DRN-3850832

The complaint

Mr B complained because Monzo Bank Limited refused to refund him for three transactions which he said he didn't authorise.

What happened

On 25 April 2022 there was a £1.500 credit to Mr B's Monzo account, from his bank account elsewhere. The same day, there was an outgoing £1,000 payment from Mr B's Monzo account to a cryptocurrency organisation.

On 2 May, there was a £1,000 credit to Mr B's Monzo account, from his bank account elsewhere. The same day, there was an outgoing £1,000 payment from Mr B's Monzo account to the same cryptocurrency organisation.

On 11 May, there was a £1,000 credit to Mr B's Monzo account, from his bank account elsewhere. The same day, there was an outgoing £1,000 payment from Mr B's Monzo account to a different cryptocurrency organisation.

On 18 June, Mr B filled up a dispute form for the three transactions, and contacted Monzo to say he hadn't authorised the three outgoing payments. He told Monzo no-one else had access to his phone, which was protected by a password or biometrics. All three had been approved using the Monzo app on Mr B's registered phone, and his PIN. Mr B initially said no-one else had access to his card, PIN, or phone. Monzo froze Mr B's account and blocked his card so no more transfers could be made.

Monzo asked Mr B for more information. It said it had separate processes for different scenarios. Both processes could recover the money, but the chances reduced if the wrong route was chosen. Monzo told Mr B that there was one process if he'd sent the money himself as a result of a scam, and a different process for when someone else had made the payment. So Monzo asked Mr B whether he'd sent the money himself as a result of a scam, or whether the money had been sent without his knowledge.

Mr B replied that the money had been sent without his knowledge. He then said he'd left his phone and wallet in a restaurant on 2 May around 10 am, and had got it back around 5 pm. Monzo asked whether there had been any other times when Mr B hadn't had his phone, and whether anyone else knew his PIN. Mr B said a few people knew his PIN, especially at work, but it had only been on 2 May that he hadn't had access to his phone.

Monzo told Mr B that it didn't agree that the transactions had been carried out by an unauthorised third party. It said the decision was based on the data available, and the timeline of transactions was suggesting it wasn't possible for anyone else to have authorised them. Monzo also reminded Mr B that the terms and conditions provided that it could close an account at any time, and it decided to close Mr B's account the next day, 21 June.

Mr B said that he'd been introduced by a friend to an investment guide. And a third party had accessed his device, using remote access software which was normally used for the maintenance of computers and other devices. He said he hadn't authorised the payments.

Mr B complained about Monzo's rejection of his fraud claim, and also because he'd asked Monzo to trace the recipient of the payments to the cryptocurrency organisations and reclaim the money, which Monzo said it couldn't do.

Monzo sent Mr B its final response to his complaint on 29 June. In this, it said:

- there was a scheme to reimburse customers who had transferred money after falling victim to a scam. This was called the Contingent Reimbursement Model (CRM) and applied to Authorised Push Payment (APP) scams. These cases were where a fraudster deceived a customer into sending a faster payment under false pretences. But Monzo said that this scheme – which Monzo didn't control - only applied to faster payments, but the payments from Mr B's account had been card payments. And in any case, Mr B had said he hadn't authorised the payments. So it couldn't use this scheme to refund Mr B.
- Monzo believed its investigation had been thorough, and had reached the right conclusion. It had reason to believe the transactions hadn't been fraudulent, so it didn't have to refund Mr B.

Mr B wasn't satisfied and contacted this service. He said he'd been investing with a company in April 2022, which had had access to his device, using the remote access software which was normally used for the maintenance of computers and other devices. He said the company also had his address and identification.

Our investigator didn't uphold Mr B's complaint. She said she'd considered what Mr B had said about the investment company which had had remote access to his device, but thought it was unlikely that a fraudster with full access would only have made three transactions over around two weeks. She also pointed out that Mr B had only been without his phone at the time of one of the disputed transactions, not all of them. And although Mr B had said he sometimes gave his phone passcode to others at work, he'd also said he always changed it after others had used his phone. So the investigator thought it was most likely that Mr B had authorised the disputed transactions himself.

