DRN-4720964

The complaint

Mr W has complained that Metro Bank PLC registered a marker against him at CIFAS, the national fraud database.

What happened

In 2020, an account was opened with Metro in Mr W's name. It was used to send some small payments between other accounts of Mr W's. Then it received around £9,600 from a victim of fraud. This money was quickly forwarded to a cryptocurrency account, also in Mr W's name. Metro called and wrote to Mr W, asking him to send evidence of his entitlement to the money to their fraud team. But Mr W didn't do so.

Metro closed the account and registered a marker against Mr W at CIFAS.

In 2023, Mr W complained. He said a close friend had stolen his details, then they opened and used the account without Mr W's knowledge or consent. He said once he found out about the account, he closed it himself.

When Mr W came to our service, he instead said that he'd opened the Metro account himself for his savings. Someone – he had no idea who – had somehow gained access to his account and used it without his knowledge. He said that as he was unaware of what had happened on his account, he didn't clock on to the fraud issues. He said that unrelated accounts of his were defrauded some years later, which he felt was evidence in his favour.

Our investigator looked into things independently and didn't uphold the complaint. Mr W asked for an ombudsman's final decision, so the complaint's 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.

In order to register this marker, Metro were not required to prove beyond all reasonable doubt that Mr W had done something wrong. They did need to have reasonable grounds to believe that he'd misused his account, which went beyond a suspicion or concern, and which had appropriate supporting evidence. Having carefully considered everything that both sides have said and provided, I think Metro did have sufficient grounds to register this marker. I'll explain why.

First, I will address Mr W's first version of events: that a close friend stole his identity and opened the account without his knowledge or consent.

The account was opened at the address Mr W confirmed was his at the time, using the same contact details he gave our service. It is not likely or plausible that a fraudster would open the account using Mr W's contact details. That would mean that all correspondence would go to Mr W and he would find out he was being defrauded straight away and be able to close the account before it was even used. Indeed, I can see that Metro sent Mr W emails, letters, and text messages about opening the account and its activity, including a link he had to click to confirm he wanted to open it. So Mr W was aware of the account, and he didn't tell Metro anything was wrong at the time.

The card was sent to Mr W's address – the address he's confirmed as being his. And Metro received a call from his registered number – the same number he gave us – from someone who was able to pass security and be identified as Mr W. They confirmed they'd received the card in the post, and they activated the card over the phone. I find it's most likely that that was Mr W. If the account had been opened fraudulently without his knowledge or consent, it is neither likely nor plausible that he would activate the card instead of telling Metro that this wasn't his account. Similarly, it appears that Mr W also called Metro to do some account admin, and again later to discuss the fraudulent activity. As far as I can see, he never mentioned that the account was not his at the time.

So the evidence strongly points to this being Mr W's account. It is not likely or plausible that it was set up without his knowledge or consent.

Mr W said his identity was stolen in 2022 to take out a loan. But the letter he sent us is chasing him for payment, it does not confirm that he was defrauded. He did send an email which confirmed someone had tried to open a phone account in his name in 2022. But that does not evidence that anyone stole his identity in 2020, and the process for opening a phone account and bank account are quite different. As I noted above, the evidence strongly supports this being Mr W's account, and it's not likely or plausible that it was anyone else's account. But perhaps most importantly, Mr W has since admitted that this was his account.

I'll move on to addressing Mr W's second version of events: that an unknown person used the account without his permission.

In order to receive and spend the fraudulent funds, the person using the account needed multiple security details of Mr W's. And it's currently unclear how an unknown person would've had these without Mr W's consent. While the technical data is more limited due to the time that's passed, I've not found any evidence of the security being bypassed.

More importantly, one-time passcodes were sent to the registered mobile phone number – the same number Mr W gave us and still uses now. So I'm reasonably satisfied that Mr W received those codes. And he would need to have either entered them himself or given them to someone in order for the fraudulent funds to be spent like they were. Further, the payees involved were set up using Mr W's mobile number well in advance of receiving the fraudulent funds. So we can be reasonably satisfied that Mr W was directly involved in the fraudulent activity on his account.

