

## The complaint

Mr D complains that Revolut Ltd won't refund him money he lost in an investment scam.

Mr D is represented by a professional representative, but for ease of reading I'll just refer to Mr D.

## What happened

The background to this complaint is well-known to both parties, so I'll summarise what I consider to be the key points.

Mr D says he received a phone call in October 2022 from a person claiming they could help him to make money in cryptocurrency investment. He says he asked questions and was satisfied with the responses he received so he decided to invest. He downloaded remote access software, as suggested by the scammer, which he says the scammer used to transfer money from Mr D's account with a cryptocurrency trading platform to the scammer's "investment" account. He says he was able to log in to a fake investment account provided by the scammer and he could see the profits his money was earning.

Mr D made the following payments from his Revolut account, to his cryptocurrency account and from there on to the scammer:

Date	Amount	Destination	Payment type
18/10/2022	£3,000.00	Own cryptocurrency account	Card payment
20/10/2022	£600.00	Own cryptocurrency account	Card payment
17/03/2023	£125.00	Own cryptocurrency account	Transfer
17/03/2023	£103.25	Own cryptocurrency account	Card payment
16/04/2023	£100.00	Payee 1	Transfer
01/05/2023	£125.00	Own cryptocurrency account	Card payment
01/05/2023	£100.00	Payee 2	Transfer
21/07/2023	£460.00	Own cryptocurrency account	Card payment

He realised this was a scam in March 2023, when he tried to withdraw money from his account with the scammers but was unable to and the scammers stopped responding to his messages.

Mr D says Revolut didn't intervene in any of the transactions, nor did it provide any warnings. He says it ought to have intervened from the first transaction, as this was out of character. He says if Revolut had intervened suitably, it would have uncovered the scam.

Revolut says warnings were provided on some of the transactions. This consisted of it sending a message to Mr D that said:

"Do you know and trust this payee?

If you're unsure, don't pay them, as we may not be able to help you get your money back. Remember, fraudsters can impersonate others, and we will never ask you to make a payment."

In general, Revolut considers Mr D authorised the payments but hadn't exercised due diligence before making them.

Our investigator didn't consider the transactions were sufficiently unusual or out of character to have required any intervention from Revolut. He didn't consider there was any reasonable prospect of Revolut being able to make a recovery of Mr D's money and he didn't think any attempted chargebacks would have succeeded.

Mr D didn't agree with the investigator's findings and so his complaint has been passed to me for an ombudsman's 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 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 that between October 2022 and July 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 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 multistage 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.

However, having considered everything, I'm not persuaded that Mr D's complaint should be upheld, as I shall go on to explain.

Mr D's Revolut account had been open for about four months at the time of the first transaction and the account opening purpose had been given as "transfers". Mr D had made some low value payments previously, some of which appear to have been for cryptocurrency purchase.

The transaction on 18 October 2022 was for a larger amount than any of the other transactions on the account in the previous months, but not so large that I consider it ought to have caused Revolut to intervene. I've borne in mind that Revolut has a duty to execute transactions without undue delay and a balance has to be struck. While I appreciate Mr D

considers the payment was large, e-money accounts and EMIs are generally used differently to high street banks and it is not unusual for transactions of this size to be made.

Mr D had also previously used the account to transfer money to cryptocurrency accounts, so the payment destination wouldn't have appeared particularly out of character either. Nor was there an obvious pattern to the transactions that might have matched known fraud risks.

On balance, I don't consider there were sufficient unusual or concerning features about this transaction for me to conclude that Revolut ought to have intervened at that point.

The transactions from 22 October 2022 to 21 July 2023 took place over an extended period of time and all involved payments that were relatively low in value, ranging from £100 - £600. There were occasions where two small payments were made on the same day, but in general, given the low value of payments and the period of time over which they were made, I don't consider they ought to have caused Revolut any particular concern or should have led to any particular intervention. I don't consider it would have appeared that these transactions matched usual, known patterns of fraud.

Revolut says some of these payments *did* trigger warnings, for example the transaction on 17 March 2023. The warnings sent to Mr D all appear to have been general, new payee warnings, the content of which I set out above. As I'm not persuaded any of the transactions were sufficiently unusual or concerning to have warranted intervention from Revolut, I think the steps it did take, such as the new payee warnings, were sufficient.

#### Recovery

Most of the transactions were card payments and would have been considered completed once funds were credited to Mr D's cryptocurrency accounts. I don't consider there would have been valid grounds for chargebacks in those circumstances, where an authorised payment had been made from the customer's account and it had successfully credited another account controlled by the customer.

Neither do I consider it likely that the money sent by bank transfer on 16 April and 1 May 2023 could have been recovered. In my experience, money is often moved quickly in scams such as this, but in this instance, a lot of time had elapsed between the payments taking place and Revolut being notified of the fraud some months later.

Overall, while I'm sorry Mr D has been the victim of a cruel scam, for the reasons given above, I'm not persuaded that Revolut was at fault here.

# My final decision

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 11 June 2025.

Greg Barham Ombudsman