

## The complaint

Mr R is unhappy that Revolut Ltd (“Revolut”) won’t refund the money he lost to a third-party scam.

Mr R is represented by a firm of solicitors.

## What happened

In April 2023 Mr R was contacted by someone on a social media messaging service about a remote job opportunity. The job was for a product optimisation role and involved completing a set number of tasks each day on an online platform, and in return Mr R was told he would receive commission paid in cryptocurrency which appeared on the job platform.

As Mr R began completing the tasks, he could see his commission building up. However, Mr R began receiving ‘lucky bonuses’ which caused his account on the fake job platform to fall into a negative balance. Mr R was required to pay funds into his job account to bring it back to a positive balance. The scammer advised that if he did this, he would have the opportunity to multiply his commission.

When Mr R could no longer repay the negative balance, he couldn’t continue and was unable to withdraw his earnings. In August 2023, Mr R received a message saying if he paid fees he could withdraw his money. However, after a further three payments the scammer cut contact and Mr R then realised, he’d been the victim of a scam.

Mr R made the following payments to genuine cryptocurrency merchant(s). From there he moved the cryptocurrency to the scammer.

Payment	Date	Transaction type	Amount
1	9 April 2023	Debit card to cryptocurrency B	£85
2	11 April 2023	Debit card to cryptocurrency B	£168.23
3	12 April 2023	Debit card to cryptocurrency B	£279.42
4	13 April 2023	Debit card to cryptocurrency B	£1,732.71
5	13 April 2023	Debit card to cryptocurrency B	£238.18
6	13 April 2023	Debit card to cryptocurrency B	£2,085.93
7	13 April 2023	Debit card to cryptocurrency B	£2,085.93
8	26 May 2023	Debit card to cryptocurrency B	£676.73
9	19 August 2023	Debit card to cryptocurrency B	£923.06
10	20 August 2023	Debit card to cryptocurrency B	£866.44
11	20 August 2023	Debit card to cryptocurrency B2	£262

The investigator who considered this complaint didn’t recommend that it be upheld. She said that Revolut should have recognised that by the seventh payment the activity was unusual and provided a written warning tailored to cryptocurrency investment scams. But the investigator wasn’t persuaded that doing so would have broken the spell and made a difference in this case, because Mr R wasn’t investing.

In terms of recovery, the investigator noted that there was no prospect of success as Mr R received a service from the cryptocurrency provider his funds went to – so Revolut acted reasonably in not raising a claim.

Mr R's representative did not agree. It said intervention ought to have been greater by the seventh payment as a pattern had emerged. Had Revolut asked probing questions Mr R would have been honest and the scam uncovered.

As the case could not be resolved informally, it's been passed to me for a 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.

In deciding what's fair and reasonable, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

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 April 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.

And for payments after 31 July 2023:

- have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so.

### **Should Revolut have recognised that Mr R was at risk of financial harm from fraud?**

It isn't in dispute that Mr R has fallen victim to a cruel scam, nor that he authorised the payments he made by card to his cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer).

Mr R opened his Revolut account on 19 March 2023 so there wasn't any activity to compare the transactions to. He had also included buying cryptocurrency, amongst other reasons, for opening the account.

The initial payments were relatively low in value and spread out and a pattern of transactions consistent with a common scam type hadn't been established. In the circumstances, I consider Revolut acted reasonably in processing these transactions without taking any additional steps. There's a balance to be struck between Revolut identifying concerning payments and responding appropriately to any concerns, and minimising disruption to legitimate payment journeys.

I agree the activity on 13 April 2023 started to create a concerning pattern and I think Revolut ought to have identified certainly by payment seven (perhaps even by payment six) that a series of increasing payments were being made to a known cryptocurrency provider.

Taking these factors into account, as well as what Revolut knew about the destination of the payment, I think Revolut should have considered that Mr R could be at elevated risk of financial harm from fraud. In line with good industry practice, Revolut should have provided a warning before the payment went ahead.

*What did Revolut do to warn Mr R?*

Revolut hasn't suggested that it took any steps to warn Mr R of the risk associated with the payment.

*What kind of warning should Revolut have provided?*

In this case, Revolut knew that the payments were being made to a cryptocurrency provider and its systems ought to have factored that information into the warning it gave.

Having thought carefully about the risk payment presented, I think a proportionate response to that risk would have been for Revolut to have provided a written warning tailored to cryptocurrency investment scams, which was the most prevalent cryptocurrency related scam at the time. Such a warning should set out the key features of a cryptocurrency investment scam.

I'm not satisfied that Revolut needed to go further at this stage or even by the following payment given the nature of the payments. I don't consider Revolut ought reasonably to have asked questions to narrow down the scam Mr R might be falling victim to. So, whilst I agree that Revolut should keep up to date with fraud trends, I don't think that in April 2023 this meant doing more than providing a written cryptocurrency investment warning.

*If Revolut had provided a warning of the type described, would that have prevented the losses Mr R suffered?*

Like the investigator, I'm not satisfied that a written cryptocurrency investment scam would have resonated with Mr R or led him to act differently as he wasn't investing - he was making payments in respect of a job. I note that Mr R's representative accepts a warning of this nature wouldn't have stopped Mr R from making the payment.

Mr R'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 R'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 R 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 R's loss in this case, for the reasons already explained.

There were additional expectations on businesses (set out at the start of this decision) by the time Mr R made the final three payments in August 2023. But given the gap since the previous payments and relatively low sums involved, I don't consider these transactions warranted any further intervention.

For the reasons explained by the investigator, I also don't think Revolut should have done more to recover Mr R's funds. His payments were to a cryptocurrency provider which provided the expected service, so a chargeback had no reasonable prospect of success. Mr R was also out of time.

### **My final decision**

My final decision is that I do not uphold this complaint.

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

Kathryn Milne  
**Ombudsman**