DRN-5981825

The complaint

Miss B complains that Revolut Ltd won't refund her the money she lost in an investment scam.

What happened

The background to Miss B's complaint is well-known to the parties, so I have summarised what I consider to be the key points.

Miss B says that in late June 2024 she saw an advertisement for an investment company that was backed by a well-known celebrity. She followed links which led her to another investment company, based overseas. She decided to invest through this company and went through an onboarding process.

She was assigned an account manager, who she says was very professional and she had daily calls with him at first. He took time to build a rapport and send her information about investments. She says she was told the investment would provide low-risk, high returns and her account manager mentioned a guarantee of doubling her money within six months. Miss B says she trusted the account manager completely and felt happy speaking to him. She regarded him as a friend. She says she felt like she was hypnotised into following his step by step instructions. He suggested Miss B increase her investment, which she did because she could see her investment returns increasing.

Miss B funded the investment by sending money through various bank accounts to newly created accounts with cryptocurrency exchanges and from there on to the investment company.

Eventually, the account manager suggested Miss B should withdraw her money and he told her that in order to do so, she would need to make a final payment of 10% of the value of her investment, which would enable the money to be released. Miss B made this final payment from a different bank, not through Revolut, but she didn't receive any return from her investment. By 28 October 2024, she told the account manager she had made enquiries and had been told that the investment platform might be a scam. She said she had been made aware of negative feedback, with customers unable to access their money. She reported the scam to Revolut on 30 October 2024.

Miss B says she made the following payments as part of this scam:

Date	Amount	Payment type	Destination
08/07/2024	£5,000	Transfer	Own cryptocurrency account X
01/08/2024	£3,000	Transfer	Own cryptocurrency account S
03/08/2024	£9,500	Transfer	Own cryptocurrency account S
04/08/2024	£4,000	Transfer	Own cryptocurrency account S
08/08/2024	£9,500	Transfer	Own cryptocurrency account X
09/08/2024	£9,500	Transfer	Own cryptocurrency account X
12/08/2024	£9,000	Transfer	Own cryptocurrency account X
13/08/2024	£8,961.94	Transfer	Own cryptocurrency account X

26/08/2024	£9,500	Transfer	Own cryptocurrency account X
28/08/2024	£9,500	Transfer	Own cryptocurrency account X
29/08/2024	£9,500	Transfer	Own cryptocurrency account X
30/08/2024	£1,500	Transfer	Own cryptocurrency account X
Total:	**£88,461.94**		

Miss B complains that Revolut ought to have intervened because the transactions were out of character for her account. She says Revolut didn't flag the transactions as unusual or provide her with real-time scam warnings nor did it implement any additional security checks. She says Revolut didn't make any contact with her about any of the payments until 26 August 2024, after most of her money had already been sent to the scammer.

Revolut says it isn't responsible for Miss B's loss. Miss B authorised the payments and controlled the accounts her money was sent to. It says Miss B was coached by the scammer and gave Revolut inaccurate answers when it asked her questions about the payments. Revolut says this prevented it from uncovering the truth and made it likely that if it had intervened further, it still wouldn't have been able to uncover the scam. That's because it considers it's likely Miss B would have provided further inaccurate answers. It says it gave Miss B appropriate warnings and other banks should have provided warnings and interventions too. It felt Miss B acted with gross negligence by ignoring warning signs that this was a scam.

Our investigator didn't uphold Miss B's complaint. He said Revolut's interventions were proportionate and he wouldn't have expected it to have intervened further. He considered that Miss B hadn't been honest with Revolut when it asked her questions about the payments and this prevented it from uncovering the scam.

Miss B didn't accept the investigator's conclusions. She says she didn't provide inaccurate answers to Revolut. She didn't think Revolut's automated interventions were sufficient. She was vulnerable at the time and the fraud has had a detrimental impact on her life. The majority of transactions were sent to a payee that has been associated with a lot of scam activity and this should have flagged with Revolut as an additional risk factor.

