

The complaint

Miss S has complained that Revolut Ltd won't refund transactions she says she didn't make or otherwise authorise.

What happened

In early 2023, two bank transfers were made using Miss S's mobile banking app, totalling £450.

Miss S says this wasn't her. She said her phone was hacked and disabled. Her phone was with her at the time, it was never lost, it was locked with a code, no one else had access to it, she hadn't received any unusual contact, clicked any unusual links, or downloaded any new apps recently, and she'd never shared her app or security details with anyone.

Revolut held Miss S liable for the payments in dispute. They found they'd been made using her genuine phone and security details along with one-time passcodes, and there didn't seem to be a likely way this could've been done without her consent.

Our investigator looked into things independently and didn't uphold the complaint. Miss S didn't agree. She particularly felt that the transactions hadn't been authenticated properly and that they must have come from a different IP address to hers. She asked for an ombudsman to look at the case afresh, 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.

Broadly speaking, Revolut can hold Miss S liable for the payments in dispute if the evidence suggests that she authorised them.

I'm satisfied from Revolut's technical evidence that the payments in dispute used Miss S's genuine mobile phone and app, her correct security details, and one-time passcodes that were sent to her mobile phone number. So I can see that these transactions were properly authenticated. The question, then, is whether the evidence suggests that it's most likely Miss S consented to the transactions, or not.

The disputed payments were made using Miss S's mobile phone – not any other device. This phone was with Miss S at the time, hadn't gone missing, was protected by a code, and only she had access to it. I can see that Miss S had access to this phone at the time as she used her Revolut app just minutes after the disputed payments. So there's no likely or plausible way that anyone else could've been using her phone in person.

I've also considered the possibility that Miss S's app was accessed remotely – i.e. that she was hacked, as she suggested. But Miss S told Revolut she had not received any unusual contact, clicked any unusual links, downloaded any new apps, shared any of her details, used any shared wallets, shared her account, or anything like that. So it's unclear how she could have been hacked. And these payments were properly authenticated using Miss S's security details, which only she knew. There doesn't seem to be a likely or plausible way a thief could've learned those details without Miss S's consent. Further, the payments were made from the same IP address that Miss S used for her genuine spending and activity. The technical data does not show that anyone other than Miss S made the disputed payments. I find it's not likely or plausible that the payments were made through hacking.

Miss S said that her phone had been effectively disabled. But I can see that she used her phone and mobile app to make a genuine payment straight after the disputed payments, to a person she'd paid many times before. She then used her phone to chat with Revolut and carry out other genuine activity a couple of minutes after that. So I can see that her phone was working and she was able to access her app at the time.

Miss S said that she wasn't asked for any confirmation for these transactions or given any warning. However, I can see that she was sent one-time passcodes to her mobile phone number to check whether she really wanted to make these payments. These passcodes were then entered to confirm the transactions and let them go through. And before letting her make the payments, Revolut also displayed a warning that she should make sure she knows and trusts the payee, as they might not be able to recover her money, and if she's unsure then she shouldn't make the payment. It's recorded that Miss S chose to proceed.

I might've expected a thief to try to take as much money as possible, as quickly as possible. But here, there were no further attempts to pay the disputed payee, and the majority of Miss S's balance – a significant sum – was left untouched. This also tends to indicate that the disputed payments were not made by a thief or fraudster.

Lastly, I've not seen any evidence that makes it seem implausible or unlikely that Miss S could've authorised these payments or given someone else permission to make them.

In summary, I'm satisfied that Miss S's genuine phone, app, and security details were used, along with one-time passcodes sent to her genuine number. There is not a likely or plausible way that someone could've made these payments without her consent, and the way the activity took place indicates that it was genuine. So it seems fair for Revolut to decline a refund in this case. This is a difficult message for me to give, and I know it's a difficult message for Miss S 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 Miss S'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 Miss S to accept or reject my decision before 27 September 2023.

Adam Charles
Ombudsman