Mr B didn't agree. He agreed that the transactions couldn't have happened when he'd left his phone at work, because no-one there knew his Monzo app passcode. He said he hadn't known that the company he was investing with had had access to all his data through apps which it had required him to download – including access to his email, where they could set up cryptocurrency accounts in his name, to which they'd transferred the money. He said that even recently, someone had tried to reopen one of the accounts under his name and Action Fraud had told him about it, and had told him to change his driving licence.

In a phone call with the investigator, Mr B also said that he'd been introduced to the investment company by a friend, so he'd expected the phone call, and had approved the company's access using the remote access software. Mr B also told the investigator that Action Fraud had told him there was now a warning on the anti-fraud database CIFAS, to show he'd potentially had his identity stolen. And Mr B clarified that the reason his work colleagues had his phone passcode was so they could buy things in the restaurant – but they didn't have Mr B's banking app passcodes, either for Monzo or for Mr B's bank from which money had been transferred immediately before the disputed transactions.

Mr B asked for an ombudsman's 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.

There are regulations which govern disputed transactions. The relevant regulations for disputed transactions taking place in 2022 are the Payment Services Regulations 2017. These say that the payment service provider (here, Monzo) must show the transaction was authenticated. That's the technical part, and here, Monzo has provided the technical evidence to show that all three disputed transactions were authenticated using Mr B's genuine card, and correct PIN, using 3D secure. So the disputed payments were authenticated.

The regulations also say that it's necessary to look at whether the card holder authorised the payments. In general terms, the bank is liable if the customer didn't authorise the payments, and the customer is liable if they did authorise them. The regulations also say that account holders can still be liable for unauthorised payments under certain circumstances – for example if they've failed to keep their details secure to such an extent that it can be termed ''*gross negligence.''*

So I've gone on to consider whether it's more likely than not that Mr B authorised the payments himself.

The payments were all carried out on Mr B's registered device, using the Monzo app on the phone. Mr B said his phone was protected with Face ID and passcode, and so was his Monzo app. So I've considered how any third party might have been able to carry out the payments.

Mr B initially told Monzo that no-one else had access to his phone, card, or PIN. He later said that he'd left his phone and wallet in a restaurant on 2 May, but it's hard to see how a third party could have accessed his phone and Monzo app when both were protected with Face ID and passcode. Mr B got the phone and wallet back when he went back at around 5pm, which isn't likely to have happened if those who found it were dishonest. Also, this wouldn't explain the other two transactions on 25 April and 11 May.

Mr B also said that work colleagues knew his phone PIN, but said he always changed the PIN after someone else had used it. And after the investigator's view, Mr B agreed that the transactions couldn't have happened when he'd left his phone at work, because no-one there knew his Monzo app passcode.

Mr B's theory is that the transactions were carried out as a result of a company he'd been investing with. He said he'd approved the company's access using the remote access software tool, which is normally used for the maintenance of computers and other devices. Mr B also told us that he provide the company with proof of his address, and a picture of his driving licence.

But there are problems with this theory. First, there is still the problem of obtaining Mr B's phone which was Face ID and passcode protected, and then accessing the Monzo app again with Face ID and passcode. I also don't think it's likely that the use of that remote access software could have enabled a third party to carry out fraudulent transactions on Mr B's account. And all three of the transactions were immediately preceded by transfers into Mr B's Monzo account from his bank account with another bank. This shows there was clear balance knowledge, and it's likely that it also indicates an intention to carry out the payments. I recognise that Mr B says he didn't make the bank transfers either – and this complaint isn't about his other bank, so I don't have the technical information for that non-Monzo account. But there are still too many factors meaning that I can't see how a third party fraudster could have carried out the transactions.

I also think that if a third party fraudster had: obtained Mr B's phone; been able to unlock it despite it being Face ID and passcode protected; and had been able to access his Monzo account despite being Face ID and passcode protected - they'd have taken more than three transactions between 25 April and 11 May. Most fraudsters maximise their gains in as short a time as possible, before anything can be discovered and stopped.

Mr B told Monzo categorically that he didn't authorise these payments. So that rules out the possibility of it having been a scam, using an Authorised Push Payment (APP).

Taking all these factors into account, I can't see how any third party fraudster could have authorised the transactions. So I think it's more likely than not that Mr B carried them out himself. This means that under the Payment Services Regulations, Monzo isn't required to refund him.

My final decision

My final decision is that do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 31 January 2023.

Belinda Knight
Ombudsman