DRN-5591950

The complaint

Mrs S complains that Revolut Ltd ('Revolut') won't reimburse the money she lost when she fell victim to a scam.

What happened

Mrs S says that she saw a celebrity endorsed advert on social media about an investment opportunity. She clicked a link and shortly afterwards she received a call from someone who explained the investment was with a company I'll call C. Mrs S made a payment of a little over £200 towards this investment using an external account. The following day, Mrs S received a message from someone who said she would be Mrs S' adviser. Mrs S didn't know at the time, but C was a fake company, and the financial adviser was a scammer.

Mrs S said she could quickly see that she was making money. The scammer then told her that because she was a new customer, if she invested a further £3,000 C would pay £1,500 into her account. The scammer used a screen-sharing application to help Mrs S set up accounts with Revolut and another electronic money institution (EMI), saying the accounts were needed to transfer Mrs S' money through. The £3,000 payment was then made from Mrs S' account with another EMI on 19 January 2023. Mrs S believed these funds were crediting her account with C.

Mrs S says that the scammer helped her to make further card payments from her Revolut account to a cryptocurrency exchange (B) to verify her liquidity. I have set out all the transactions Mrs S made to B in the table below:

Transaction	Date	Amount
1	02/02/23	£15
2	03/02/23	£4,950
3	03/02/23	£9,800
4	03/02/23	£4,950
5	03/02/23	£4,900
6	03/02/23	£8,200
7	03/02/23	£15,000
8	07/02/23	£24,900
9	07/02/23	£15,000
Total		**£87,715**

Whilst Mrs S was aware of the payments, she says she didn't fully understand the position and thought they were being made to enable her to withdraw funds from B. She didn't know at the time, but emails she received from Revolut and B were fake.

Mrs S contacted Revolut via its chat function on 8 February 2023. She asked why she was

unable to withdraw funds from her trading platform and referred to a figure of £130,000. The Revolut adviser confirmed that Mrs S had £310.01 in her account and the rest had been transferred to B. Mrs S contacted Revolut again after this and the scam was uncovered.

Mrs S' appointed representative sent a letter of complaint to Revolut at the end of January 2024. They said that Revolut should have identified that payment two was unusual and asked probing questions about it, at which point the scam would have been uncovered.

Revolut considered Mrs S' claim but didn't agree to reimburse her. It said it had no chargeback rights in respect of any of the card payments.

Revolut told this service the transactions were 'self-to-self' and didn't take place on its platform, so it can't be held responsible for them. It also referred to the fact the account was newly created (the account was opened on 17 January 2023), so it had no transaction history to compare the payments with, and to Mrs S' lack of due diligence.

Our investigation so far

The investigator who considered this complaint didn't recommend that it be upheld. He didn't think Revolut could have been expected to prevent the loss. This was because Mrs S' bank discussed transfers from her current account to the other EMI account she was supported to open. During these conversations Mrs S misled her bank about the reason for the payments. Mrs S' bank provided scam warnings that were relevant to the scam Mrs S was falling victim to, which she didn't heed. So, the investigator thought that any intervention by Revolut wouldn't have made a difference.

Mrs S didn't agree with the investigator's findings and asked for a final decision. The main point made by Mrs S was that Revolut should have intervened, asked open and probing questions, and held her answers up to a reasonable level of scrutiny – taking into account that scammers often coach their victims.

Mrs S went on to say that the intervention by her bank (referred to by the investigator) was insufficient and not a reflection of what would have happened if Revolut had intervened appropriately. The reason Mrs S gave to her bank for a payment (to buy materials for a property) couldn't be used in any intervention by Revolut, as Mrs S was paying a cryptocurrency provider. And Mrs S' representative said the scammer didn't give her a cover story.

The complaint was passed to me to decide. I intended to reach a different outcome to the investigator, so I issued a provisional decision on 8 May 2025 to explain why. In the "What I've provisionally decided – and why" section of my provisional decision I said:

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.

I'm sorry to hear that Mrs S has been tricked into making these payments. I understand she has lost a significant amount of money.

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.

I consider that Revolut should in January and February 2023 have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances.

Overall, 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 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 Mrs S was at risk of financial harm from fraud?

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

I'm aware that cryptocurrency exchanges generally stipulate that the card used to purchase cryptocurrency at its exchange must be held in the name of the account holder, as must the account used to receive cash payments from the exchange. So Revolut likely thought the transactions I have set out in the table above would be credited to a cryptocurrency account in Mrs S' own name.

But by the time these payments were made, firms like Revolut had been aware of the risk of multi-stage scams involving cryptocurrency for some time. Scams involving cryptocurrency have increased over time. The FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018 and figures published by the latter show that losses suffered to cryptocurrency scams have continued to increase since.

So, taking into account all of the above, I am satisfied that by the end of 2022, prior to the payments Mrs S made, 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 and

good practice, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments. I don't think that the fact payments were going to an account held in Mrs S' own name should have led Revolut to believe there wasn't a risk of fraud.

