

## **The complaint**

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

Mr R is being represented by solicitors in this complaint.

## **What happened**

The detailed background to this complaint is well-known to the parties and has been previously set out by our investigator.

Briefly, Mr R fell victim to a cryptocurrency investment scam in late 2022. Between November 2022 and February 2023, he made five transactions totalling just over £15,000 to a popular cryptocurrency provider using his Revolut debit card. These were made in connection with an opportunity provided by a company "M, who he came across on social media. Mr R states that M appeared to be endorsed by a well-known broadcaster.

Mr R initially used his account with a high street bank "B" to make deposits. Later, under the scammer's instructions, he opened an e-money account with Revolut. He transferred funds into his Revolut account from his bank account with B, before purchasing cryptocurrency from a cryptocurrency exchange. The converted cryptocurrency was then sent on to cryptocurrency wallets as instructed by the scammer. At the time Mr R thought he was loading it on to his account with the investment platform, given the balance went up accordingly.

Encouraged by the profits seemingly being made, Mr R agreed to 'upgrade' his investment account and continued making payments. He realised he'd been scammed when he requested a withdrawal and was asked to make further a payment – commission – to the scammer. Mr R made a partial payment. He carried out further checks while waiting to be paid his wages so he could pay the remaining amount. These checks led to the scam discovery.

Revolut looked into Mr R's scam claim but refused to refund his losses. A complaint was then made and subsequently referred to our service. Our investigator concluded that Revolut should have provided a scam warning about investment scams when Mr R made the third payment (£4,000 on 19 January 2023). They were persuaded that such a warning would have stopped Mr R in his tracks and limited his losses. The investigator recommended Revolut to refund Payments 3-5 with a 50% deduction for contributory negligence.

Mr R accepted the investigator's findings, but Revolut didn't. So, the complaint was passed to me to decide.

I issued a provisional decision and gave reasons for why I intended reaching a different outcome to the investigator. I said:

*"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.*

*It isn't in dispute that Mr R authorised the transactions in question. He's therefore presumed liable for the loss in the first instance.*

*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 November 2022 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); and*
- 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.*

*EMIs are set up with the purpose of sending and receiving money and the type of payments they're generally used for tends to be somewhat different to banks and building societies. Often, the payments will be for larger sums. Where there's no previous account history, as was the case here given the account was opened two days prior to the first disputed transaction, what should reasonably strike Revolut as concerning for a first payment isn't down solely to the transaction amount involved.*

*I haven't seen any other factors at play here such that, in my view, Revolut should have been concerned and ought to have taken additional steps when Mr R authorised the first disputed transaction (£990 on 9 November 2022). Or, for that matter the second transaction (£1,990 on 14 November 2022). I accept that Mr R was sending money to a cryptocurrency exchange. But that in and of itself doesn't mean that the transaction ought to have flagged as suspicious. Buying cryptocurrency is a legitimate exercise.*

*But by the time Mr R authorised the third transaction (£4,000 on 19 January 2023), Revolut ought to have recognised that it carried a heightened risk of financial harm from fraud. This is because a pattern of increased activity on cryptocurrency spending had emerged. And there was a significant jump in the amount involved. I consider Revolut should have taken additional steps when it received Mr R's instruction.*

*The investigator's view was that Revolut should have asked Mr R to select the purpose of the payment from a list of options in order to provide a tailored scam warning. Given when this transaction happened, I don't consider Revolut needed to ask for the payment purpose before providing a written warning specific to the risk identified based on Mr R's selection. That said, the transaction was identifiably cryptocurrency related. So, a proportionate response to that risk would still have been for Revolut to have provided a written warning about the most prevalent type of cryptocurrency scams, i.e., investment scams, tackling some of the key features.*

*The investigator concluded that a written warning about cryptocurrency scams would have likely impacted Mr R's decision-making and prevented his losses from that point on, given there's nothing to suggest that he wouldn't have responded to such a warning. But this is where my findings differ to the investigator's. I'll explain why.*

*A transfer of £1,000 which Mr R attempted to make from B to Revolut on 8 November 2022 flagged as suspicious and was blocked by the bank. Mr R had to phone B to discuss it. I've seen B's system notes from this time. And I've also listened to a recording of the call that took place. Mr R can be heard telling the agent that he's transferring funds to a new account he's opened for budgeting and some cryptocurrency transactions. When the agent picks up the reference to cryptocurrency, Mr R backtracks and says the funds he's attempting to transfer are going to stay in his Revolut account.*

*The agent asks Mr R if he's installed remote access software on his device. Mr R initially says he isn't sure, but when the agent tells him that B's system has identified it on his device Mr R says a friend who he's known for 20 years has on some occasions controlled his device to help with security. A discussion about the risks involved with remote access ensues.*

