

The complaint

Miss M complains Revolut Ltd registered a fraud marker at CIFAS, the national fraud database. She doesn't think it's done so fairly.

What happened

Miss M held an account with Revolut. Between 10 and 12 December 2022, her account was credited with a number of payments from third parties through bank transfers. Immediately afterwards, a lot of the money was withdrawn through payments to a cryptocurrency business who I shall refer to as 'N'.

Payments into the account were identified as fraudulent because several of the banks from which the funds had come, notified Revolut that their customers had been the victim of a fraud. Miss M told Revolut that she didn't recognise or authorise any payments on her account from 9 December. Revolut investigated and said that following a review, it would be withdrawing banking facilities and closing her account.

Miss M found it difficult to get banking facilities elsewhere (after another provider also closed her account). Upon making a subject access request, CIFAS told Miss M that Revolut had also recorded a 'misuse of facility' marker against her.

Miss M complained to Revolut. She said she wasn't involved in anything that had led up to the marker. She thought scammers were involved in what had happened and she didn't think Revolut had treated her fairly. But Revolut didn't think the activity could have happened without Miss M's knowledge or involvement. It didn't accept that someone had taken over the account. It believed it had correctly recorded the marker and wouldn't agree to remove it.

Miss M referred matters to us. One of our adjudicators looked at the complaint. Ultimately, she thought that Revolut had acted fairly in the circumstances. She noted that Revolut's records showed that an earlier payment to N had been held for a fraud check and was verified by Miss M as being genuine on its online app chat facility. The evidence also showed the payments to N had been made using Miss M's mobile banking app and from a mobile device that matched hers. She noted that Revolut had also sent SMS messages to the phone to assist in verifying the payments. And as she'd not disclosed her mobile banking information/passcodes to anyone or lost her phone, the investigator couldn't understand how the payments could have been made, unless Miss M was complicit in some way.

Miss M disagreed so the complaint has come to me. In summary, she has made the following points:

- She would never have spoken to Revolut about N and cryptocurrency.
- She hadn't got any SMS messages from Revolut about the transactions.
- She believed scammers had got her details and made the transactions by getting into her phone.

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.

Firstly, for the purposes of clarity this decision will only focus on the complaint brought against Revolut. It will not deal with or comment on any other complaints Miss M may have about other respondent businesses.

The marker that Revolut has filed is intended to record that there's been a 'misuse of facility' – relating to using the account to receive fraudulent funds. In order to file such a marker, it's not required to prove beyond reasonable doubt that Miss M is guilty of a fraud or financial crime, but it must show that there are grounds for more than mere suspicion or concern. The relevant guidance says, there must be reasonable grounds to believe that an identified fraud or financial crime has been committed or attempted and the evidence must be clear, relevant, and rigorous.

What this means in practice is that a bank must first be able to show that fraudulent funds have entered Miss M's account, whether they are retained or pass through the account.

Secondly, the bank will need to have strong evidence to show that Miss M was deliberately dishonest in receiving the fraudulent payment and knew it was, or might be, an illegitimate payment. This can include allowing someone else to use their account to receive an illegitimate payment. But a marker should not be registered against someone who was unwitting; there should be enough evidence to show complicity. To meet the standard of proof required to register a fraud marker; the bank must carry out checks of sufficient depth and retain records of these checks. This should include giving the account holder the opportunity to explain the activity on their account to understand their level of knowledge and intention.

Miss M says she doesn't know anything about fraudulent funds crediting and leaving her account from 9 December. She has said the first she knew about this was when she got back from her holiday. So, I need to decide whether I think Revolut has enough evidence to show fraudulent funds entered Miss M's account and she was complicit. And I'm satisfied it has. I'll explain why.

I've seen evidence from Revolut that it received reports from a number of different third-party banks saying that some funds which entered Miss M's account were fraudulent. Miss M doesn't dispute this – but she says she has no knowledge of why those payments were made.

Once the funds entered Miss M's account, transfers were carried out fairly quickly to N using the Revolut mobile banking app registered to Miss M's account. I can say this because I've reviewed Revolut's mobile banking records and the device used to make the payments is the same device that Miss M had registered with it. And there were no other new devices or numbers added.

Miss M says this wasn't her making the payments, including the payment to N on 10 December for £1900 that was verified as genuine during an on-line app chat. She's also said that no one else knew her mobile banking details and passwords as she'd never disclosed or shared them either directly or through links. She lives alone and her phone wasn't missing. However, thinking about this it's difficult to see how someone could have done this and made the payments without her knowledge if all her details and information were kept secure.

Miss M has said scammers must have got into her phone and carried out the transactions, but there's no tangible evidence to support this is what happened. Also, presumably she would have still got the SMS messages. But she says she didn't. Overall, I consider the possibility of scammers doing this without Miss M's involvement is highly unlikely based on the available information and I'm satisfied the mobile banking app records are compelling evidence in this complaint.

I'm sorry to hear about the difficulties Miss M is facing opening an account, but I'm not going to require Revolut to do anything further here. For the reasons I've outlined, I think Revolut followed the relevant guidance when loading the fraud marker.

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 M to accept or reject my decision before 21 December 2023.

Sarita Taylor
Ombudsman