

## **The complaint**

Mrs R complains that Revolut Ltd won't refund money she lost when she fell victim to an employment scam.

Mrs R is being represented by solicitors in this complaint.

## **What happened**

The detailed background to this complaint is well known to the parties. The facts about what happened aren't in dispute, so I'll provide a brief overview and focus on giving my reasons for my decision.

The complaint concerns eight transactions – faster payments and debit card payments – totalling over £8,000 which Mrs R made in May 2023 in connection with a job opportunity with a company "S", who she came across on a popular social media platform. Mrs R understood that the job involved completing 'tasks' assigned to her on S's platform which were in relation to product reviews. She was told she could earn wages through commission and a basic salary. When she couldn't withdraw her wages, Mrs R realised that she'd fallen victim to a 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. It's not in dispute that Mrs R authorised the payments in question.

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 May 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), and

- 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've reviewed the available information and I'm not persuaded that Revolut ought to have recognised that the transactions carried a heightened risk of financial harm.

I acknowledge that there were several transactions in one day – six on 11 May. But that in and of itself doesn't mean the transactions ought to have flagged as suspicious to Revolut. The transactions were spread over nine hours and were relatively low in value. Only the first three transactions (the debit card payments) were identifiably cryptocurrency related. Given their individual and combined values, considered in conjunction with previous history of cryptocurrency related transactions on Mrs R's account, I wouldn't have expected Revolut to have been on notice that Mrs R was at a heightened risk of harm from financial fraud.

I understand that the subsequent payments, made to individuals, were peer to peer cryptocurrency purchases. But that isn't something Revolut could have reasonably known. Given the amounts involved, I'm not persuaded that they warranted an intervention beyond the provision of a new payee warning.

Mrs R's representative submits that several credits followed by payments ought to have appeared unusual. But I think it's important to note that e-money accounts tend to be used in a different way to regular bank accounts. It isn't that unusual for funds to be credited just before being paid out. People tend to top up the account as and when required to make a payment. A review of Mrs R's account supports this pattern of activity.

The representative has also said that Mrs R took out a loan with another business to fund the payments and this trend (of taking out loans) should have been picked up by Revolut. But Revolut couldn't reasonably have known from the transactions on Mrs R's Revolut account that she had taken out a loan. The loan proceeds were paid into her account with another business before being transferred into her Revolut account through card top-ups.

In summary, given what Revolut knew or ought to have known about the destination of the payments, and how Mrs R used her account, on balance, I'm not persuaded that Revolut acted unfairly or unreasonably in executing her authorised instructions.

Thinking next about the recovery of payments, given that the transactions made from Mrs R's account involved purchasing cryptocurrency from legitimate sellers it's unlikely recovery would have been successful. We know from her submissions that the cryptocurrency purchase was successful. So, services were rendered by the recipient of Mrs R's payments. I don't think Revolut could or should have taken further steps to recover funds from cryptocurrency sellers.

In summary, I recognise that Mrs R will be disappointed with this outcome. I'm sorry that she fell victim to such a cruel scam. But I have to consider whether Revolut could have prevented the scam from happening. Having given this some thought, as set out above, it wouldn't be fair of me to hold Revolut liable for her losses.

### **My final decision**

For the reasons given, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs R to accept or reject my decision before 2 January 2025.

Gagandeep Singh  
**Ombudsman**