As I will discuss below, I consider Revolut ought to have intervened when Mrs S made payments two and six.

What did Revolut do to warn Mrs S?

I can't see that Revolut took any steps to warn Mrs S.

What kind of warning should Revolut have provided to Mrs S?

I've gone on to consider, taking into account what Revolut knew about the payments, at what point, if any, it ought to have identified that Mrs S might be at a heightened risk of fraud. I've given due consideration to Revolut's duty to make payments promptly, as well as what I consider to have been good industry practice at the time.

When Mrs S 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. It was to an identifiable provider of cryptocurrency and was for a relatively large amount. 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 tailored written warning.

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 should have highlighted, in clear and understandable terms, the key features of these scams, for example referring to: an advertisement on social media, possibly 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.

By payment six I think a proportionate response to the risk presented would have been for Revolut to have attempted to establish the circumstances surrounding the payment before allowing it to debit Mrs S' account. Mrs S had made a series of higher value payments that were going to an identifiable provider of cryptocurrency. I think it should have done this by, for example, referring Mrs S to its in-app chat rather than providing an on-screen warning.

If Revolut had provided warnings of the type described, would that have prevented the losses Mrs S suffered?

I'm not persuaded that a written on-screen warning as set out above would have resonated with Mrs S and prevented her loss when she made the second payment. Mrs S was under the spell of the scammer and was following the advice she was given. She had opened multiple accounts on her instructions and had lied to her bank about the reason for transferring funds to Revolut. So I think that Mrs S might have mentioned the warning to the scammer and accepted any response that told her to proceed.

I've also thought about what's most likely to have happened if Revolut had intervened and asked further questions, for example in its chat, about payment six.

I'm aware that Mrs S' bank had spoken to her the day before about a transfer she was making to her Revolut account. In the call, Mrs S told her bank that her daughter had recommended that she opened the accounts with Revolut and another EMI and referred to

being able to get cashback. She said she and her son-in-law had bought a house and she was transferring funds to him.

After completing some checks, Mrs S' bank's fraud adviser provided her with some scam advice. He said that if anybody calls her and wants her to make a payment or transfer from her account, it's part of a scam. Mrs S was also advised that genuine organisations will never ask her to download anything to her devices. He referred to the fact that scammers can be very skilled and convincing. Mrs S has explained that she was coached in how to answer questions posed by her bank.

It wouldn't have been possible for Mrs S to have plausibly told Revolut that she was moving funds in respect of a house, as she had told her bank. Revolut would have known that this wasn't true, as it could readily identify that the funds were being paid to a cryptocurrency wallet. And by the time Mrs S made payment six she had received an email that she thought had been sent by Revolut (but was fake) on the morning of 3 February 2023. This email said she had successfully received £40,000 but needed to complete 'Liquidity Verification'. Mrs S responded and said she had completed the verification and was told to expect a phone call. She discussed the call purporting to be from Revolut with the scammer and said that she had been asked to provide statements from all her banks. The scammer agreed to help Mrs S send these documents.

Mrs S thought she was interacting with Revolut when she responded to emails and had a phone call (although this wasn't the case), so I see no reason why, if Revolut had asked her questions when she made payment six, she wouldn't have referred to her communications with Revolut or explained that she was making payments to prove her liquidity. There can't have been a cover story to tell Revolut. This is borne out by the fact that Mrs S contacted Revolut's genuine chat on 8 February 2023 and asked why she was unable to withdraw funds from her trading account.

I recognise that Mrs S' bank told her that genuine organisations wouldn't get her to download anything, but this advice wasn't given in the context of an investment scam warning. Mrs S' bank focused primarily on safe account scams.

Overall, I consider it more likely than not that human intervention in respect of payment six would have led to the scam being unravelled and no further payments being made.

<u>Is it fair and reasonable for Revolut to be held responsible for Mrs S' loss?</u>

In reaching my decision about what is fair and reasonable, I have taken into account that Mrs S purchased cryptocurrency which credited a wallet in her own name, rather than making a payment directly to the fraudsters. So, she remained in control of her money after she made the payments from her Revolut account, and it took further steps before the money was lost to the fraudsters.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mrs S might have been at risk of financial harm from fraud when she made payment six, and in those circumstances it should have declined the payment and made further enquiries. If it had taken those steps, I am satisfied it would have prevented the losses Mrs S suffered. The fact that the money used to fund the scam came from elsewhere and wasn't lost at the point it was transferred to Mrs S' own account does not alter that fact and I think Revolut can fairly be held responsible for Mrs S' loss in such circumstances. I don't think there is any point of law or principle that says that a complaint should only be considered against either the firm that is the origin of the funds or the point of loss.

