

The complaint

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

Mrs L is being represented by solicitors in this complaint.

What happened

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

The complaint concerns several transactions totalling just over £39,000 which Mrs L made over a period of 12 days in May 2023. These were made in connection with a job opportunity which Mrs L was contacted about on an instant messaging platform. The representative from the recruitment company advised Mrs L that the job involved completing a set of tasks on an online platform to boost ratings for products.

It was explained to Mrs L that she needed to create an account with a cryptocurrency exchange as wages and commission would be paid in cryptocurrency. She was also told that she needed to make deposits in cryptocurrency as required to complete some of the tasks. To make that deposit, Mrs L first transferred money from her accounts with other payment service providers to Revolut, before buying cryptocurrency through peer-to-peer purchase. Once converted, the cryptocurrency was sent to cryptocurrency wallets as instructed by the third-party assisting Mrs L with the job.

When she was unable to complete tasks and instructed to top up her account with more money repeatedly, Mrs L eventually realised 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.

But, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to be good industry practice at the time, I consider it fair and reasonable that in May 2023 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),
- 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 considered the operation of Mrs L's account, and I don't find that the first disputed transaction – £41 on 4 May – should have given Revolut cause for concern. I accept that the account hadn't been used for months. But I haven't seen any other factors at play here such that, in my view, Revolut should have been concerned and ought to have taken additional steps before executing Mrs L authorised instructions.

The next transaction – £330 on 5 May – flagged on Revolut's fraud detection systems. It says it asked Mrs L to select the purpose of the payment from a list of options and displayed a warning based on the purpose selected. I understand that Mrs L selected 'safe account', and after displaying a warning covering the typical hallmarks of safe account scams, Revolut presented her with the option to (1) read its scam guidance, (2) get advice from one of its agents, (3) cancel the payment, or (4) go ahead with it. Mrs L decided to go ahead with the payment.

I don't think 'safe account' could ever be a legitimate reason for sending money to another account. While Revolut displayed warnings which covered the most common features of such scams, I think it ought to have contacted Mrs L to discuss the payment further, even if it meant directing her to an in-app chat. But I don't think that would have made a difference here.

The investigator made enquiries with Mrs L's representative about why she selected that option. Mrs L said she couldn't recall the reason, and that she may have selected safe account in error. So, had Revolut directed her to its in-app chat function for an agent to make further enquiries, on balance, I think it's more likely than not that Mrs L would have explained she'd selected that option in error.

Given that the transaction had triggered on Revolut's systems prior to it being told the 'safe account' payment purpose, I would have expected it to continue with its enquiries on discovering that Mrs L likely selected that payment purpose in error. But I'm not persuaded that this would have uncovered the scam. This is because on the day in question, Mrs L had made transactions linked to the scam from her account with another EMI. When asked for the payment purpose, she indicated she was buying goods and services.

The EMI in question had told our service that at the time of Mrs L's transaction, the payment purpose also included 'paying to earn money by working online' as one of the options. Given Mrs L didn't select that option when she made a payment from that EMI and instead said she was buying goods and services, I think it's most likely she would have given a similar answer to Revolut. There were no other factors at play here which in my view would have given Revolut cause to doubt Mrs L's response. In the circumstances, Revolut couldn't reasonably have prevented her from going ahead.

It's also important to highlight that the scammer was in constant contact with Mrs L. Reading the chat messages exchanged between them, whenever Mrs L raised any doubts, the scammer was able to provide reassurances. For instance, the day after Revolut flagged the transaction I've referred to above, a peer-to-peer cryptocurrency seller Mrs L was transacting with asked her if she was buying cryptocurrency to clear a negative balance. She put this to the scammer and said that it is what she was doing. Mrs L told the scammer that the seller had said many people were being scammed by false opportunity to gain money. But the scammer told Mrs L to say that she wanted the cryptocurrency for her own use, or to choose a different seller as the seller was always like that. The scammer told Mrs L that she also received similar messages randomly and it could be a 'bot' message. Although Mrs L said she didn't want to do something that wasn't safe, she felt reassured by the scammer's replies and went ahead with the cryptocurrency purchase.

This exchange of messages shows that Mrs L would likely have reached out to the scammer had Revolut made enquiries or provided warnings. And the scammer would have been able to provide reassurances and answer any queries she might have had following an intervention.

We also know that a few days later, when the other EMI blocked a transaction linked to the scam because it was concerned about the safety of her money, Mrs L carried on making payments from her Revolut account. And when another bank intervened and asked about a transfer that she was making into her account with Revolut, Mrs L said she was going to use her Revolut account while visiting abroad.

As Mrs L's representative knows (or ought to know), causation is a critical determinative factor. Based on my observations about the contemporaneous evidence, which I've set out above, I'm not convinced that better intervention by Revolut along the lines I've described above would have positively impacted Mrs L's decision-making. And much for the same reasons, I don't think further intervention at a later point would have made a difference either.

I've also thought about whether Revolut could have done more to recover the funds once it became aware of the situation. Given Mrs L had legitimately bought cryptocurrency from sellers who were unlikely to have been connected to the job scam, before sending it on to wallets in control of the scammer, it's unlikely recovery would have been successful. That said, I understand Revolut was able to recover around £4 from one of the beneficiaries.

What this means is that in the circumstances of this case, I don't consider Revolut acted unfairly. It follows that I don't find it liable for her financial loss. I know that Mrs L will be disappointed with this outcome. Not least because the matter has been ongoing for some time, and the investigator originally upheld the complaint in part. I acknowledge that there's a considerable amount of money involved here. Despite my natural sympathy for the situation in which Mrs L finds herself, for the reasons given, it wouldn't be fair of me to hold Revolut responsible for her loss.

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 L to accept or reject my decision before 23 August 2024.

Gagandeep Singh
Ombudsman

