

## **The complaint**

Mrs B complains that Revolut Ltd won't reimburse her after she fell victim to a job scam.

Mrs B is professionally represented in bringing her complaint to our service, but for ease of reference I'll refer to all submissions as being made by Mrs B directly.

## **What happened**

The circumstances of the complaint are well known to both parties, so I won't repeat them in detail here. But briefly, both parties accept that in around January 2023, Mrs B was approached via an instant messaging app by an individual purporting to work for a recruitment company, offering part time roles. As Mrs B had been looking for work online, this did not appear unusual to her. Mrs B expressed her interest and was passed on to another individual who claimed to work for the company offering employment. Unfortunately, unbeknownst to Mrs B at the time, both individuals she'd spoken to were in fact fraudsters.

Mrs B was told the job entailed working for a known firm, finding products and improving sales for them. Mrs B was told she needed to complete 40 'orders per day' and that the daily income for doing so was over £100, plus bonus payments for working consecutive days and additional commission. Mrs B was told the job would take around 20-40 minutes per day to complete.

Mrs B created an account with the firm, as well as separate cryptocurrency accounts. She was told that for some orders, she would need to add funds to her account via cryptocurrency. Mrs B was added to an instant messaging group with other fraudsters posing as employees, where she could see positive posts of them receiving their daily commission. However, when Mrs B attempted to complete her own 40 tasks, she kept receiving requests for further funds to be added to her account, increasing in value each time, then additional tasks were added which Mrs B was told was due to a 'lucky bonus' and additional fees to withdraw her funds.

Mrs B made payments towards the scam from several of her bank account providers, as well as pension withdrawals, re-mortgages and loans from friends. Mrs B's losses from just her Revolut account are around £100,000, made up of around 20 transactions, mostly card payments, to cryptocurrency platforms.

When the fraudster kept asking Mrs B to pay further fees and she eventually ran out of money to send, the fraudster stopped communicating with Mrs B. At this point she realised she'd fallen victim to a scam. Mrs B contacted Revolut to raise a scam claim.

Revolut considered Mrs B's claim but said it hadn't been provided with enough information to investigate fully, despite having requested this further information. Mrs B remained unhappy and referred her complaint to our service.

An investigator considered Mrs B's complaint but didn't uphold it. He thought that Revolut ought to have intervened more than it did for payments Mrs B made to cryptocurrency providers - but thought that even if it had done, Mrs B would've still proceeded with the payments. This

was based on Mrs B having received a number of warnings from her other bank account providers and (on the fraudster's instruction) not being truthful with these providers regarding the nature of the payments.

Mrs B disagreed with the investigator's view. She said the value of payments leaving her account within the space of a week ought to have resulted in further investigation, and more effective intervention ought to have taken place.

As Mrs B disagreed with the investigator's view, the complaint has been passed to me for a final decision.

### **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.

Having done so, while I'm sorry to disappoint Mrs B, I'm not upholding her complaint. I appreciate this is a significant amount of money that Mrs B has lost – and I haven't reached my decision lightly with these losses in mind, but I've explained my reasons for reaching this outcome below.

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 January 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);
- 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.

It isn't in dispute that Mrs B has fallen victim to a cruel scam here, nor that she authorised the disputed payments she made from her account, but I've thought about whether Revolut should have reasonably intervened further, prior to processing the payments.

Mrs B's Revolut account was opened for the purposes of this scam, so Revolut had no previous account history to consider when assessing whether these payments were out of character or not. But regardless of this, I think there were certainly notable indicators that Mrs B was at risk of financial harm from fraud here. The day after Mrs B opened her Revolut account, she began making payments to a number of different cryptocurrency providers,

each payment for a significant amount and totalling around £14,000 in just the first day of account use.

When Mrs B made her first payment transfer, she was asked for the payment purpose and selected 'investment'. On this basis, she was provided with some general warnings about scams of this nature. She also received a warning related to buying 'goods and services' for a later payment that was made, then cancelled, towards the scam. However, other than these, Mrs B received no warnings from Revolut on any other payments.

