

The complaint

Mr B is unhappy Revolut Ltd (“Revolut”) won’t reimburse him for the money he lost when he fell victim to a scam.

What happened

The details and facts of this case are well-known to both parties, so I don’t need to repeat them at length here.

In short, Mr B says he saw an advert for a trading company on social media that I will call “B”. Mr B completed an enquiry form and was contacted by a representative of B.

Subsequently, the following payments were made to a cryptocurrency exchange. My understanding is that the funds were then converted to cryptocurrency and were then transferred on to B.

The following transactions went from Revolut to the cryptocurrency exchange.

Transaction Number	Date	Amount	Type of payment
1	3 March 2023	£1,035	Card Payment
2	22 March 2023	£2,000	Card Payment
3	5 April 2023	£4,184.25	Card Payment
4	8 April 2023	£7,840	Card Payment
5	11 April 2023	£7,840	Card Payment
6	14 April 2023	£5,920	Card Payment
7	14 April 2023	£3,000	Card Payment
8	15 April 2023	£4,990	Card Payment

Mr B realised that he had been scammed when he was repeatedly asked to send further funds but, after sending the funds, he remained unable to withdraw his “profits”.

He made a complaint via a representative to Revolut and requested that the above transactions be refunded. It declined to do this.

I issued a provisional decision on 12 November 2024 in which I said the following;

“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 in March 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 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.*

In this instance, the first two transactions were not, in isolation, large enough to be deemed unusual for Mr B. And the pattern of spending was not sufficiently indicative of a scam, to be considered unusual or sufficiently out of character to have prompted an intervention from Revolut. The transactions were spaced out and the account had also not really been used before, so Revolut did not have a transaction history to compare the scam payments to, to understand whether the payments were unusual for Mr B.

I note that this was a new account and Revolut did not have a payment history to compare the payments to. But payment 3 was clearly to a cryptocurrency exchange and was large enough in my view to have prompted an intervention from Revolut. Given this I think that Revolut should have really been aware that Mr B was at a heightened risk of financial harm.

My understanding is that Revolut did not provide Mr B with a warning for payment 3 or indeed the other payments he made.

I’ve thought carefully about what a proportionate warning in light of the risks presented would be in these circumstances. In doing so, I’ve taken into account that many payments that look very similar to this one will be entirely genuine. 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.

Taking that into account, when Mr B attempted the third payment, I think Revolut ought, knowing (or strongly suspecting) that the payment was going to a cryptocurrency provider, to have provided a warning (whether automated or in some other form) that was specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022. In doing so, I recognise that it would be difficult for such a warning to cover off every permutation and variation of cryptocurrency scam, without significantly losing impact.

So, at this point in time, I think that such a warning should have addressed the key risks and features of the most common cryptocurrency scams – cryptocurrency investment scams.

The warning Revolut ought fairly and reasonably to have provided should have highlighted, in clear and understandable terms, the key features of common cryptocurrency investment scams, for example referring to: an advertisement on social media; an ‘account manager’, ‘broker’ or ‘trader’ acting on their behalf; the use of remote access software and a small initial deposit which quickly increases in value.

I’ve thought carefully about whether a specific warning covering off the key features of cryptocurrency investment scams would have likely prevented any further loss in this case. And on the balance of probabilities, I don’t think it would have.

I say this because Mr B has confirmed on a number of his submissions that it was the scammer making the payments using remote access. This has led me to conclude that Mr B would not have seen any warning that was provided, and I don’t think the scammer would have heeded any warning either.

In addition, had further interventions happened later in the scam when larger payments were made, I don’t think the scam would have been stopped. I say this because either the scammer would have given misleading information if questions had been asked on an online chat or further warnings would have been ignored by the scammer.

So overall I think that Revolut should have intervened and provided a warning. But I don’t think that this would have stopped the scam. It follows then that I currently don’t think that Revolut should refund any of these transactions.

I note Mr B’s representatives’ comments that Revolut has confirmed that remote access software cannot be used when making payments. I have carefully considered this and my understanding is that this is when using the app on a mobile device. Whereas when using a computer, it is possible to use remote access. I am also mindful that Mr B has confirmed that when the payments were made, he was told to not touch his computer for 30 minutes and in a different submission that he had no idea where the payments were going or what the process was. He has further confirmed that he did not have the technical knowledge to do the transactions himself. I have no reason to doubt Mr B’s testimony. So overall it’s clear that the scammer made the payments after Mr B had given them remote access to his computer.

And so, even if Revolut had issued warnings, I think the scammer (rather than Mr B – given that he was told not to access his computer for 30 minutes) would’ve seen such warnings and would no doubt have continued making payments from Mr B’s account for as long as they could get away with it. So I don’t think any intervention would have stopped the scam.

I have considered whether the payments in question could have been recovered by other means. But given the timescales involved, the method of the payments and that Revolut is not a signatory of the Contingent Reimbursement Model, I don’t think that the funds could be recovered.

So overall whilst I have a lot of sympathy for Mr B, as he is clearly the victim of a cruel scam, I cannot currently uphold this complaint.”

Revolut did not add any additional points in response to my provisional decision. Mr B’s representative responded with some additional points these included in summary;

- That its understanding was the remote access could not be used on a mobile device and that setting up new payees and acknowledging authorised push payment (APP) warnings could not be done via Revolut's website and has to be done via the mobile application.
- The consumer duty is clear that firms have to have processes in place to essentially stop scammers impersonating account holders.
- The payments were out of character enough to have prompted a call with Mr B.

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.

I note Mr B's representatives' comments in relation to the limitations of what can be done on a Revolut account when remote access is being used. But even if Mr B had to enter new payee or indeed acknowledge APP warnings, I think that Mr B was so far under the spell of the consumer that he would have followed the scammers instructions regardless.

This is demonstrated by him trusting the scammer so much he gave over complete control of his computer and was willing to not touch anything for 30 minutes whilst the scammer moved his funds around. I think it likely that if during that process Mr B had needed to acknowledge something through the app he likely would have done so and if he had questioned it, the scammer who was persuasive enough to have received full access to Mr B's accounts would have explained away any warning.

In relation to the consumer duty comments given when this scam occurred this was not in place.

Finally, I note Mr B's representatives' comments that it believes that Revolut should have spoken to Mr B but there is no obligation or requirement as to how firms carry out a human intervention. In this instance I believe an in app chat would have been sufficient and for the reasons I have stated I don't think that this would have stopped the scam. As either the scammer would have answered the questions or would have persuaded Mr B to answer them in a way designed to allay the suspicions of Revolut.

It therefore follows then that I do not uphold this complaint as I don't think that Revolut could have uncovered or prevented the scam.

My final decision

Because of the reasons given above and in my provisional decision, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 6 January 2025.

Charlie Newton
Ombudsman