Mrs S brought complaints to this service against other firms. This service said that her bank

acted reasonably when Mrs S transferred funds to her Revolut account. So that case doesn't impact my decision against Revolut. Mrs S also has a complaint against the EMI, about funds that went from her bank to the EMI, and then to B. This complaint also has no impact on this case and there was no intervention. In this case it is appropriate to hold Revolut responsible as it could have prevented Mrs S' loss. That isn't, to my mind, wrong in law or irrational but reflects the facts of the case and my view of the fair and reasonable position.

Should Mrs S bear any responsibility for her losses?

In considering this point, I've taken into account what the law says about contributory negligence as well as what's fair and reasonable in the circumstances of this complaint.

I recognise that there were some sophisticated elements of this scam which involved a fake celebrity endorsed advert and platform, and faked emails from Revolut and B (and a fake call from Revolut) which would have given the investment legitimacy.

But I consider there were red flags that should have concerned Mrs S. Mrs S hasn't suggested that she completed research in respect of C before investing and I'm unable to find any reviews at the time Mrs S made the payments, which is unusual. Mrs S then received messages from someone who said they were a financial adviser but made no mention of C. This adviser told Mrs S to lie to her bank about the reason for transfers to her Revolut account. I can't see that a legitimate investment company would ask a customer to do this. The scammer also advised Mrs S to download a screen sharing app. When Mrs S spoke to her bank about a transfer on 2 February 2023, she was told that legitimate companies wouldn't ask her to download anything.

The fake emails Mrs S received contained errors in terms of content and grammar. For example, a fake email from Revolut said at the bottom that it was from her EMI account's billing team. Mrs S recognised this error, as she raised it in the chat with the scammer but took no further action. The reasons for the requests to pay further funds also became less plausible.

The messages supplied aren't all dated but I believe on 6 February, before the final two payments, the scammer gave Mrs S advice about attending branch if she was required to do so. She told Mrs S to delete the screen sharing app and her app for her account with B before going into branch, and not to open her Revolut app. It's difficult to understand why such deceit was necessary if Mrs S was dealing with a genuine company.

I also consider that Mrs S ought reasonably to have had concerns about being asked to pay such large amounts of money to withdraw her funds. She had invested a small initial amount and an additional £3,000 and then was asked to pay increasing amounts of money to verify accounts and withdraw her funds. And the profits Mrs S was told she had received were unrealistic. On 20 January 2023 (after investing £3,000 the day before from her EMI account) Mrs S was told she had a profit and bonus of £1,240.

Revolut has referred to the fact there was an FCA warning about C from 2 February 2023. But Mrs S had been involved with the scammers for some time by this date. And, without being given any form of warning to highlight the importance of making this check, I don't consider Mrs S would have known about it.

Overall, I'm persuaded that Revolut should reimburse 50% of Mrs S' loss from and including payment six together with interest as set out below, as Mrs S has been deprived of the funds.

Responses to my provisional decision

Revolut let me know that it had nothing further to add.

Mrs S said that the fairest trigger point in this case would be payment three, as it was the second payment that day to a known cryptocurrency merchant and brought the total spend that day to £14,750. Mrs S also expressed concern that the decision in this case wasn't consistent with the decision I reached on a linked case.

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.

After reviewing Mrs S' response to my provisional decision my decision remains the same. I set out my full reasoning in my provisional decision (and reproduced it above) so I won't repeat it in full here.

I still think that Revolut ought reasonably to have provided a written warning tailored to cryptocurrency investment scams when Mrs S made payment two and asked Mrs S questions about payment six before processing it. I'm not persuaded a written warning when transaction two was made would have resonated with Mrs S and prevented her loss from that point. But I'm satisfied that human intervention when payment six was made would have uncovered the scam, as Mrs S had received fake emails from Revolut by this point and would likely have discussed them.

Mrs S has said that Revolut should have asked her questions in the chat when she made payment three given that it was the second payment that day to an identifiable provider of cryptocurrency and the cumulative value of the two payments. But I don't agree. I consider Revolut ought to have provided a written warning for the previous payment and that it didn't need to go further than this until payment six, when an unusual pattern of payments had emerged. My decision about when Revolut should intervene doesn't solely depend on the number of payments in a day as Mrs S' representative seems to be suggesting.

For the reasons previously stated, I consider Mrs S should be held partly responsible for her loss. Whilst there were some aspects that would have made the scam seem convincing, there were many red flags. Mrs S doesn't appear to have completed any research before deciding to invest, the returns were unrealistic and being asked to pay huge sums to withdraw profit was concerning. The scammer asked Mrs S to download a screen sharing app and to lie about her payments. And the fake emails Mrs S received contained errors. On balance, I think a 50% deduction is fair.

My final decision

I uphold this complaint and require Revolut Ltd to:

- Pay Mrs S £31,550; and

- Pay interest on the above amount at the rate of 8% simple per year from the date of each transaction to the date of settlement.

If Revolut Ltd is legally required to deduct tax from the interest it should send Mrs S a tax deduction certificate so she can claim it back from HMRC if appropriate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs S to accept or reject my decision before 26 June 2025.

Jay Hadfield
Ombudsman