

The complaint

Mr D complains that Revolut Ltd didn't protect him when he fell victim to a job scam.

What happened

In June 2023, Mr D was actively looking for additional work and received a WhatsApp message from someone he thought was associated with the recruitment firms he contacted. They offered him a job where he had to complete tasks associated with reviewing products for a mall. Shortly after starting the job, Mr D had a negative balance on his account which prevented him from completing tasks. It was explained he needed to recharge his account with his own funds via a cryptocurrency merchant, but he'd be able to withdraw once he'd completed the required tasks.

Mr D realised he'd been scammed after sending just over £8,700 pounds to a cryptocurrency merchant. He wasn't able to withdraw, and the scammer ceased contact with him. He complained to Revolut that it failed in its duty to protect him, but it didn't uphold his complaint. Mr D came to our service, but our investigator also didn't uphold his complaint. Mr D asked for an ombudsman to review his case as he said Revolut failed to recognise he was at risk of financial harm and if it had spoken to him, it would've unravelled the scam.

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.

In broad terms, the starting position at law is that an Electronic Money Institution ("EMI") such as Revolut is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account.

But, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in June 2023 that Revolut should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;
- have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – (as in practice Revolut sometimes does including in relation to card payments);
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts

as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

I'm satisfied that Revolut ought to have recognised that the £2,500 card payment Mr D made on 5 July 2023 carried a heightened risk of financial harm from fraud. This is because it was the 4th payment to cryptocurrency merchants within an hour that day and took the spending on cryptocurrency to a fairly high figure. At this time Revolut should've been aware of the increased prevalence of cryptocurrency related scams and the common spending patterns involved with these.

I think that a proportionate response to that risk would have been for Revolut to provide a tailored written warning for the most common kind of scam associated with these kind of payments – so cryptocurrency investment scams. But, had it done so, I'm not persuaded that would have prevented Mr D's loss or him making further payments. I'll explain why.

Mr D was falling victim to a job scam, not a cryptocurrency investment scam. So the content of the warning would largely not have related to his situation and so wouldn't have been concerning to him. It's possible the warning could have included some information around being contacted by, and/or being asked to make payments by, an unknown party. But we're aware that the cryptocurrency merchant Mr D paid provided him with a warning which included this information, but this did not stop him completing the transaction. And considering Mr D was actively looking for extra income, he may not have considered that the scammer's contact fitted this situation.

Mr D's representative has said that a human intervention was warranted in this case, but I don't agree that this would be proportionate in the circumstances. Many payments that look very similar to Mr D's will be entirely genuine. And I've given due consideration to Revolut's duty to make payments promptly, as well as what I consider to have been good industry practice at the time this payment was made.

I'm satisfied that a proportionate way in this case for Revolut to have minimised the risk of financial harm to Mr D would've been to show a tailored warning covering the key features of scams affecting many customers. This wouldn't have imposed a level of friction disproportionate to the risk the payment presented, but would've looked to address the risk. But unfortunately this wouldn't have prevented Mr D's loss in this case, for the reasons already explained.

I've considered whether Revolut could've recovered the funds after the scam, but I'm not persuaded there were any prospects of it successfully recovering the funds, given the money was used to purchase cryptocurrency from a legitimate provider.

Whilst Mr D has undoubtedly been the victim of a cruel scam, I don't find there were any failings on Revolut's part that would lead me to uphold this complaint.

My final decision

For the reasons given above, my final decision is that I don't uphold Mr D's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr D to accept or reject my decision before 17 January 2025.

Amy Osborne
Ombudsman