

The complaint

Mr R complains that Revolut Ltd (Revolut) won't refund the money he lost when he fell victim to a scam.

What happened

When Mr R initially complained to Revolut (via a representative), he said he watched a segment on television about someone who had made money through cryptocurrency investing. He then found an article online, which appeared to be from a well-known newspaper, about the investment company (N) – and got in touch. The people he spoke to befriended him and gained his trust, so he decided to invest with N.

N prompted Mr R to set up the Revolut account, seemingly for the purpose of sending money on to the investment platform. The account was being topped up from elsewhere. Funds were then sent to another account in Mr R's name with an authorised Electronic Money Institution (EMI). But most were sent to cryptocurrency exchanges (and a substantial credit was also received from such an exchange). We've been told all these payments – in the region of £100,000, accounting for the credit – were lost to the scam.

According to Mr R's initial complaint, it was N who made the transactions – with his consent – using remote access software. Unfortunately, it seems N were operating a scam and weren't actually investing Mr R's funds.

The disputed transactions took place in 2021. Mr R complained to Revolut about the scam in 2023. It asked him for more information about what had happened. When it didn't receive this, it declined his complaint. Mr R then referred the matter to our service.

Since then, Mr R's representative has told us the device Mr R was using was sent to him by fraudsters. They claimed be a phone company, and said the device was being sent as part of an upgrade. Through this guise, they directed him to download remote access software. It says it's unclear how this later turned into an investment scam – but Mr R wasn't aware that payments were being taken from the Revolut account.

Our investigator didn't uphold the complaint. In summary, they thought Mr R was likely involved with the payments and knew they were being taken. They did think Revolut should have questioned Mr R more about the payments, due to the account activity looking suspicious. But they weren't persuaded that would have succeeded in uncovering the scam – noting in particular that it appeared the scammers had access to the chat function on Mr R's account, and was using this to speak to Revolut – posing as him.

Mr R has appealed the investigator's outcome. In summary, he says it was Revolut's choice to intervene by chat. And that was ineffective and bad industry practice, given that Revolut says it can't detect whether the chat was being accessed remotely. He has also highlighted the vulnerable circumstances he was in, which he says would have been obvious to Revolut if it had spoken to him.

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, I've decided not to uphold it. I'll explain why.

I've first considered whether the payments were authorised. That is significant as, under the relevant regulations – the Payment Services Regulations 2017 (PSRs) – the starting position is that Mr R is liable for payments he authorises. Whereas Revolut is generally liable for unauthorised payments.

I appreciate Mr R's representative has now said the scammers made these payments without his consent. But it's difficult to reconcile this with what they originally told us; the nature of the scam; and what we know about Revolut's payment processes

To expand on this – while I appreciate Mr R's representatives may have gained further insight into the scam, they initially told us he consented to the scammers accessing his account and making the payments. I'm not satisfied we've received an adequate explanation for why they now allege he didn't in fact agree to this. Especially as the nature of the scam (as reported to us) is that Mr R thought he was investing. So that would require him to be sending funds on to N's platform.

Furthermore, based on what we know about the device and operating system Mr R was sent, and which we know was used to make the payments, it doesn't appear remote access would have allowed the scammers complete access to, and control over, the account. It appears Mr R would need to complete some of the payment steps. Overall, I consider it more likely Mr R knew he was taking action to make payments – or at least knew he was taking action to allow the scammers to make them on his behalf. Under the PSRs, that means the payments are considered authorised.

Revolut is expected to execute Mr R's authorised payment instructions without undue delay. However, that isn't an unfettered duty. There are circumstances when it might be appropriate for Revolut to identify a fraud risk and to therefore take additional steps before processing a payment. That might occur when a payment appears significantly uncharacteristic compared to the normal use of the account.

We've been told this account was opened as part of the scam. So Revolut didn't have knowledge of how Mr R normally transacted, to know whether the payments were uncharacteristic. However, I do think Revolut had cause for concern based on the general account activity – as a lot of high-value payments were sent.

There were occasions when Revolut detected risks and took action – such as declining some payments and displaying in-app warnings. At one point, it placed restrictions on the account until it had discussed the account activity with (who it thought was) Mr R. It also requested statements for the account being used to fund the Revolut transactions, records of the cryptocurrency account the funds were sent on to, and Mr R's payslips.

Looking over these records, I'm not persuaded Revolut did enough. I think it should have questioned Mr R more about the circumstances in which he had come to make these payments, in order to properly assess whether he was falling victim to a scam and warn him appropriately about the risks. However, I'm not persuaded that further, proportionate intervention by Revolut was likely to uncover the scam and prevented his loss.

That's because of the level of access and control the scammers seem to have had. From what we've been told, it appears they were able to access Revolut's chat function to respond to its requests for further information and its queries about the account activity. So, even if Revolut had probed further, or issued a more tailored warning about the common features of cryptocurrency scams – it's likely this would have been seen and responded to by the scammers than Mr R. So I don't think this would have deterred Mr R, and it's unlikely the scammers would have responded in a way that made it obvious he was being scammed.

I do appreciate what Mr R has said (via his representative) about why he doesn't think this form of intervention was sufficient, given Revolut seemingly can't detect whether remote access is being used to respond on the chat. But I can't see it had cause to suspect that was happening here. Getting access to the chat would still require knowledge of/access to Mr R's Revolut account. And Revolut's records suggest only one device was being used to access the account. Furthermore, it also appears some of the information it was requesting and receiving was being done over email. So I can't see why Revolut had cause to doubt that it was Mr R responding.

For the scam to have worked in the way that has been reported to us, it appears the scammers had a very significant amount of control over Mr R – beyond what we commonly see when remote access is involved. It appears they had access to his payslips, emails – and to multiple other accounts in his name. We know the scam continued to run for at least a few months after these payments – as we have looked into a separate case about payments made from a different account Mr R was subsequently convinced to set up.

I appreciate this was all part of the scam. But it does give me significant doubt over whether Revolut would realistically have been able to reach Mr R away from the scammers' influence, uncover what was really happening, and dissuade him from proceeding.

I've thought about the points raised around Mr R's vulnerability. I do appreciate this likely contributed to the way in which the scam unfolded. But I can't see Revolut had been informed of anything which meant it ought to have known Mr R might need a different level of support. Nor can I see it had cause to realise this based on the communication it received, seemingly from Mr R, in relation to the account.

I also agree with the investigator that Revolut didn't miss an opportunity to recover Mr R's loss. It wasn't notified of the scam until 2023, by which point it appears the funds had been moved on from the accounts they were sent to.

I appreciate this will be disappointing for Mr R. I don't doubt he has been taken advantage of, in vulnerable circumstances, by the scammers. But having carefully considered all the circumstances, I don't consider it fair to hold Revolut liable for the loss he incurred.

My final decision

For the reasons given above, 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 10 January 2024.

Rachel Loughlin
Ombudsman