

The complaint

Mr D complains that Monzo Bank Ltd (“Monzo”) closed his account and unfairly lodged a marker against him with a fraud prevention agency.

What happened

Mr D has explained that Monzo contacted him about some payments he didn’t recognise. He told Monzo that someone had “hacked” his email and was able to make payments from his account.

Monzo had earlier received a report from another bank about several payments that had been sent to Mr D’s account. The sender of the payments had reported they’d been defrauded and persuaded to send four payments totalling over £3,000 to Mr D’s account.

Those payments had then been sent to various other accounts (one in Mr D’s name), some to other financial merchants and some to an individual’s account. Monzo asked Mr D about the payments, their reporting describes the evidence Mr D sent them about the transactions to show they were legitimately received.

Monzo decided to close his account and lodged a marker with CIFAS – a fraud prevention agency, based on the evidence they’d received and Mr D’s responses to them. Mr D complained and Monzo looked into their investigation but didn’t change their original position.

Mr D then brought his complaint to the Financial Ombudsman Service for an independent review. An investigator looked into the situation and asked both parties for evidence about the issue. Mr D has since denied knowing about the payments, being responsible for the receipt of them or using the funds. He believes his account was taken over by someone who was responsible for using his account to receive and send the fraudulent funds, including communicating with Monzo.

Mr D confirmed he was the only one to use his phone (to access his account) and kept it with him. He left for a holiday and said he wasn’t aware of the issue until Monzo contacted him in November 2023, some three months after the payments were made into his account.

Monzo provided details of their investigation, including a copy of the fraud report and audit information concerning Mr D’s account, showing how those payments were utilised. Monzo said that only one device was “trusted” to use the account which was Mr D’s phone. There was some evidence that other devices had been used at various points to attempt to access the account, but as they didn’t complete Monzo’s procedures, they were unable to access it.

Monzo’s evidence showed that Mr D’s own phone/payment card was used to send those fraudulent payments out of the account after they’d been received.

After reviewing the evidence, the investigator concluded that Monzo had acted fairly when they closed Mr D’s account and lodged a CIFAS marker. It was noted that there was no evidence to suggest a third party had been involved and only one device had used the

account – Mr D's own phone to make transactions that he later disputed.

Mr D disagreed with the investigator's conclusions and said he himself had used his computer to access his account, which explained how someone else could have done so. Mr D stressed that he wasn't involved, and the marker was causing him difficulties opening other accounts which were affecting his education.

As no agreement could be reached, the complaint has now been passed to me for a decision.

As part of my own investigation I asked both Monzo and Mr D for more information.

Monzo provided further audit details of the use of the account showing:

- Payment details of Mr D's phone and registered card and Apple Pay being used to send the fraudulent funds out of the account (27 July 2023).
- Further payment data showing other payments to these accounts had been made prior to the receipt of the fraudulent payments.
- Authentication data for outgoing payments connected to the incoming fraudulent funds.

Mr D confirmed that his phone was kept with him whilst he was travelling. Mr D sent in two photographs of his passport.

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.

Monzo closed Mr D's account and lodged a Cifas marker after they received fraud notifications from another bank and carried out an investigation. Mr D's case is that he wasn't responsible for (the incoming fraudulent payments or the outgoing payments which utilised them) because his account had been compromised.

So, in order to determine if Monzo acted fairly, I first need to consider the issue of the disputed payments. Mr D has denied knowing anything about them and has stated that it was a "hacker" who carried them out and also communicated with Monzo when they asked him about the payments. Specifically, these relate to the funds sent from Mr D's account that resulted from the incoming fraudulent payments.

The relevant law surrounding authorisations are the Payment Service Regulations 2017. The basic position is that Monzo can hold Mr D liable for the disputed payments if the evidence suggests that it's more likely than not that he made them or authorised them, but Monzo cannot say that the use of the card/apple pay, or internet banking conclusively proves that the payments were authorised.

Unless Monzo can show that consent has been given, it has no authority to make the payment or to debit Mr D's account and any such transaction must be regarded as unauthorised. To start with, I've seen the bank's technical evidence for the disputed transactions (principally the outbound payments utilising the fraudulent funds). It shows that the transactions were authenticated using the payment tools issued to Mr D.

The relevance here is that if the evidence pointed toward a third party being involved who had "taken over" Mr D's account, it would be much harder for Monzo to make a case that Mr

D was somehow involved in receiving and moving funds that have been reported as fraudulent.

Monzo's evidence shows that those transactions Mr D has disputed were carried out using the payment tools issued to him, either his card, apple pay set up on his phone or using his phone to send payment to another account via a bank transfer (faster payment). Mr D has said it's possible that the "hacker" was able to use the internet to make the payments, and whilst that's technically possible, they would still need to have obtained Mr D's passcodes (that only he knew) and then somehow convince Monzo's systems that they were using Mr D's phone. I don't think it's plausible that these transactions were carried out by someone else, rather that they support Monzo's position that it was Mr D himself who carried out the payments.

Once the fraudulent payment(s) were received into Mr D's account, they were quickly sent out again (which is a typical pattern for such activity) to other accounts, most of which were set up prior to the receipt of the first fraudulent payment. So, this indicates those accounts were already operating and unlikely to have been set up by an unknown "hacker".

I've noted Mr D's comments that he'd travelled home (to another country), which I've taken to mean he wasn't aware of those transactions when they took place. But I'm afraid the evidence doesn't support that. Mr D's passport details don't show Mr D was back at home at the time of the disputed transactions and his statements show he was travelling home (based on payments at an airport in the UK)– but this was after the last payment was received into his account and then sent to another person's account. The final outgoing payments were made the day prior to the expiry of Mr D's visa which supports the case that he was still able to make these payments and wasn't overseas or unaware of what was happening.

So, I'm satisfied it was more likely than not that Mr D was responsible for the outgoing disputed transactions which utilised the fraudulently received funds.

Cifas marker

In order to lodge a Cifas marker, Monzo are required to satisfy a number of different "pillars". The standard of proof is set at a high bar because a marker can have a detrimental impact on a person's ability to obtain financial services.

The two main "pillars" that are particularly relevant here say that Monzo must have evidence to show:

- That there are reasonable grounds to believe that a Fraud or Financial Crime has been committed or attempted;
- That the evidence must be clear, relevant and rigorous

So, Monzo's evidence can't merely indicate there was a suspicion, Monzo must be satisfied it could confidently report the crime to the police if necessary.

Monzo are also required to ask Mr D about the funds and obtain a response (if given). Here they approached Mr D after they received the report and Mr D responded with a version of events that Monzo believed was supportive of his involvement in the fraud. Mr D has since denied it was him; but given that the information from the other bank didn't reach Monzo for some months after the disputed transactions took place, I don't think it's plausible that the "hacker" was still monitoring his account to the extent that they'd answer Monzo's questions. They'd already had the money, so why would they be interested in what the bank thought?

Far more likely that the responses were made genuinely by Mr D. I'm afraid that the change in story to put the responsibility on an unnamed "hacker" isn't plausible given the evidence provided by Monzo. They've shown Mr D's phone and payment card were used to administer the payments, including sending some to his own account shortly after receiving the funds. There's nothing I've seen that indicates it was anyone else but Mr D who moved the funds, although I don't doubt that others were involved. As the evidence indicates it was Mr D who utilised those funds, I can only reasonably conclude that he had some knowledge of them.

I think Monzo's decision to close the account and lodge a fraud marker with Cifas was both fair and reasonable, so I won't be asking them to do anything.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr D to accept or reject my decision before 27 January 2025.

David Perry
Ombudsman