

The complaint

Mr D is unhappy that Barclays Bank UK PLC closed his bank account and loaded fraud markers against his name.

What happened

Mr D held an account with Barclays. In May 2021, Mr D received a letter from Barclays informing him that it'd frozen his account. It told Mr D that it needed to review some payments into the account and asked him to get in touch.

Mr D contacted Barclays but claimed no knowledge of the payments entering the account. Barclays decided to withdraw Mr D's banking facilities with immediate effect and load his information to fraud databases.

Mr D was unhappy with Barclays' decision, so he made a complaint. Barclays contacted Mr D to obtain more information on what occurred at the time of the transactions entering his account. Mr D maintained that he had no knowledge of the payments into his account and provided an explanation regarding some of the outbound payments. He said that some of these were payments to buy products that he sells and others, to a cryptocurrency platform, he wasn't aware of. Mr D said that he'd not shared his account details or security information with any third-party.

Barclays didn't overturn its original decision based on the information Mr D provided. Mr D, being unhappy with this response, referred his complaint to our service.

An Investigator considered the evidence provided by both parties but concluded that Barclays hadn't made an error. Broadly, the Investigator said that there was no evidence to support Mr D's testimony. They also commented on Mr D providing conflicting testimony and couldn't substantiate a point of compromise for his account.

The Investigator also felt that the account closure was fair in the circumstances. They pointed out that the terms and conditions of the account had been breached and Barclays had the right to close the account as it did in line with those terms.

Mr D disagreed with the Investigator's assessment. He maintained that he was of good character and had not committed any fraud on his account. He also described the detrimental impact the fraud marker was having on his day-to-day life.

As Mr D disagreed with the Investigator's opinion, the matter has now been passed to me for a final 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.

Fraud marker loading

In order to decide what's fair and reasonable, I've taken into consideration the relevant guidance set out by the fraud marker database controller: Cifas. In its Handbook, Cifas provides its members with expectations on the required burden of proof needed to load markers. This includes:

- It has reasonable grounds to suspect that a fraud or financial crime has been committed or attempted.
- That the evidence must be clear, relevant and rigorous such that the member could confidently report the conduct of the subject to the Police.

My interpretation of these rules is that Cifas requires a high bar to be met in order to load markers to its database. That bar isn't so high that the person must be proven beyond all reasonable doubt to have been involved in the fraud or financial crime, but it needs to be more than mere suspicion.

Mr D's testimony throughout has generally been that he had no awareness of the funds entering his account. However, the evidence provided by both parties suggests that this isn't likely. I'll explain why.

While I acknowledge that there is a remote possibility that a third-party paid Mr D's account by accident—by inputting the incorrect account information—that doesn't explain some of the other activity present on Mr D's account.

Mr D has told our service that he hadn't provided any of his account information to a third-party: that includes his security information. He's also told us that he has never had any dealings or relationship with the cryptocurrency platform where several of the fraudulent payments were forwarded to. But the evidence doesn't support this either.

On 19 April and 5 May 2021, a £2 bill payment was made to the same cryptocurrency platform that was paid after the fraudulent funds were paid into Mr D's account. The payments also bear the same reference details. There is no evidence that Mr D challenged or disputed these payments prior to the fraudulent activity despite using his account regularly between. And this would suggest he was likely aware of the payments and had likely authorised them. This is supported by the fact that Mr D admitted to making one of the payments to the cryptocurrency platform prior to the fraudulent payments when questioned by Barclays. However, I realise Mr D has since said that he had no knowledge of this platform.

Furthermore, there is no likely explanation as to how an unknown third-party accessed Mr D's account without his authority. Mr D says he's never provided his account or security information to anyone. Considering the amount of information that is required to logon to an online banking account, I can't see how someone could have guessed this information.

Barclays has also told our service that a new device logged onto Mr D's account prior to the fraudulent activity. And in order for the new device to be added to the account, a text message was sent to Mr D's registered telephone number to authorise its use. As the correct code was entered to allow the device access, this could only mean that either Mr D registered the device himself, or, he passed this information onto a third-party.

In either scenario, I think there is persuasive information to support that Mr D likely knew about the activity on his account. And so it follows that the burden of proof required to load the fraud markers has been met in the circumstances.

Account closure

Businesses do have the right to end their relationship with a customer. Broadly speaking, it must be done so in line with the account's terms and conditions and in compliance with the law. I can also consider if the account closure was fair and reasonable in the circumstances.

In section 5 of Barclays' terms of the account, it sets out circumstances in which it may end an agreement with a customer immediately or with less notice. These include, but are not limited to, where the bank has reasonable grounds to believe the customer has:

- Seriously or persistently broken any terms of the agreement.
- Committed (or attempted) fraud against Barclays or someone else.
- Used their account illegally or for criminal activity, including receiving proceeds of crime into their account – or if they let someone else do this.

It's clear from the evidence that Mr D's account did receive funds that originated from crime. And this in turn presented a substantial risk to the bank. It also had no evidence to reasonably suspect a third-party had compromised Mr D's account.

I therefore find that in line with the terms and conditions of the account, and considering what I deem to be fair and reasonable, the immediate closure in these circumstances was fair.

My final decision

For the reasons I've given above, I don't 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 18 November 2022.

Stephen Westlake
Ombudsman