

The complaint

Miss B is unhappy that Kroo Bank Ltd applied a fraud marker against her name.

What happened

In February 2024, Miss B opened an account with Kroo. Between 22 February 2024 and 6 March 2024, the account received faster payments from a number of different people. The funds were transferred to one of Miss B's relatives.

On 6 March 2024, Kroo sent a message to Miss B. It asked her how she intended on using the account and asked for some supporting documentation for the payments that had been received into the account to date. Kroo received a reply explaining that the funds were from friends and family that were helping financially. The reply said that they were all very close people and the references to the payments explain that the money is a gift or for food and shopping. Kroo closed Miss B's account on 7 March 2024.

In May 2024, Kroo received a fraud report alleging that funds paid into Miss B's account in March 2024 had been received fraudulently. It carried out an investigation and asked questions in its in-app chat about the disputed transfers. Kroo received a response from Miss B's credentials explaining that the funds were from a friend she had met on a mobile phone app who was helping her when she wasn't working.

In August 2024, Miss B contacted Kroo to query a fraud marker it had loaded against her name on the Cifas database. She told Kroo that she had been a victim of a scam and provided a reference number from Action Fraud. She said that she had not been involved with the Kroo account and wanted Kroo to remove the fraud marker.

Kroo looked into Miss B's complaint. In its final response it said it had made the decision to close her account in line with its terms and conditions and hadn't made an error in loading the marker. Miss B referred her complaint to us.

Miss B told us she had been a victim of a scam. She explained that around February 2024, she and another member of her family joined a group online that was offering discounts on items from a well-known online retailer. Miss B explains that after joining the group, her mobile phone was hacked, and she no longer had access to her banking apps.

Our Investigator looked into the situation but didn't uphold the complaint. They felt Kroo had adhered to the standards set out by Cifas when loading the marker. They pointed out there were inconsistencies in what Miss B said happened. Miss B told our Investigator that someone else responded to Kroo's questions about the activity on the account. But the Investigator wasn't persuaded that a hacker would respond to the bank to answer questions about a closed account, nor was she persuaded that someone could have gained access to Miss B's Kroo account by clicking a link for discounted goods. They also weren't persuaded that a hacker would have transferred funds into an account belonging to one of Miss B's relatives. The Investigator concluded that Kroo received reasonable evidence and information to suggest Miss B's account had been in receipt of fraudulent funds and that Kroo had not acted unfairly by recording a fraud prevention marker.

Miss B didn't agree. She said she was innocent and had no bad intentions when opening the account. She provided screenshots of conversations with her relative to support that they had both been victims. Our Investigator wasn't persuaded they were enough to show it was wrong of Kroo to record a Cifas marker.

As no agreement could be reached, the complaint has been referred 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.

One of the relevant considerations here is set out by Cifas: the fraud marker database controller. In its Handbook—which members must adhere to when loading markers—it sets out the burden of proof the member must meet. The relevant standards regarding this complaint are:

1. That there are reasonable grounds to believe that a fraud or financial crime has been committed or attempted.
2. That the evidence must be clear, relevant and rigorous such that the member (Kroo) could confidently report the conduct of the subject (Miss B) to the police.

My interpretation of these standards is that a member cannot simply load a marker against an individual based on mere suspicion. It must be able to meet a higher bar; in that a customer was likely a witting participant in the alleged conduct. This has been reinforced by Cifas' Money Mule Guidance, which it released to its members in March 2020.

Having considered the evidence carefully, I'm satisfied Kroo has been able to demonstrate it has met the first of the two standards I've listed above. It's been able to show that it received a report of a potential fraud from a third-party bank setting out the transactions that were reported as fraud by its account holder. This clearly meets the bar that there are reasonable grounds to believe that a fraud or financial crime has been committed. So, I've gone on to consider if Kroo has been able to meet the second of the above two standards.

Miss B maintains that she's been the victim of a scam after clicking a suspicious link, but there does appear to be inconsistencies within the evidence available to support her submissions.

Miss B says a hacker accessed her Kroo account. But clicking the links as she's described would not have disclosed her Kroo mobile app security credentials to a third party, so it remains unclear to me how a hacker could have gained access to Miss B's account or why a hacker would have sent the funds to one of Miss B's relatives after gaining access to the account.

Miss B says she did not respond to Kroo's questions, it was someone else. She's told us that she did not get the opportunity to use the Kroo account before the scam happened. But I'm not persuaded that a hacker would have engaged with Kroo's information requests after the account had been closed, nor do I understand why a hacker that was connected to an online shopping group would have told Kroo that they recognised incoming payments as being made by friends and family that were helping them financially. I'm also mindful that the information that was given to Kroo about interaction on a mobile phone app broadly aligns with the information provided by the sending account holder when they reported a potential fraud.

Miss B has explained how upsetting this situation has been and continues to be and I have considered what she's said about the impact the fraud marker is having on her. But for the reasons I've explained above, I don't find what she's said about the scam to be credible or plausible. I'd like to make it clear that my findings aren't intended as an accusation that Miss B has committed a fraud, only that Kroo has demonstrated sufficient evidence that it loaded the marker in line with the standards set out by Cifas.

My final decision

My final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss B to accept or reject my decision before 21 February 2025.

Claire Marsh
Ombudsman