

## **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 March 2023 Mr H saw an advert online for Company B, which was endorsed by a well-known celebrity. He clicked on the link and completed an online contact form, before receiving a call from someone I'll refer to as the scammer who introduced themselves as his account manager. They explained the company was based overseas and that he'd be investing in Bitcoin, oils, gasses, and other commodities. She explained the more he invested the more profit he'd make, he could withdraw his profit at any time, and he could begin with an investment of £250.

The scammer told Mr H to download AnyDesk remote access software to his device and to open accounts with Revolut and a cryptocurrency exchange I'll refer to as "B". He also opened an account on the trading platform. The told him to first purchase cryptocurrency and then load it onto an online wallet. Between 21 March 2023 and 24 April 2023, he made twenty payments to three cryptocurrency exchanges totalling £85,632. Nineteen of the payments were made by card, and one was a faster payment.

By the end of March, Mr H had over £100,000 in his trading account, but when he tried to make a withdrawal, the scammer told him he'd have to pay fees. He made a further fourteen payments, but he realised he'd been scammed when he didn't receive a withdrawal and he lost contact with the scammer.

Complaining to this service, Mr H said the scammer came across as caring and informative, he acted according to her exact instructions and guidance, and if Revolut had warned him about the scam risk he wouldn't have proceeded with the payments.

Revolut said Mr H it initiated the recovery process on 3 January 2024, but it was told that no funds remained. It said it didn't raise a chargeback request because Mr H didn't provide sufficient information, but the card payments were authorised via 3DS and once the funds were deposited to the beneficiary account, the service was considered to have been provided, so there were no chargeback rights.

It said Mr H was engaged in a live chat on 29 March 2023 after he acknowledged the initial Transfer Review warning which warned him about the risks he could face if he decided to proceed with the transfer. She declared the payment purposes as 'something else' and then chose to start a live chat with one of Revolut's agents before the payment was processed. It said its warnings were proportionate and appropriate and that further intervention or questioning wouldn't have changed the outcome.

It said it is an Electronic Money Institute (EMI), and typically, this type of account is opened and used to facilitate payments to cryptocurrency wallets, so the payments weren't out of character with the typical way in which an EMI account is used and the intended purpose of the account, which was to facilitate cryptocurrency purchases. So, there was no reason for it to be suspicious.

It said Mr H transferred funds to accounts in his own name and it was used as an intermediary to receive funds from Mr H's external account and then transfer on to legitimate external accounts, to the fraud didn't occur on the Revolut platform.

It cited the Supreme Court's judgment in *Philipp v Barclays Bank UK plc* [2023] UKSC 25. The Court held that in the context of APP fraud, where the validity of the instruction is not in doubt, no inquiries are needed to clarify or verify what the bank must do. The bank's duty is to execute the instruction and any refusal or failure to do so will prima facie be a breach of duty by the bank.

It said that for this service to effectively apply the reimbursement rules to self-to-self transactions executed by Revolut is an error of law. Alternatively, we have irrationally failed to consider the fact that these transactions are self-to-self and therefore obviously distinguishable from transactions subject to the regulatory regime concerning APP fraud.

And it is irrational (and illogical) to hold it liable for customer losses in circumstances where it is merely an intermediate link, and there are typically other authorised banks and other financial institutions in the payment chain that have comparatively greater data on the customer.

Our investigator didn't think the complaint should be upheld. He noted that the payment for £10,500 flagged and Mr H was pulled into a live-chat, where he was asked tailored questions and given tailored warnings based on the answers he gave. Mr H said he was buying Bitcoin and using it for an investment, he hadn't downloaded AnyDesk and he hadn't been contacted or encouraged to invest by someone he doesn't know or had only met online recently.

Our investigator was satisfied the intervention was proportionate to the risk associated with the payment and that Mr H's responses prevented it from detecting the scam. He didn't think it needed to do anything else and he was satisfied it was reasonable for it to have processed the payment. And he didn't think it would have made any difference if Revolut had intervened again because the same thing would have happened.

Mr H has asked for the complaint to be reviewed by an Ombudsman. His representative has explained that Mr H can't recall the intervention which shows it was ineffective and basic and that it failed to ask probing and relevant questions and to provide the effective scam warnings.

### **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 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, Mr H 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 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;
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving 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 genuine cryptocurrency exchange companies. 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 did enough when Mr H 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 first two payments were low value payments to a legitimate cryptocurrency exchange and so Revolut didn't need to intervene. I note it did intervene on 29 March 2023 when Mr H made the third payment which was for £10,500. Mr H said the payment was for 'something else' and was then engaged in a live-chat with one of Revolut's agents where he was asked whether he'd been asked to install AnyDesk, whether he'd been told to withhold information, whether he'd been told to create a Revolut account, whether he was being pressured to act quickly at risk of missing out on an investment, whether he'd been promised returns which were too good to be true, whether he'd done any research and whether he'd been encouraged to invest by someone he'd met online recently.

I'm satisfied these questions were sufficiently probing and that the answers he gave were misleading and prevented Revolut from detecting the scam. I'm also satisfied that the

warnings Revolut gave to Mr H during the chat were relevant and proportionate to the risk presented by the payment, and that there was nothing further it could reasonably have done to prevent his loss.

I've considered whether Revolut missed any further opportunities to intervene, and I think it ought reasonably to have intervened again on 21 April 2023 because Mr H sent five payments totalling £20,500. But I would expect him to have been asked very similar questions to those he was asked on 29 March 2023, and I think it's likely he'd have given the same answers and dismissed the warnings again. So, I don't think a further intervention would have made a difference.

### *Recovery*

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

Mr H's own testimony supports that he used a cryptocurrency exchange to facilitate the card payment. It's only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchange would have been able to evidence they'd done what was asked of them. That is, in exchange for Mr H's payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I'm satisfied that Revolut's decision not to raise a chargeback request against either of the cryptocurrency exchange companies was fair.

### *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 25 April 2025.

Carolyn Bonnell  
**Ombudsman**