

The complaint

Mr T complains that Revolut Ltd (Revolut, hereinafter) hasn't refunded the losses he's incurred when falling victim to an investment scam.

What happened

Mr T found the scam via a social media platform at the beginning of 2025. It was advertised as being aimed at beginners only just starting out with cryptocurrency trading, which caught Mr T's attention.

Mr T expressed his interest and was later contacted by the scammer, who introduced him to a fake online investment platform and persuaded him to open an account with Revolut to make the payments. Mr T already had a cryptocurrency wallet with a genuine provider I'll refer to as T but also opened wallets with other two providers I'll address as B and C for the purpose of the scam.

Mr T received some returns halfway through the scam, which were paid into Mr T's account with Revolut.

From his Revolut account Mr T made the following payments (the returns or credits into the account are highlighted in bold):

Date	Time	Type of transaction	Amount
07/02/2025	20:29:03	Debit Card Payment to Mr T's cryptocurrency wallet with C	£30.00
07/02/2025	22:42:14	Debit Card Payment to Mr T's cryptocurrency wallet with T	£70.00
08/02/2025	10:08:15	Debit Card Payment to Mr T's cryptocurrency wallet with T	£100.00
08/02/2025	14:59:21	Debit Card Payment to Mr T's cryptocurrency wallet with T	£100.00
09/02/2025	17:56:43	Debit Card Payment to Mr T's cryptocurrency wallet with T	£1,000.00
10/02/2025	12:17:27	Debit Card Payment to Mr T's cryptocurrency wallet with B (DECLINED)	£3,750.00
10/02/2025	12:19:52	Debit Card Payment to Mr T's cryptocurrency wallet with B (REVERTED)	£3,750.00
10/02/2025	12:55:53	Debit Card Payment to Mr T's cryptocurrency wallet with C	£3,750.00
10/02/2025	12:57:06	Debit Card Payment to Mr T's cryptocurrency wallet with C	£9.99
12/02/2025	17:20:33	Credit from Mr T's cryptocurrency wallet with C	£100.00
12/02/2025	17:27:24	Credit from Mr T's cryptocurrency wallet with C	£100.00
15/02/2025	19:31:07	Debit Card Payment to Mr T's cryptocurrency wallet with T	£130.00
22/02/2025	10:08:23	Debit Card Payment to Mr T's cryptocurrency wallet	£50.00

		with T	
22/02/2025	13:13:38	Debit Card Payment to Mr T's cryptocurrency wallet with T	£100.00
02/03/2025	14:13:00	Debit Card Payment to Mr T's cryptocurrency wallet with C	£30.00
02/03/2025	14:54:32	Debit Card Payment to Mr T's cryptocurrency wallet with C	£40.00
03/03/2025	19:55:03	Debit Card Payment to Mr T's cryptocurrency wallet with T	£50.00

Mr T realised he had fallen victim to a scam when his returns dropped to zero on the fake investment platform and would not increase again, even if he continued making payments. Mr T made a complaint to Revolut about what happened on 21 March 2025, via his representatives.

Revolut said it raised chargeback claims for all the disputed transactions, but they were unsuccessful as payments had been authorised by 3D Secure protocol, and because the cryptocurrency exchanges Mr T had sent funds to, had provided a genuine service to him, so there was no valid chargeback code under which these claims would be successful.

Revolut said also that it had questioned Mr T appropriately at the time it identified that he may be at risk of falling victim to a scam and it blocked the merchant for all future payments as a consequence of that interaction. It was only after Mr T asked for the merchants to be unblocked, that the payments were processed. So, it thinks it's done enough to protect Mr T and declined to refund his losses.

So, Mr T referred the complaint to the Financial Ombudsman Service.

Our Investigator found that Revolut's intervention was proportionate. They said any further intervention was unlikely to prevent Mr T's scam losses because of how Mr T's interacted with Revolut's questionnaire, which ultimately didn't allow Revolut to identify he was being scammed.