*The agent then brings up the cryptocurrency transactions attempted from Mr R's account with B. He explains he's been having issues setting up the new account, and funds transferred keep getting returned. Mr R explains he's 'trying to get something going'. When asked, he tells the agent that while he's tried forex and binary (options) before, he's relatively new to cryptocurrency. The agent warns Mr R that cryptocurrency is one of the biggest scams B is seeing. And it starts with customers being asked to open intermediary accounts with firms like Revolut which don't offer high street branches.*

*The agent tells Mr R that scammers make promises of doubling money, to which he replies that this opportunity caught his eye and he thought he'd stick £1,000 into it – 'if it's gone its gone'. The agent asks Mr R whether he's researched into cryptocurrency and Mr R says 'a little'.*

*Not satisfied with Mr R's answers and noticing that a new IP address had been used recently, the agent asks Mr R that he would need to visit a branch with ID for further verification and questioning. The agent explains that some additional questions regarding the cryptocurrency opportunity would likely be asked.*

*The call ends and the flagged payment isn't released at this time. However, the next day – 9 November – Mr R successfully transferred £1,000 to his Revolut account. Within the hour, he made the first disputed payment of £990 using his Revolut debit card.*

*The written correspondence between Mr R and the scammer that has been forwarded to our service only starts around 10 January 2023. So, it's unclear if Mr R*

*discussed B's intervention with the scammer in November 2022. I don't have the specific details of the intervention by B's branch staff. But given that the second attempted transaction was executed, on balance, I think it's more likely than not that Mr R reassured B that he'd since looked into the investment opportunity further, and he was happy to go ahead with the payment.*

*This is not a finding I've made lightly. But given Mr R had already been warned about the typical features involving cryptocurrency investment scams, such as the involvement of a broker or the use of remote access software, there's likely two scenarios – either he ignored B's warning and didn't carry out any independent due diligence or he discussed the intervention with the scammer who provided reassurances.*

*Given Mr R's actions when bank B took additional steps on 8 November and warned him about cryptocurrency investment scams, I'm not persuaded that a written warning about cryptocurrency investment scams by Revolut nearly two months later would have positively impacted his decision-making like the investigator has suggested. By the suggested intervention point (19 January), Mr R had upgraded his account and had seen his initial investment making profits.*

*Therefore, in the circumstances of what happened here, I'm not convinced that Mr R would have stopped in his tracks and investigated the opportunity further had Revolut provided a written scam warning. From the available information, it seems it was the difficulties he experienced when attempting a withdrawal a month later (February) that prompted Mr R to investigate M.*

*I know that Mr R will be disappointed with this outcome. Not least because the matter has been ongoing for some time and our investigator previously upheld the complaint and recommended a partial refund. But I can only ask Revolut to reimburse Mr R if I find that any wrongdoing on its part caused his loss. I've explained above why I don't believe that to be the case.*

*I've also thought about whether Revolut could have done more to recover the funds once it became aware of the situation, as in some circumstances the money can be recovered. Here, the recovery avenue would have been limited to chargeback. But Mr R's payments went to a cryptocurrency exchange. He wouldn't be able to make a successful chargeback claim in the circumstances because the merchant he paid did provide the service requested (i.e., conversion of fiat money into cryptocurrency). For completeness, Revolut couldn't attempt a chargeback against any another party."*

I invited both parties to provide further comments and evidence for my consideration before finalising my decision.

Revolut didn't reply and the deadline date I gave has now passed. I've therefore assumed it has nothing further to add.

Mr R's representative replied and said that Mr R remains unhappy with my provisional 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.

I thank Mr R and his representative for their reply to my provisional decision which I've carefully reviewed.

The crux of the appeal is that a different firm's intervention shouldn't be used as an excuse to negate Revolut's failure; it failed to provide any effective intervention and so it shouldn't escape liability on this basis.

Mr R's representative has received several decisions from our service which set out our well-established approach to scam complaints. Therefore, the representative knows (or ought to know) that causation is a critical determinative factor in such cases. It isn't enough that a firm failed to sufficiently intervene; its acts or omissions must be the immediate and effective cause of losses that were reasonably foreseeable at the time of the breach.

What this means is that Revolut's failure to intervene at the suggested trigger point isn't enough on its own for me to uphold this complaint. I would also need to be satisfied, on balance, that but for this failure Mr R would not have gone ahead with the payment in question (and the subsequent payments). In my provisional decision, I gave reasons for why I wasn't satisfied. The appeal makes no reference to why Mr R or his representative believe that he wouldn't have gone ahead with the payments had Revolut intervened. As such, my position on causation remains unchanged.

I fully acknowledge that there's a considerable amount of money involved here. Despite my natural sympathy for the situation in which Mr R finds himself, for the reasons given, it wouldn't be fair of me to hold Revolut responsible for his loss.

### **My final decision**

For the reasons given, my final decision is that I don't 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 14 February 2025.

Gagandeep Singh  
**Ombudsman**