

## **The complaint**

Mr A complains Revolut Ltd hasn't refunded money he lost to a cryptocurrency investment scam.

## **What happened**

Mr A connected with the scammer on a dating website in May 2023 and from June 2023 they then began speaking on Whatsapp. A little while into the relationship, the scammer introduced Mr A to a scam trading platform where he believed he would be trading in cryptocurrency. Mr A sent three payments successfully from his Revolut account in July 2023 to buy cryptocurrency, which he then sent to the scam.

Mr A, via a representative, complained to Revolut about these payments. They said that the second payment Mr A made for £3,069 should've been concerning to Revolut and prompted an intervention. And that it could've then unravelled the scam. Revolut didn't agree and didn't uphold Mr A's complaint. It also said the first payment hadn't been successful and so had already been returned.

Mr A then brought his complaint to our service. Our investigator didn't uphold the complaint. They set out that Revolut ought to have done more to protect Mr A when this payment was made, but said that proportionate action it wouldn't have prevented the scam. Mr A disagreed and asked 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.

In broad terms, the starting position in 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 July 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

- 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.

Revolut has shared with us the warnings it presented to Mr A, but I don't consider these were tailored or clear enough on the financial risks or scams Mr A could be falling victim to. This is particularly because he did select he was buying cryptocurrency as the reason for the first payment. However, while I think Revolut ought to have recognised that Mr A was at heightened risk of financial harm from fraud, I don't think any proportionate intervention by Revolut would have prevented Mr A's loss. I'll explain why.

Mr A had been introduced to this investment opportunity through someone he believed he was in a romantic relationship with. They'd been speaking for a while and it's clear from the messages they shared that he trusted the scammer and followed her directions explicitly in regard to making the cryptocurrency purchases. Even when he first reported the scam to Revolut, he still referred to her as his girlfriend.

Mr A had some initial problems with buying cryptocurrency, and he told the scammer about this, sending screenshots of his account. She then advised him on how else to complete the transaction and provided annotated screenshots of where/what to click. And when he received a pop-up warning on the cryptocurrency exchange, we can see he immediately shared that with her. She used this as an opportunity to tell him that exchanges and banks don't like people taking their money out. Another screenshot Mr A shares says his payment has been flagged as a potential scam and the scammer reiterates about banks not wanting people to move their money. I'm confident she would've referred back to this had Mr A shared tailored warnings from Revolut about his payments.

Considering the relationship they had, I don't think a tailored cryptocurrency warning from Revolut would've unravelled this scam. While the warning would've focussed on the common features of cryptocurrency scams, I'm not persuaded Mr A would've recognised that he could be or was in this situation. He wouldn't consider, for example, he'd been contacted by a broker or was being coached by someone; and he wasn't using screen sharing software or giving anyone access to his accounts. He met the scammer on a dating website, and he was now in a relationship with someone who he believed – and in his mind, had evidenced to him – they were making money from this kind of investing.

Also, as already set out above, I think Mr A would've likely shared any concerns he had with the scammer and she'd have reassured and coached him with the next steps. I note that Mr A used a different purpose for each of the payments and didn't select cryptocurrency again after he sent the first payment. It's not clear why he did this and the chat we have doesn't cover this either. But considering he was doing exactly the same thing each time, it seems strange he chose to select different payment purposes – possibly indicating some coaching did in fact take place. And again, I don't consider that tailored warnings shown would've resonated with Mr A or stopped him going ahead.

I accept Mr A has been the victim of a cruel scam, but I don't think Revolut can be held responsible for his losses here. Considering the amounts involved, I think a proportionate intervention would've been a tailored cryptocurrency warning on the first payment, but that this wouldn't have prevented the scam in this case. And tailored warnings after this, based on what Mr A said he was doing, also wouldn't have prevented his losses.

**My final decision**

For the reasons set out above, I don't uphold Mr A's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr A to accept or reject my decision before 4 September 2024.

Amy Osborne  
**Ombudsman**