

The complaint

Mr H complains that Revolut Ltd didn't do enough to protect him from the financial harm caused by an investment scam, or to help him recover the money once he'd reported the scam to it.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

In January 2023, Mr H saw an advertisement on social media for an investment company, which I'll refer to as "S". The advert claimed that S used expert traders and brokers to train beginners on the investment process.

Mr H followed a link to S's website, and noted it included an 'about us' section, FAQs, a 24/7 live chat option, and full details of the various company directors. He thought the website looked professional, and he could see there were positive reviews. Mr H was an inexperienced investor and struggled to complete any further due diligence, but he felt S was genuine, so he completed an online enquiry form.

He was then contacted by someone I'll refer to as "the scammer", who claimed to be a broker working for S. The scammer told Mr H to open an account on the trading platform, which required him to provide photo ID. She also told him to download AnyDesk remote access software to enable her to guide him through the trading process.

The scammer told Mr H to open an account with a cryptocurrency exchange I'll refer to as "K" and to first purchase cryptocurrency and then move it to an online wallet. Between 23 February 2024 and 22 March 2024, Mr H made eight transfers to the cryptocurrency exchange totalling £19,260.

He could see his profits on the trading platform, but when he asked the scammer if he could make a withdrawal, she said he'd need to deposit £9,705 for fees and taxes, which he did on 22 March 2024. He realised he'd been scammed when he didn't receive the withdrawal and was told he'd have to pay a further £20,000 to withdraw the funds.

Mr H complained to Revolut with the assistance of a representative who said it should have intervened when he made the fourth payment and had it asked questions and provided a relevant scam warning, it would have been apparent that he was falling victim to a scam, and he wouldn't have gone ahead with the payments.

But Revolut refused to refund any of the money. It said it launched a request to freeze and retrieve the funds from the fraudulent account, but it didn't receive a response. It also explained that it presented Mr H with a new beneficiary warning, and it wasn't at fault for processing the transfers.

Mr T wasn't satisfied and so he complained to this service. Responding to the complaint, Revolut maintained that its transaction monitoring controls were in line with the expected

behaviour for this type of transaction. It said the first transaction was identified as high risk and Mr H confirmed that he trusted and knew the payee.

It also said that if Mr H had done proper checks, he'd have realised that S didn't have an online presence, it had a bad trust score, and it wasn't regulated by the Financial Conduct Authority ("FCA"). He was also warned that the transactions were high risk and would also have received a warning when he downloaded AnyDesk.

It further explained that Mr H created the account on 21 February 2024, giving the account opening purpose as 'transfers', so it had no reasonable basis to believe he could be a victim of financial harm. It said Mr H was coached to open the account, and it was being used as an intermediary account to send funds to a legitimate cryptocurrency platform. So, there was no fraud on the Revolut platform.

Our investigator didn't think the complaint should be upheld. He thought Revolut should have provided a 'better automated warning' which would involve asking a series of questions to try and establish the actual scam risk. But he didn't think this would have stopped the scam because he was satisfied that Mr H would have still wanted to go ahead with the payments.

In reaching that conclusion he explained that the messages between Mr H and the scammer showed he was prepared to follow her advice, noting that on 16 March 2024, he said "I did exactly what you said, and all is sorted at the bank". He further noted that Mr H's representative had stated that he had found the scammer to be extremely professional and articulate, and that he immediately built a trusting rapport with her.

Finally, he explained that Mr H had transferred funds to a legitimate cryptocurrency exchange in his name before transferring it to a wallet address, so there would have been no prospect of a successful recovery. And he didn't think he was entitled to any compensation. Mr H has asked for his complaint to be reviewed by an Ombudsman. His representative has argued that it's unfair to assume an intervention wouldn't have been effective based on messages he wrote to the scammer, and that an effective intervention should have included questions and tailored warnings which would have prompted him to reconsider the legitimacy of the investment.

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 reached the same conclusion as our investigator. And for largely the same reasons. I'm sorry to hear that Mr H has been the victim of a cruel scam. I know he feels strongly about this complaint, and this will come as a disappointment to him, so I'll explain why.

I'm satisfied Mr H 'authorised' the payments for the purposes of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although he didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of his bank account, he is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mr H didn't intend his money to go to scammers, he did authorise the disputed payments. Revolut is expected to process payments and withdrawals that a customer authorises it to make, but where the customer has been the victim of a scam, it may sometimes be fair and reasonable for the bank to reimburse them even though they authorised the payment.

Prevention

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 February 2024 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.

I’ve thought about whether Revolut could have done more to prevent the scam from occurring altogether. Buying cryptocurrency is a legitimate activity and from the evidence I’ve seen, the payments were made to a genuine cryptocurrency exchange company. However, Revolut ought to fairly and reasonably be alert to fraud and scams and these payments were part of a wider scam, so I need to consider whether it ought to have intervened to warn Mr H when he tried to make the payments. If there are unusual or suspicious payments on an account, I’d expect Revolut to intervene with a view to protecting Mr H from financial harm due to fraud.

The payments didn’t flag as suspicious on Revolut’s systems. I’ve considered the nature of the payments in the context of whether they were suspicious, and I think they were. Revolut would have known Mr H was sending funds to a high-risk cryptocurrency merchant and so I would expect it to have intervened on 12 March 2024 when he transferred £4,850 to K. I think a proportionate response would have been to provide a ‘better automated warning’, which would include questions about the purpose of the payment, and as Mr H was sending funds to a cryptocurrency merchant, I would expect it to provide a warning tailored to cryptocurrency investment scams, regardless of the answers he gave.

I’ve thought carefully about whether an impactful warning giving details about how cryptocurrency investment scams work and how he could protect herself from the risk of fraud would have likely prevented any further loss, and, on the balance of probabilities, I don’t think it would.

I accept there were several key hallmarks of cryptocurrency investment scams present, such as finding the investment through an advert on social media, being assisted by a broker, and being asked to download remote access software. However, I’ve considered the message to

which our investigator has referred, and I agree it shows Mr H he was in close contact with the scammer and was following her instructions, which his representative has explained were given by phone. And while he wouldn't have been able to hide the fact he was buying cryptocurrency, I'm satisfied the message shows he trusted the scammer to a degree that I think Revolut would have found difficult to counter through a written warning.

Significantly, it wasn't until Mr H was repeatedly asked to make further payments to make a withdrawal that he realised he was being scammed. He found the scammer to be likeable and professional, and he was impressed with the website. And at the point at which I think Revolut should have intervened, he didn't have any concerns about what he was being asked to do. So, I think he'd likely have sought advice from the scammer who would have told him to disregard the warning, and the scam would have continued.

I've considered whether there were any further opportunities to intervene and while I accept the payment amount increased to £9705 on 22 March 2024, this was the eighth payment that Mr H had made to the same payee within a month, so K was by then an established beneficiary, and the payments weren't made in quick succession. Therefore, on balance, I don't think it would have needed to intervene again.

Recovery

I don't think there was a realistic prospect of a successful recovery because Mr H paid an account in his own name and moved the funds onwards from there.

Compensation

The main cause for the upset was the scammer who persuaded Mr H to part with his funds. I haven't found any errors or delays to Revolut's investigation, so I don't think he is entitled to any compensation.

I'm sorry to hear Mr H has lost money and the effect this has had on him. But for the reasons I've explained, I don't think Revolut is to blame for this and so I can't fairly tell it to do anything further to resolve this complaint.

My final decision

For the reasons I've outlined above, 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 H to accept or reject my decision before 30 September 2025.

Carolyn Bonnell
Ombudsman