Mr T and his representatives disagreed with our Investigator's view on the basis that Revolut should have stopped the scam from the earlier payments, as it should have identified they were going to a scam platform and that the appropriate mode of dealing with this was via human intervention. Mr T's representatives believed Revolut should have done this due to Mr T's vulnerabilities and very young age. Mr T's representatives said Mr T would have been honest, if the appropriate questions had been asked and the scam would have been unveiled.

In light of this disagreement, I have been asked to review everything afresh and reach a decision on the matter.

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'm aware that I've summarised this complaint briefly, in less detail than has been provided, and in my own words. No discourtesy is intended by this. Instead, I've focused on what I think is the heart of the matter here. If there's something I've not mentioned, it isn't because I've ignored it. I'm satisfied I don't need to comment on every individual point or argument to be able to reach what I think is the right outcome. Our rules allow me to do this. This simply reflects the informal nature of our service as a free alternative to the courts.

Where the evidence is incomplete, inconclusive, or contradictory, I must make my decision on the balance of probabilities – that is, what I consider is more likely than not to have happened in the light of the available evidence and the wider surrounding circumstances.

I don't doubt Mr T has been the victim of a scam here – he has lost a large sum of money and has my sympathy for this. However, just because a scam has occurred, it does not mean Mr T is automatically entitled to recompense by Revolut. It would only be fair for me to tell Revolut to reimburse Mr T for his loss (or a proportion of it) if:

- I thought Revolut reasonably ought to have prevented all (or some of) the payments Mr T made, or
- Revolut hindered the recovery of the payments Mr T made

whilst ultimately being satisfied that such an outcome was fair and reasonable for me to reach.

I've thought carefully about whether Revolut treated Mr T fairly and reasonably in its dealings with him, when he made the payments and when he reported the scam, or whether it should have done more than it did.

Having done so, I've decided to not uphold Mr T's complaint. I know this will come as a disappointment to Mr T and so I will explain below why I've reached the decision I have.

Should Revolut have intervened on the scam payments?

I have kept in mind that Mr T made the payments himself, and the starting position is that Revolut should follow its customer's instructions. So, under the Payment Services Regulations 2017 (PSR 2017) he is presumed liable for the loss in the first instance.

I appreciate that Mr T did not intend for his money to ultimately go to fraudsters and was deceived into doing so – but he did authorise these payments to take place. However, there are some situations when a bank, or an electronic money institution such as Revolut, should have had a closer look at the wider circumstances surrounding a transaction before allowing it to be made.

Considering the relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time – Revolut should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and 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 payment service providers are generally more familiar with than the average customer.
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or make additional checks, before processing a payment, or in some cases decline to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.
- Have acted to avoid causing foreseeable harm to customers, for example by

maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so.

So, I've thought about whether the transactions should have highlighted to Revolut that Mr T might be at a heightened risk of financial harm due to fraud or a scam.

Mr T's representatives have argued that Revolut should have intervened earlier than it did, however I'm mindful Revolut didn't have any historic information about the account or what Mr T's typical usage was like. So, it wasn't in a position to know whether Mr T's activity was unusual or out of character – as it had nothing to compare it against.

I must also consider that not every payment going to cryptocurrency providers will be part of a scam, and that it would be wholly impracticable for financial firms to block every cryptocurrency payment made from their payment facilities, as trading cryptocurrency isn't per se an illegal activity.

The scam payments Mr T made before Revolut's intervention on 10 February 2025, were of very small value, and whilst some took place on the same day, they were still spaced out between one another. Moreover, Mr T had selected when opening his Revolut account that he wished to use it for the purpose of cryptocurrency trading and investing.

So, I don't think a clear fraud pattern had emerged up until the first attempted payment of £3,750 on 10 February 2025, and I'm satisfied Revolut wasn't required to intervene until it did.

I understand that Revolut did intervene on both payments Mr T attempted to make to his cryptocurrency wallet with B. However, when Mr T then proceeded to make a payment for the same amount to his cryptocurrency wallet with C, Revolut did not intervene.

