our investigator has suggested that Mr F should have been shown a written warning about cryptocurrency investment scams, and I agree the fact it had already asked probing questions in respect of the same beneficiary means it didn't need to do so again. And even if there had been further human intervention, I don't think it would have made any difference because he lied to Metro Bank on 17 May 2024 and he lied to Revolut and Bank H when they intervened on 6 June 2024, so it's likely he'd have done so again.

It's clear from the messages with the scammer and Mr F's conduct throughout the scam, that he was being coached (the scammer told him banks don't approve of cryptocurrency, and he believed that because he was an inexperienced investor) and that he trusted the scammer to the extent that he repeatedly lied to his banks. In addition, he followed the scammer's advice to borrow money to fund the investment, including from his mother, and he went ahead with

the investment despite concerns around payments he'd received into the account from third parties.

So, while I agree Metro Bank could have done more, I think Mr F would have continued to lie if he'd been asked more questions, and I don't think he'd have listened to a tailored warning about cryptocurrency investment scams. So, I don't think Metro Bank missed any opportunities to prevent Mr F's loss.

### *Recovery*

I don't think there was a realistic prospect of a successful recovery because Mr F paid an account in his own name and moved the funds onwards from there.

### *Compensation*

The main cause for the upset was the scammer who persuaded Mr F to part with his funds. I haven't found any errors or delays to Metro Bank's investigation, so I don't think he is entitled to any compensation.

I'm sorry to hear Mr F has lost money and the effect this has had on him. But for the reasons I've explained, I don't think Metro Bank is to blame for this and so I can't fairly tell it to do anything further to resolve this complaint.

### **My final decision**

For the reasons I've outlined 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 F to accept or reject my decision before 9 October 2025.

Carolyn Bonnell  
**Ombudsman**