

## The complaint

Miss M has complained that Kroo Bank Ltd registered a fraud marker against her.

## What happened

In May 2023, a new device was registered to Miss M's Kroo account. Shortly afterwards, the account received the proceeds of fraud, which were sent on via an online card payment.

Kroo contacted the registered email address about the activity, but received no reply. So it closed the account and registered a fraud marker against Miss M.

In February 2024, Miss M complained. She explained her email had been compromised and her account was hacked. She said she hadn't carried out the disputed activity. Kroo referred her to our service.

Our Investigator looked into things, and didn't uphold the complaint. Miss M appealed, so the complaint's been passed to me to decide.

I sent Kroo and Miss M a provisional decision on 12 August 2024, to explain why I thought the complaint should be upheld. In that decision, I said:

*I need to consider whether this report to Cifas was made fairly. On this point, Kroo needed to have more than just a suspicion or concern. It needs to be able to show that it had reasonable grounds to believe that Miss M had knowingly and willingly involved herself in an attempt to commit fraud or a financial crime, backed up by evidence rigorous enough to support the matter being reported to the authorities.*

*I should clarify that the matter of whether or not the account's activity was carried out with Miss M's knowledge and consent is central to the matter of whether or not she should have this fraud marker registered against her. Because the fraud marker would only be fair if she were a knowing and witting participant in the fraud. Whereas if, for example, her account was hacked and used without her knowledge or consent, then it would be unfair to maintain a fraud marker against her and it would need to be removed. Our Investigator was mistaken to suggest that those matters should be considered separately.*

*We repeatedly requested key evidence from Kroo, starting from 1 May 2024. However, this has not been received. The onus is on Kroo to evidence that this fraud marker is justified, and as part of that: to evidence that the account's activity was carried out with Miss M's consent. Without that, the default position is that the marker must now be removed.*

*As Kroo has not provided the requested evidence, I do not have a sufficient basis on which to conclude that the disputed activity was properly authenticated – let alone that it was made with Miss M's consent. And Kroo has not provided any evidence which reasonably shows that Miss M was knowingly involved in the activity here.*

*From the evidence which has been provided, I can see that a new device was registered to the account shortly before the disputed activity started. And it looks like this wasn't Miss M's usual device. Miss M has provided evidence supporting the possibility that her email account was compromised, which could well have led to her Kroo account being accessed without her consent. And it looks like it was possible for a fraudster to learn Miss M's card details from the Kroo app directly.*

*So I've not been given sufficient evidence to show that Miss M was knowingly involved in the fraudulent activity. On the other hand, it seems there's likely and plausible ways that her account may have been used without her consent. As such, I currently think that the fraud marker should be removed.*

*Of course, I do appreciate that at the point Kroo registered the marker, Miss M had not yet contacted it to explain herself. So at the time, Kroo didn't know about the allegation that her account was hacked – all it knew was that her account had been used for fraud and it wasn't getting a reply from her email. Further, Miss M has accepted that even after she regained access to her email account and saw Kroo's contact, she didn't get in touch until months later. So Miss M did delay things herself.*

*As such, I'd only tell Kroo to pay compensation for the stress it caused in failing to remove the marker after it was given the allegation that Miss M's account was compromised. Taking into the account the impact that had on Miss M – including the stress and upset she felt, and the disruption at being unable to keep accounts open – alongside our guidelines for awarding compensation, I currently think that Kroo should pay her £200 to put things right.*

*Lastly, I've also considered whether Kroo acted fairly in closing Miss M's account. Based on what it knew at the time, I think it did. Miss M did not explain herself until 2024, so far as Kroo could tell back in 2023, the account was being used for fraud and needed closing. Further, Miss M has accepted that she did not take sufficient care of the account – which contributed to its closure. And she wasn't using it at the time anyway, so its closure won't have caused her much in the way of impact.*

I said I'd consider anything else anyone wanted to give me – so long as I received it before 26 August 2024. I'll talk about the replies below.

### **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.

Kroo disagreed with the provisional decision. It claimed that in order to register the disputed device, someone would've needed not just Miss M's email address, but also a one-time passcode sent to her phone number.

However, Kroo did not provide any evidence of this process, nor any evidence to show that the process was properly followed here. It did not provide any evidence that this one-time passcode was sent, nor conclusive proof of which number it was sent to, nor evidence that it was entered properly – as opposed to being bypassed, for example. It did not provide any technical information to rule out the possibility that the phone number was spoofed or subject to a SIM-swap scam and so on. And it did not provide any of the other technical information we asked for – such as audit trails, IP address information, authentication evidence and so on – which might otherwise substantiate that Miss M authorised the activity involved.

As such, it remains the case that Kroo has not sufficiently evidenced that the disputed activity was properly authenticated – let alone that it was made with Miss M's consent. And it has not evidenced that Miss M was knowingly involved in the activity here. As far as I can see, the disputed activity took place on a new device which was not Miss M's normal device, Miss M has provided evidence supporting the possibility that her email account was compromised, and there was a clear point of compromise for the card details too.

Kroo pointed out that after Miss M regained control of the account and it told her it was closing the account, she attempted to pay out the remaining balance of the disputed credits – around £5. But Miss M has already explained that she only did so because Kroo's own instructions said that's what she should do. And I can indeed see that it says one needs to transfer positive balances to another bank before Kroo can close one's account. So I can see why Miss M would think that's what she needed to do here. The amount there was not significant, and Miss M has repeatedly and consistently explained that she does not otherwise claim any entitlement to the money, she was happy for it to be returned in the end, and she was just doing what she thought she was supposed to. So we can plausibly chalk that up to being a misunderstanding. It's not a sufficient basis for this fraud marker.

Similarly, Kroo pointed out that Miss M didn't raise concerns until February 2024. But given that she was happy for the money to be returned to sender in the end, her main account was at a different bank, her own money wasn't at risk, and she didn't know about the fraud marker until then, I can see why she might not have felt the need to raise a complaint until then. Again, this was not a sufficient basis for a fraud marker – Kroo needed to be able to show that Miss M had knowingly and willingly involved herself in attempted fraud or financial crime, backed up by rigorous evidence to report it to the authorities. And its terms and conditions about sharing data with fraud prevention agencies does not overrule those requirements, nor absolve Kroo of its responsibilities.

Ultimately, I'm afraid that Kroo has provided too little evidence, too late. In order to defend itself in this case, it really needed to provide the evidence we told it to provide, in full and on time, rather than only providing insufficient snippets of evidence at the last minute.

Meanwhile, Miss M accepted the provisional decision. She added that Kroo had declined to give her technical information which might help her show her innocence. She said the stress from the situation had exacerbated her health problems. And she'd had to use a less convenient type of account due to the difficulties the marker caused in keeping accounts open. So this only reinforces that Kroo should pay Miss M compensation – though I must bear in mind that this is only applicable for the period *after* Kroo was given the allegation that Miss M's account was compromised, and that a good deal of Miss M's distress would've been caused by the fraudster rather than Kroo.

So having reconsidered the case, I've come to the same conclusion as before.

## **Putting things right**

I direct Kroo Bank Ltd to:

- remove any information it's shared with fraud marker databases in relation to this matter; and-
- pay Miss M £200 compensation for the trouble and upset it caused.

## **My final decision**

I uphold Miss M's complaint, and direct Kroo Bank Ltd to put things right in the way I set out above.

If Miss M accepts the final decision, Kroo Bank Ltd must carry out the redress within 28 days of the date our service notifies it of the acceptance.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss M to accept or reject my decision before 23 September 2024.

Adam Charles  
**Ombudsman**