Revolut justified its position by stating it didn't intervene because Mr T unblocked all payments to genuine cryptocurrency merchants on the Revolut app. But I disagree that such action from Mr T or any other customer would justify Revolut's inaction, when the payment they are attempting suggests they may be at a heightened risk of financial harm from fraud or a scam.

Revolut should be on the lookout for signs of fraud and review its customers' activity regularly, independently of whether a customer thinks they're making a legitimate transaction.

I believe that when Mr T made the £3,750 payment to his wallet with C, Revolut ought to have intervened. I say this because of the value of the individual payment and its combined value with the earlier payments Mr T had sent, and the fact all of the payments were going to identifiable cryptocurrency providers.

The transaction was made on the same day as Mr T's payment to another cryptocurrency provider had been declined by Revolut, and after Mr T had cancelled another one. I think these factors, taken together, ought to have alerted Revolut about the potential risk of scams or fraud, by the time this payment was being made.

Revolut shouldn't have processed that payment without first taking steps to warn Mr T about the risk of scams. Whilst Mr T's representatives have claimed that human intervention was warranted in this scenario, I don't believe the value of the payment was such to require that.

In the individual circumstances of this case, I would have expected Revolut to have intervened, and a proportionate intervention would have taken the form of a better

automated warning, specifically tailored to the risks posed by investment and cryptocurrency scams, and the reasons Mr T had given for the payment.

Would Revolut's intervention have made a difference?

The question for me to answer next is whether, on the balance of probabilities, Revolut would have been able to prevent Mr T's further losses, had it intervened at that stage of the scam.

I've considered that point carefully and I'm not persuaded it would have been.

The chat transcripts with the scammer don't suggest the scammer coached Mr T on how to deal with Revolut's interventions. It does transpire, though, that Mr T relied heavily on the scammer's advice on how to open and close trades on the fake investment platform, and that the cryptocurrency wallet addresses to send funds to the scammer were communicated to Mr T on the fake investment platform too.

Our service is also aware that Mr T started out by making cryptocurrency payments from another bank account in his name. It was only later that Mr T opened the account with Revolut and the cryptocurrency wallets with B and C for the purpose of the scam, due to limits on cryptocurrency payments imposed by his other bank.

So, I think it's likely Mr T had been advised by the scammer on what accounts to open, one way or another, to facilitate the transactions to the scammer's wallet. And whilst evidence of these interactions with the scammer isn't available, I can't exclude that Mr T may have communicated with the scammer either via call or via the fake trading platform to receive such advice.

Revolut has also provided records of how Mr T interacted with its earlier questionnaires on 10 February 2025. So, I've based myself on the evidence available to me to decide what would have most likely happened if Revolut had intervened on the £3,750 payment to Mr T's cryptocurrency wallet with C.

In the earlier interventions on that same day, Revolut blocked the payment Mr T was making and asked him to clarify the reasons for it. Before doing so, Revolut warned Mr T against the consequences of being untruthful when answering its questionnaire, which Mr T acknowledged. Mr T was also asked to confirm if he was being aided in making the payment and said he was acting alone and no one was telling him what to do.

Mr T proceeded to select that he was sending funds to his other account, even though he had the option to select that the payment was part of an investment. In the following screen, Revolut asked him again to clarify the purpose of the payment, at which point Mr T selected he was sending the funds to his investment account. Mr T then proceeded to say he had discovered the investment opportunity through family and friends, and that he had checked that the company he was investing with was on the FCA register.

Mr T had the opportunity to select that he had found the opportunity on social media, as it was genuinely the case. He also told us, via his representatives, that he didn't check the FCA register because he already knew that cryptocurrency isn't regulated, so he didn't think the investment would feature on the register. So, I would have expected him to select that he had not checked the FCA register. Because Mr T's responses to the questionnaire weren't an accurate reflection of how he came across the investment and what checks he had carried out, I don't think that his responses should have highlighted or put Revolut on notice that he was at a heightened risk of falling victim to a scam.