Similarly, the fraudulent funds were sent to a cryptocurrency wallet in Mr W's name. The only other transactions also went to Mr W's other accounts. So Mr W appears to have been the sole beneficiary of the fraud. It is neither likely nor plausible that an unknown person would go through substantial risk and effort to carry out complex fraud, just to give all the proceeds to Mr W. In this situation, the only reasonable explanation for Mr W profiting from this fraud is that he was involved in it.

As noted before, Mr W was sent contact about the account's activity, and he also called Metro to discuss it. So he was aware of the activity on his account at the time. From what I can see, Metro made him aware that he needed to contact their fraud team to justify the account activity, and they chased him. So Mr W reasonably knew what had happened on his account, he knew he was in trouble for fraud, and he was also notified that his account would be closed. Yet at the time, he did not query this, dispute the activity, or tell Metro that these were not his transactions.

Mr W pointed out he had an unauthorised payment on a PayPal account in 2023. But again, I'm afraid that's not really relevant. That was a completely different account to this one, which works in a different way, and happened in a different year. It does not reasonably relate to this situation. As I've discussed above, in *this* situation I've found that it's neither likely nor plausible that the account activity happened without Mr W's knowledge or consent. Similarly, while Mr W points out that he's not been caught doing any fraud since, that does not rule out that he was involved in *this* instance of fraud.

As I've found that it's most likely this was Mr W's account, and that it's most likely Mr W authorised the account's activity, I will turn to whether the resulting marker was fair or not.

While Mr W says he opened this account for savings, he did not use it for savings. In fact, there was no normal saving or spending on the account at all. Essentially, he opened it, made some small test payments between his other accounts and crypto wallets, then received and spent the proceeds of fraud. As noted before, Mr W did not challenge Metro when they asked him about the activity, made him aware he was in trouble for fraud, or closed his account.

Indeed, the activity on Mr W's account is highly consistent with fraudulent use. For example, Mr W emptied his account of his own funds beforehand, such that none of his own money could be used to repay the fraud victim. He made test payments, as noted above. Then when the fraudulent funds came in, he acted quickly to send them on to his crypto account, which meant they couldn't be recovered once the fraud was reported. And as far as I can see, Mr W was the only beneficiary of the fraud.

There is no evidence that Mr W was in any way entitled to the money he received and spent. Whereas Metro received an official report that the money he received and spent came from a victim of crime, who'd been defrauded into paying Mr W.

Mr W's testimony has been notably contradictory, and at points clearly untrue. For example, at different points he said the account was opened fraudulently without his knowledge, or that he opened it himself. He repeatedly said the activity was carried out by a close friend, then said he didn't know the person who'd carried it out. He said he opened the account for savings, but he didn't pay any savings into the account, he only used it to facilitate fraud. He said he closed the account himself due to the fraud, but he did not – Metro closed the account themselves after giving Mr W notice, and there is no record of Mr W ever asking for it to be closed. Mr W says these were just mistakes or poor choices of words on his part. But that's not plausible. These are clear contradictions, and they mean that I cannot reasonably rely on any of Mr W's versions of events.

Lastly, I've not found any evidence which makes it seem implausible or unlikely that Mr W was knowingly involved in the fraud.

In summary, the evidence supports that Mr W opened this account and authorised the activity on it, and that the activity in question was fraudulent. It's not likely or plausible that the fraud happened without Mr W's knowledge or consent, as he's claimed. Mr W appears to have been the main beneficiary of the fraud. There's no evidence he was entitled to the money. And his testimony has contradicted both itself and the evidence at hand.

So based on that, I can only fairly conclude that Metro were justified in closing the account and registering a marker against Mr W at CIFAS. This is a difficult message for me to give, and I know it's a difficult message for Mr W to receive. But given the evidence I have, and the balance of probabilities, I'm unable to reasonably reach any other conclusion.

My final decision

For the reasons I've explained, I don't uphold Mr W's complaint.

This final decision marks the end of our service's consideration of the case.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr W to accept or reject my decision before 15 May 2024.

Adam Charles
Ombudsman