I issued a provisional decision on Miss B's complaint on 3 November 2025, in which I said:

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

Evidence of loss

In order to uphold Miss B's complaint, I would need to be satisfied she has been the victim of a scam and that it could be established how much money she has lost. In this case, while I'm satisfied it's likely Miss B has been the victim of a scam, it isn't clear how much she has lost.

Miss B moved a lot of money between several accounts held in her name but there is very little showing how much was deposited into her investment account with the scammer. The screenshots from the investment account appear to show a number of fictious trades but they don't record the amounts of any deposits into that account or where they came from. There is some evidence in the form of emails, from one of her cryptocurrency accounts, confirming trades, that show some money was withdrawn to another wallet, possibly controlled by the scammers, on 9 July and 8 and 9 August 2024 but I haven't seen much evidence showing all the money sent to her cryptocurrency accounts was withdrawn and sent to the scammers.

In addition, while I can see three payments on 1,3 and 4 August 2024, totalling £16,500, left Miss B's account with Revolut (listed above) and were sent to one of her cryptocurrency accounts, the evidence shows the cryptocurrency provider closed Miss B's account and sent a payment of £36,998.94 back to another of Miss B's bank accounts on 7 August 2024. This money was then sent back to Revolut from Miss B's other bank account in payments on 8, 9, 11 and 12 August 2024 amounting to £37,000. So, Miss B's actual loss from her Revolut account must be lower as it seems there is an element of double-counting.

Control of the cryptocurrency accounts

All the payments from Revolut were made to cryptocurrency accounts held in Miss B's name, but Miss B says she didn't have control over one of the accounts, which I've labelled cryptocurrency account 1 in the list above.

I can see that the scammer sent her screenshots from that cryptocurrency account, suggesting he had access to it. But I can also see that Miss B sent instructions to that cryptocurrency exchange from her email account, instructing it to make payments and that she received confirmations back from the cryptocurrency exchange once the payments had been made. She was contacted by the scammer for confirmation that the cryptocurrency had been sent from this account because I've seen emails where he asks Miss B for confirmation. I don't see why he would have needed to do that if he had control of the account. It seems that the scammer might have had some access to this cryptocurrency account, but Miss B has confirmed that she instructed these payments to be made from that cryptocurrency account to her investment account so I don't think I could reasonably conclude she didn't control it, as she instructed and authorised the payments from it.

Revolut's interventions

The starting position is that Revolut is expected to process payments and withdrawals that its customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And in this case, it's accepted by all parties that Miss B authorised the payments and Revolut made the payments in accordance with Miss B's instructions.

The Contingent Reimbursement Model (CRM) Code doesn't apply in this case because Revolut wasn't a signatory of the code and the payments were made to accounts that appear to have been under Miss B's control. But the matter doesn't end there. Having taken into account longstanding regulatory expectations and requirements, and what I consider to be good industry practice, I think Revolut ought to have been on the look-out for the possibility of fraud and made additional checks before processing payments in some circumstances.

I've considered Revolut's interventions and whether further and better intervention by Revolut is likely to have made a difference. But having considered everything, while I consider Revolut could have intervened further, I'm not persuaded it would have made any difference here. I'll explain why.

Revolut sent warnings to Miss B on 8 July, 1 August and 26 August 2024 in relation to this series of payments. Given the significant amount of most of these payments and the frequency with which they were made, for example payments of £9,000 or more made to the same payee on consecutive days, I consider Revolut ought to have intervened on further occasions. I don't agree with Miss B that payments to these payees ought to have been blocked. The payees were legitimate businesses. They did provide cryptocurrency exchange as a service and so it's arguable Revolut ought to have known this and due to the prevalence of fraud involving cryptocurrency, this ought to have been an additional risk

factor that informed whether it intervened and what form that intervention took.

