DRN-3323365

The complaint

Mr P is unhappy that Monzo Bank Ltd won't refund the money he's lost to a fraudster.

What's happened?

In May 2021, Mr P noticed some suspicious activity on his Monzo account. He was reporting it to Monzo using its online chat function when he received a telephone call from a fraudster pretending to work for Monzo. Mr P has told us that the fraudster used the following tactics to convince him that the call was genuine:

- They called from a spoofed telephone number, which was very similar to the number on the back of his Monzo debit card (only the last two digits were switched, and he didn't notice this until he had been speaking to the fraudster for a while).
- They sent text messages to his mobile phone from a spoofed telephone number, which was identical to the number on the back of his Monzo debit card.
- They took him through security checks – they knew his residential address including the full post code and his email address.
- They told him that a fraudulent transaction had been attempted on his account which directly related to the suspicious activity he was in the middle of reporting to Monzo.

The fraudster told Mr P that an unrecognised device was logged into his Monzo application ('the app') and they'd need to block his account to prevent any further fraudulent transactions being attempted. They asked him to move all the money he held in Monzo accounts into his Monzo current account and said they would then close the compromised account and transfer Mr P's money to a new, secure account. As a precaution, Mr P sent the money in his Monzo accounts to an account he held with another bank. But the fraudster said this might compromise his account with the other bank and asked him to put the money back in his Monzo current account. He even received a call from a spoofed number which matched the number on the back of the debit card the other bank had issued him with, confirming that his account with that institution had been compromised.

Once Mr P had moved his money back into his Monzo current account, he was told to log-out of the app, delete and reinstall it, then sign-in again as normal. In the meantime, the fraudster said he would receive a text message with a security name, which he did. Mr P says he didn't give the fraudster any personal information and he wasn't asked for any. He didn't download any other software either. When he signed back into the app, he saw that his account was still blocked, and showed a nil balance. He became suspicious at this point, especially when the fraudster told him he would now need to apply for a £3,000 overdraft to secure his account. He also noticed that the number the fraudster was calling from wasn't identical to the number on the back of his Monzo debit card. He told the fraudster he was in an online chat with Monzo and he was going to speak to them about the situation. The conversation ended abruptly but £4,887.50 had already been transferred out of his account by then.

Mr P says his funds were taken out of his account without his knowledge - he didn't send any payments or authorise anything. The only time he entered his credentials is when he deleted and reinstalled the app.

What did Monzo say?

Monzo has said that:

- No funds remained in the beneficiary account for it to recover.
- Its records show that Mr P authorised the transfer of funds out of his account – he approved the payment using his PIN. But, as Mr P says he didn't authorise the payment, it can't treat it as fraudulent or reimburse him under the Lending Standards Board's Contingent Reimbursement Model ('CRM Code') – which only covers Authorised Push Payments ('APP').

What did our investigator say?

Our investigator was satisfied that the payment out of Mr P's account was 'authorised', and he said that Monzo should have fully reimbursed Mr P under the CRM Code. But Monzo didn't agree. It maintained that, as Mr P had reported the transaction as unauthorised, it isn't covered by the CRM Code.

The complaint has now been passed to me to decide.

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.

The CRM Code requires firms who have signed up to the Code to reimburse customers who have been the victims of APP scams in all but a limited number of circumstances. Although Monzo isn't yet a signatory of the CRM Code, it's allowed us to apply the Code's principles to complaints about it which meet the relevant criteria.

I appreciate that Mr P has said he didn't send any payments or authorise anything. The fraud was sophisticated, and perhaps he didn't realise he was authorising a payment out of his account from the actions he was taking. But, from the evidence I've seen, and from what Monzo has told us, I'm satisfied that he did and that he has been the victim of an APP scam, which is covered by the CRM Code. And I haven't seen any evidence which persuades me that any of the permitted exceptions to reimbursement apply in the circumstances of this case.

I say this because Monzo hasn't argued that Mr P ignored an effective warning it gave during the payment journey, nor has it pointed to any warning it gave which it believes was effective and ignored. And I'm satisfied that Mr P had a reasonable basis for belief in this case for the following reasons:

- Mr P had noticed genuine suspicious activity on his account and was in the process of reporting this to Monzo when he received the call from the fraudster. The fraudster told him that a transaction had been attempted on his account which directly related to the suspicious activity he was in the middle of reporting. I think this added authenticity to the fraudster's story.
- The telephone number the fraudster called Mr P from was very similar to the number on the back of his Monzo debit card – only the last two digits were switched. Mr P says he checked this and didn't notice the slight difference initially. I think is understandable in the heat of the moment and given how similar the number was. In addition, the text messages Mr P received from the fraudster came from the same telephone number as the one on the back of Mr P's Monzo debit card.
- The fraudster took Mr P through security checks, asking him questions which

demonstrated that they knew both his residential address and email address.
- During the scam, Mr P received a call from another spoofed telephone number which was the same as the one on the back of his debit card issued by another bank. I think this would've added another layer of persuasiveness to the scam.

Overall, it appears that Mr P fell victim to a sophisticated scam, and I can see why his suspicions weren't aroused at first. I don't think it was unreasonable for him to have believed that he was speaking to Monzo in the circumstances.

From everything I've seen, I'm satisfied that Monzo should have reimbursed the money Mr P lost to this scam under the CRM Code. I can't be certain what Mr P would have used the money he lost for if he had not been defrauded, so I think it's fairest to award interest at a rate of 8% simple per year from the date Mr P should have received a refund under the CRM Code to the date of settlement.

My final decision

For the reasons I've explained, my final decision is that I uphold this complaint and instruct Monzo Bank Ltd to:

- reimburse Mr P's loss within 28 days of receiving notification of his acceptance of my final decision; plus
- pay 8% simple interest per year from the date Mr P should have received a full refund under the CRM Code to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr P to accept or reject my decision before 27 April 2022.

Kyley Hanson
Ombudsman