

The complaint

Mr S complains that Monzo Bank Ltd (“Monzo”) won’t refund money he lost when his wife, Mrs S, fell victim to an employment scam.

Mr S is being represented by a claims management company in this complaint.

What happened

In March 2023, Mrs S fell victim to an employment scam. She was approached by a recruitment company “R” in connection with a job opportunity with a company “H” where she would be required to complete tasks – reviews for pre-determined products – in return for a commission as well as salary which would all be paid in cryptocurrency. It was explained to Mrs S that the cryptocurrency account needed to be topped up as required to complete some of the tasks.

Mr S’s representatives have recently confirmed that Mrs S doesn’t have a bank account in the UK. So, Mr S’s bank and cryptocurrency accounts were used with his permission. And it was him who made the payments on behalf of his wife.

Mr S initially made payments from his bank account with a different bank before switching to his Monzo account, from where he made seven payments totalling just over £27,000 over a period of two weeks. A small amount of return was received. Mr and Mrs S realised they’d been scammed when they were unable to withdraw Mrs S’s commission / salary as they’d expected to. They say they’ve since discovered that both R and H are clones of genuine companies.

Monzo refused to refund Mr S’s loss. Our investigator didn’t realise that Mrs S was involved in this scam; they understood that it was Mr S who had been approached by R. They partially upheld the complaint and asked Monzo to refund 50% of all but the first two payments. The investigator explained they didn’t think the earlier payments looked unusual and they thought a deduction for contributory negligence was warranted for the remaining payments that Monzo was liable for.

Mr S agreed with the investigator’s recommendations, but Monzo didn’t. In summary, while it acknowledged some of the transactions were larger than previous payments from Mr S’s account, it didn’t consider them significant in the wider scheme of transactions it sees on a regular basis.

The complaint was passed to me for a decision and, as I’ve alluded to above, I had some further questions when it became clear that Mrs S was involved in the scam. Mr S’s representatives confirmed that it was Mr S who made the disputed transactions whenever Mrs S needed to send money. I was satisfied that the circumstances of this case met the definition of an authorised push payment (APP) scam, given the account holder (Mr S) was involved in making the transactions for what he and his wife believed were legitimate purposes, and the funds were lost to the scammer from his account with a cryptocurrency exchange.

After finishing my review of the case file, I wrote to Mr S's representatives informally and explained that I didn't intend upholding this complaint. I said that while I agreed with the investigator that the third payment ought to have flagged as unusual to Monzo, I wasn't persuaded that questioning by Monzo would have positively impacted Mr S's decision-making. Mr S's representatives didn't agree, and so it's now appropriate for me to proceed to a formal 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've decided I'm not upholding this complaint. I know Mr S and his representatives will be disappointed with this outcome, not least because the matter has been ongoing for some time and the investigator previously upheld the complaint. I'll explain my reasons for my decision.

Under regulations and in accordance with general banking terms and conditions, banks should execute an authorised payment instruction without undue delay. The starting position is that liability for an authorised payment rests with the payer, even where they are duped into making that payment. There's no dispute that Mr S made the payments using his security credentials, and so they are authorised.

But in accordance with the law, regulations and good industry practice, a bank should be on the look-out for and protect its customers against the risk of fraud and scams so far as is reasonably possible. If it fails to act on information which ought reasonably to alert a prudent banker to potential fraud or financial crime, it might be liable for losses incurred by its customer as a result.

I've looked at the operation of Mr S's Monzo account which he'd opened more than six months prior to making the disputed transactions. I don't consider the first two disputed transactions, £1,000 and £1,325 respectively on 12 March, to be *that* unusual such that I think Monzo ought to have intervened. But by the time Mr S made the third transaction, £5,000 also on the same day and just over an hour after the earlier transactions, I think a pattern had emerged that ought to have given Monzo cause for concern. There had been a significant jump in the payment amount and third such payment to the same payee. I consider enough was going on here to warrant further enquiry. We know none of the transactions flagged on Monzo's systems.

Causation is a critical determinative factor in every scam case. It isn't enough to make a finding that a payment service provider failed to suitably intervene. To uphold a complaint, I would also need to be persuaded that such an intervention would more likely than not have a positive impact on the complainant's decision-making. I can't say for certain how Mr S would have responded to Monzo's enquiries. In such instances, I must make my decision based on a balance of probabilities. In other words, deciding what is most likely to have happened based on the information that I do have.

As I explained in my previous communication with Mr S's representative, I've reviewed the chat correspondence between Mr S and the scammer, as well as between Mrs S and the scammer. I've also paid close attention to Mr S's response to the investigator's questions around being coached and deciding to switch to Monzo. I'll discuss each in turn.

The chat correspondence shows instances of the scammer telling Mr S not to make any reference to cryptocurrency when he was in the process of making a peer-to-peer purchase (i.e., the transactions he made from his Monzo account). Specifically, on 11 March, the

scammer says, 'when paying dont [sic] write anything related to crypto', and Mr S replies 'Ok'. The scammer goes on to say, 'for this to be successful dont [sic] choose anything related to crypto.'

It's important to mention that this is against the background of Mr and Mrs S being frustrated with his other bank which kept blocking the transactions he'd attempted to send from his account with that bank. I can see that just the day before the chat I've referred to, in her chat with her 'mentor', Mrs S said her payment had been held by her (Mr S's) bank twice that day. She said, 'bank says transfers into crypto account are considered fraud transactions sometimes.'

The scammer went on to suggest moving to peer-to-peer purchase of cryptocurrency instead of sending money to crypto exchange directly. And not to make any reference to cryptocurrency if questioned by the bank. But, I haven't seen anything in the chat correspondence that suggests it was also the scammer who suggested that Mr S makes payments from a different bank account. It seems to me that the decision to use a different bank was Mr S's, amidst his frustration with his other bank.

This is further clarified in Mr S's response to this service where he says,

"We (me and my wife) had voice calls with X (one of the scammers) a couple of times because we wanted clarification and thought of getting help from the people having experience doing this job already. The scammer convinced us not to mention crypto, saying not all banks consider crypto currency as a regulated mode of exchange and that a few block crypto related transactions. The scammer also said that I can tell the bank that I want to go ahead with the transaction. I switched to Monzo and P2P trading in Binance to make the transactions faster.

I was literally following them as all other people in the group chat and all customer service people were looking convincing. I never could think of anything bad going to happen."

Mr S's representatives have said I'm insinuating that Mr S purposely stopped using his other bank account to evade detection of his activity. They've further said that Mr S's comments (quoted above) are not an admission of him trying to circumvent the fraud systems. And that all he was explaining was that he switched to Monzo and peer-to-peer because these were quicker and easier options.

I understand the point Mr S's representatives are trying to make in relation to his decision to switch to Monzo. But that still doesn't change the fact that he's told us he had been convinced by the scammer not to mention cryptocurrency if questioned by Monzo. The payments weren't identifiably going to a cryptocurrency provider, so Monzo wouldn't have been able to tell if Mr S's answers didn't quite fit in with the intended beneficiary – and the scam uncovered – like his representatives have suggested.

Based on what I've seen, I remain unconvinced that Mr S would have been honest about the true purpose of the transactions had Monzo questioned him when I think it should have. For that reason, I'm not persuaded that the scam would have been uncovered.

Despite my natural sympathy for the situation in which Mr S finds himself, for the reasons given, it wouldn't be fair of me to hold Monzo responsible for his loss.

My final decision

For the reasons given, 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 S to accept or reject my decision before 26 June 2024.

Gagandeep Singh
Ombudsman