

The complaint

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

What happened

Mr K says that he was contacted by someone on a messaging app who claimed to be from a recruitment company. This person passed Mr K's details on to a representative of a company I'll call S in this decision. The representative of S discussed a remote job role that involved completing sets of tasks to optimise products. By working for a maximum of an hour a day, Mr K could earn a basic salary of 500USDT for completing tasks on five consecutive days and 3,000USDT for 30 days. In addition to the basic salary, Mr K could earn commission.

Mr K was told that if he received a randomly generated combination task, he would be required to clear the negative balance it created on his account. But combination tasks brought five times more profit and increased commission.

Mr K was required to buy cryptocurrency from a cryptocurrency exchange and send it to the wallet address details provided by a representative of S. He could then see his payments on S' platform. Soon after starting the role, Mr K received combination tasks and was required to make payments as set out in the table below.

| Transaction | Date | Amount |
|--------------|----------|----------------|
| 1 | 10/01/23 | £1,750 |
| 2 | 11/01/23 | £3,650 |
| 3 | 11/01/23 | £4,600 |
| 4 | 12/01/23 | £2,000 |
| 5 | 13/01/23 | £730 |
| Total | | £12,730 |

Mr K realised he was the victim of a scam when he was asked to make further payments that he could not afford. He contacted the CEO of S and was told that he had been the victim of a scam. Mr K contacted Revolut via its in app chat on 26 January 2023.

Revolut didn't agree to reimburse any of Mr K's loss. It said it wasn't at fault for processing the payments Mr K authorised, and that it had no chargeback rights.

Mr K was unhappy with Revolut's response and brought a complaint to this service. He said Revolut didn't do enough to protect him when the payments were made.

Our investigation so far

The investigator who considered this complaint didn't recommend that it be upheld. She said that Revolut should have provided a written warning tailored to cryptocurrency investment

scams when Mr K made payment two, given the increased risk associated with such payments. But, based on Mr K's calls with another bank, and his messages with the scammer, she didn't think this would have made a difference and prevented his loss.

Mr K didn't agree with the investigator's findings and asked for a final decision, so his case has been passed to me to decide. In summary, he said:

- There was no evidence in the calls with Mr K's bank that he was asked for the reason for the payments or given general scam advice. He was simply told on one occasion that if his payment related to a scam, he wouldn't be able to get his money back. And when he expressed dissatisfaction with his bank his comments related to the time taken to make the payment.
- Given that Revolut didn't intervene at all, Mr K shouldn't be held fully responsible. If Revolut had intervened Mr K would have paused and thought about what he was doing.
- Mr K's representative referred to another decision issued by this service when an ombudsman said Revolut should have intervened by asking questions and providing a warning tailored to the specific scam risk identified. He went on to say this proactive response would have resulted in the scam being uncovered.
- Revolut had the opportunity to intervene in a phone call but failed to do so.

When providing its file to this service, Revolut also said that the fraudulent activity did not take place on the Revolut platform. Instead, Mr K used Revolut as an intermediary to receive funds from Mr K's external bank account and transfer them to a legitimate cryptocurrency account in Mr K's own name.

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've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

In deciding what's fair and reasonable, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

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.

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 January 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); 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.

Should Revolut have recognised that Mr K was at risk of financial harm from fraud?

It isn't in dispute that Mr K has fallen victim to a cruel scam here, nor that he authorised the payments he made to his cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer).

The transactions Mr K has asked me to consider were card payments to an identifiable cryptocurrency exchange. I am satisfied that by the end of 2022, prior to the payments Mr K made in January 2023, Revolut ought fairly and reasonably to have recognised that its customers could be at an increased risk of fraud when using its services to purchase cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name.

In those circumstances, as a matter of what I consider to have been fair and reasonable, good practice and to comply with regulatory requirements, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments.

I don't consider Revolut ought to have been concerned when Mr K made payment one. It was relatively low in value and in line with one of the reasons Mr K had given for opening the account. Many transactions to cryptocurrency exchanges are also legitimate. There's a balance to be struck between Revolut identifying concerning payments and responding appropriately to any concerns, and minimising disruption to legitimate payment journeys.

When Mr K made payment two, I consider Revolut ought to have recognised that it carried a heightened risk and taken additional steps before processing it. This was because Mr K's account had been dormant since 2018 and then the day before he started making payments to an identifiable cryptocurrency exchange. The amounts Mr K was paying were increasing.

What did Revolut do to warn Mr K?

Revolut didn't take any steps to warn Mr K of the risks involved.

What kind of warning should Revolut have provided?

When Mr K attempted to make payment two, I think Revolut ought fairly and reasonably to have recognised there was a heightened possibility that the transaction was linked to a scam. In line with the good industry practice that I've set out above, I think a proportionate response to that risk would have been for Revolut to have provided a written warning tailored to the most common form of cryptocurrency scam - cryptocurrency investment scams.

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, promoted by a celebrity or public

figure; 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.

Mr K's representative has said that Revolut should have gone beyond this and asked questions to identify the particular scam risk Mr K was falling victim to. I don't consider this to be a proportionate response at the time the payments were made though.

If Revolut had provided a warning of the type described, would that have prevented the losses Mr K suffered?

After careful consideration, I don't consider that intervention by Revolut of the type I have described above would have made a difference in this case.

Although I have listened to the calls Mr K had with his bank, I don't consider they impact my decision making in this case. Mr K initially attempted to make cryptocurrency payments from his bank, but his bank limited the number of such transactions he could make in a day which led to Mr K being frustrated and saying he would use Revolut. His bank didn't provide any advice about cryptocurrency related scams and how to avoid them or ask him any questions. All that Mr K was told was that regular cryptocurrency payments carry a history of fraud, and that cryptocurrency is high risk. I also can't see anything in the messages Mr K exchanged with the scammer to suggest he was told to lie or mislead Revolut.

As I have said above, I consider a proportionate response to the risk posed by payment two was a warning tailored to cryptocurrency investment scams, as these were the most prevalent at the time. But Mr K wasn't investing, he was making payments connected to a job role. In the circumstances, I'm not persuaded that a warning covering the key elements of a cryptocurrency investment scam – like an advertisement on social media, celebrity endorsement, an account manager or broker, the use of remote software and a small deposit that rapidly increases in value – would have resonated with him and prevented him from continuing to make payments. None of these factors applied to what Mr K was doing.

Chargeback

Revolut said there was no valid chargeback right in respect of the payments Mr K made. I'm satisfied that Revolut acted fairly in these circumstances, as chargeback only looks at the merchant Mr K paid, which was a genuine cryptocurrency exchange, not the end destination of the funds. In this case, the exchange provided the cryptocurrency that Mr K paid for, so a chargeback wouldn't be successful.

Overall, whilst I'm very sorry to hear about this cruel scam and the impact it has had on Mr K, I can't ask Revolut to reimburse his loss.

My final decision

For the reason stated, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr K to accept or reject my decision before 19 March 2025.

Jay Hadfield
Ombudsman