Mr T's representatives argued that, had Revolut issued relevant warnings to Mr T, he would have taken heed of them and the scam would have been unveiled.

But I'm not persuaded this would have been the most likely outcome, here.

I say this because, after the questionnaire, Revolut sent Mr T a series of in-app unskippable warnings, that described the common features of cryptocurrency scams. Some of the descriptions were very relevant to Mr T's scenario, as they mentioned professional-looking platforms and very high returns.

I note Mr T was informed by the scammer in the chat transcripts of 800% returns being paid to some investors, so I'm confident this feature of cryptocurrency scams should have been very relevant in Mr T's case.

The warning proceeded to describe how these opportunities are introduced on social media, as it was the case for Mr T's scam. Sadly, however, these warnings didn't resonate with Mr T, despite their contents being very relevant to his circumstances.

Revolut's second intervention unfolded along similar lines, except Mr T also selected that he was investing in stocks, bonds, currency exchange, or commodities, before reiterating he was investing unaided and that the opportunity had been recommended by family and friends.

The chat transcripts show the scammer suggested very early on in the scam that Mr T focused his portfolio on cryptocurrency contract trading, so I think the most appropriate option for Mr T to select on Revolut's questionnaire would have been "cryptocurrency" and not stocks and bonds.

So, I think that, independently of whether he was heavily coached to give a cover story or if he came up with his responses to the questionnaire alone, Mr T was intent on keeping the true reason of his payments hidden from Revolut and would have continued to disguise it for as long as he could.

Overall, I believe that Mr T's answers to the questionnaire didn't allow Revolut to identify the scam risks Mr T was facing, and because earlier proportionate and tailored warnings didn't resonate with Mr T, I'm not persuaded that any future ones would have either.

Finally, Mr T has also argued that he was vulnerable to the scam, due to his age and his learning difficulties. While I acknowledge this, the evidence I've seen doesn't suggest that Revolut had been notified by Mr T of any vulnerabilities or needs such that it should have known to take additional steps to protect him, as he was making the payments.

I don't believe that Mr T's age alone should have prompted Revolut to take steps beyond the ones it took, to try and warn him about the scam risks associated with his transactions.

Overall, based on all of the above, I believe Revolut wouldn't have been able to prevent Mr T's losses, even if it had intervened further in the scam.

The Contingent Reimbursement Model Code

Mr T's representatives have claimed that Revolut should have refunded Mr T in line with the Contingent Reimbursement Model Code. However, it's important to note that the Code doesn't apply to debit card payments, but faster payments only, and it can't be applied to payments made between accounts in the name and control of the scam victim. Furthermore,

Revolut has never been a signatory to the Code, so, I cannot fairly and reasonably say that Revolut should have to refund payments under the Code when it doesn't apply here.

Recovery

Because the scam payments were made via debit card, the only potential avenue for recovery would have been via a chargeback claim.

The chargeback scheme is a voluntary scheme set up to resolve card payment disputes between merchants and cardholders.

Revolut is bound by the card scheme provider's chargeback rules, both Visa and Mastercard in this instance. Whilst there is no 'right' to a chargeback, I generally consider it to be good practice that a chargeback be raised if there is a reasonable chance of it succeeding. But a chargeback can only be made within the scheme rules, meaning there are only limited grounds and limited forms of evidence that will be accepted for a chargeback to be considered valid, and potentially succeed.

Given how the payments were authenticated through 3D Secure protocol, it's unlikely a chargeback would be successful on the grounds of authorisation.

I can see Revolut did raise chargeback claims for Mr T on the basis that goods and services had not been provided, but they unfortunately failed.

This is because the payments went to legitimate cryptocurrency providers, which did provide services to Mr T in exchange for his funds, albeit just not for his benefit. So, I don't think Revolut could have done more to attempt to recover Mr T's funds in this instance.

My final decision

For the reasons given above, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr T to accept or reject my decision before 3 February 2026.

Daria Ermini
Ombudsman