I'm satisfied that Revolut ought to have recognised that Mrs B's pattern of payments carried a higher risk of financial harm from fraud. As the majority of payments were made via card, Revolut would have been able to identify that payments were going to cryptocurrency providers (which contradicted the reasons Mrs B provided to Revolut for wishing to open an account) and payments of this nature are known to carry an elevated risk of fraud. Mrs B then made a number of high value payments for further subsequent days.

I think that a proportionate response to that risk, as repeated high value payments were being made, would have been human intervention to further question Mrs B on her reason for making payments – while Mrs B had said her first payment was being made towards an investment, this itself is a common scam linked to cryptocurrency and something that I think Revolut ought to have been questioning further, based on the volume of payments. But had it done so, I'm not persuaded that would have prevented Mrs B's losses. I'll explain why.

As mentioned previously, Mrs B made payments towards the scam from several account providers. Some of these intervened to greater extents than Revolut did. And throughout questioning, Mrs B wasn't honest with the reasons for payments. To one provider, Mrs B explained in detail how she had been trading cryptocurrency for around six months, but using her husband's account, and had now decided to set up her own account for ease. She was asked questions relevant to job scams within the call, but confirmed she had not seen advertisements for job opportunities and had invested before, outside of cryptocurrency. Mrs B was read a scam script that covered job scams in some detail, and was also sent the same information by message, which she had to respond to, confirming she understood. The warning explained that fraudsters may ask you to complete tasks - and ask you to send money in order to receive wages – exactly as Mrs B was doing.

Another banking provider also called Mrs B questioning payments she made. Again, she advised she was 'dabbling' in cryptocurrency and that she was only investing money she was willing to lose, but so far, was doing well.

From reviewing the instant messaging conversation Mrs B has provided between her and the fraudster, I can also see that the fraudster was advising Mrs B on what to say (and not say) to her banking providers, including not letting her bank know about the platform she was working on. Additionally, it seems apparent that Mrs B was resolute in her decision to do whatever it took to complete the tasks set on the scam platform. During her conversations with the fraudster she says *'there is no way I am leaving...over £150k of my own money in there – that just [isn't] going to happen. ... The only way I am not getting my money back is when I send all the money that is needed to the platform and then I find out this is a scam and they keep all my money.'* Mrs B also continues trying to speak to the fraudster, even when the fraudster has largely cut off contact. Four months after the fraudster's last contact, Mrs B still messages her to advise that when she receives her house proceeds, she'll return the funds the fraudster 'lent' her towards completing tasks. I think this demonstrates how entrenched in the scam Mrs B was, further supporting the idea that even significant intervention wouldn't have broken the spell she was unfortunately under.

Therefore, having considered all evidence holistically, while I agree Revolut should've intervened further by calling Mrs B during the period of the scam, based on how Mrs B responded to calls and intervention attempts from other account providers, there's no evidence that Mrs B wouldn't have maintained the same story that she was investing in cryptocurrency. As Mrs B was making payments to genuine cryptocurrency platforms, I can't conclude that Revolut ought to have denied her request to process her payments on this basis.

I've also considered whether Revolut did enough to attempt to recover Mrs B's funds, once it was made aware of the scam. However, payments Mrs B made went to her own cryptocurrency accounts, before being passed on from there to the fraudster and therefore unfortunately, there is little Revolut can do to recover these funds.

For the reasons I've explained above, while I'm genuinely sorry to hear of the impact this scam has had on Mrs B, I can't conclude that Revolut is liable for her losses and it therefore follows that I can't direct Revolut to refund any losses incurred from her account.

### **My final decision**

My final decision is that I don't uphold Mrs B's complaint against Revolut Ltd.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs B to accept or reject my decision before 15 October 2024.

Kirsty Upton  
**Ombudsman**