Revolut says it sent Miss B a new beneficiary warning and a tailored written warning on 8 July 2024 in relation to payment 1. The new beneficiary warning was a general warning about being sure who she was paying but the tailored written warning contained a request for further details. Revolut asked Miss B what the purpose of the payment was and then asked further questions based on her response. These further questions were relevant to her response and designed to narrow-down the particular scam risk she was facing. Miss B told Revolut the payment purpose was to move money to another of her accounts. Revolut then asked a number of questions relevant to own-account transfers. For example, it asked whether anyone had asked her to move money to another account or told her that her existing account wasn't safe. Her answers were broadly accurate, but if she had selected that she was making an investment, which was an option, she would have been given more relevant warnings.

Revolut sent another tailored written warning on 1 August 2024 and Miss B once again said she was transferring money to another account of hers. But she also selected that she was making the payment to an investment account. Revolut asked her relevant questions based on her answers, such as whether she had been asked to download remote access software, how she had discovered the investment and whether she had researched the company. Miss B said she had heard about the investment from a friend and she had checked the FCA register and reviews. While Miss B says she considered the investment advisor to have been a friend, I don't consider this answer was accurate because she hadn't heard about the investment from the advisor, she discovered it through a social media advertisement.

Revolut says it told Miss B, in both interactions, that she shouldn't let anyone tell her how to respond to Revolut, to get a second opinion and to do research. But Miss B was letting someone tell her how to respond, she didn't seek a second opinion and doesn't appear to have researched the investment.

A further new beneficiary warning and a tailored written warning were sent on 26 August 2024. This time it was followed up with contact by a member of staff through in-app messaging. When she received the automated warning asking her about the purpose of the payment, Miss B selected "I'm transferring money to another account of mine." She said she was transferring money to an account with another bank. Revolut didn't ask many questions and I don't find the questions it asked were effective or probing.

However, Miss B has provided evidence of a stronger intervention from another business. Payments 2, 3 and 4 went to Miss B's account with a cryptocurrency exchange. That exchange warned her that it thought she might be being misled or tricked. It warned her about investments where she was guaranteed returns or told that she could make high returns with little or no risk. These were relevant to her situation. She was asked probing questions about these payments. In an email dated 29 July 2024, the cryptocurrency exchange asked her how she had found out about the cryptocurrency exchange and she said she had found it through her own research. She was asked whether she was receiving advice from a financial advisor and she told it she wasn't receiving advice. In a follow-up email on 30 July 2024, Miss B had been asked where she was moving her cryptocurrency to when attempting to make a withdrawal and what her general investment strategy was. She said she intended to move her cryptocurrency to a wallet she held with another exchange and hold onto it there. In a later email the cryptocurrency exchange asked to see screenshots from the other exchange. The scammer then told Miss B to send him screenshots from the other cryptocurrency account to see if he could hide the payments she was making from that cryptocurrency exchange to her investment account. All Miss B's responses to the cryptocurrency exchange mentioned above were inaccurate.

As Miss B didn't tell the truth when she was asked probing questions about related payments by her cryptocurrency exchange, I'm not persuaded she would have been any more open with Revolut if it had intervened on other occasions or had asked her more probing questions. When one bank or cryptocurrency exchange asked Miss B questions, Miss B seems to have switched to making payments from another. There is mention of four different cryptocurrency exchanges used by Miss B as part of this scam and three different banks. The copies of emails and messages between Miss B and the scammer suggest he gave advice in relation to all these businesses, in terms of how to answer their questions and which accounts to make payments from. It seems likely that even if Revolut had intervened further, or declined to make some payments, Miss B would have moved her money elsewhere and found another way to make the payments. This is exactly what happened with the cryptocurrency exchange mentioned. When it started asking probing questions and ultimately closed Miss B's account with it, the advisor told her to make payments through another exchange.

I find that Miss B was deeply taken-in by the scammer and it isn't clear to me that any intervention would have been effective. I say this because Miss B says she felt hypnotised by the scammer and followed what he said step by step. Miss B says the scammer coached her on exactly how to answer Revolut's questions. The evidence, such as emails between Miss B and the scammer shows that she did indeed follow his instructions very closely, providing word for word responses in some cases. She told us she didn't have a shadow of a doubt about these payments and she trusted the scammer. Miss B also indicated that she thought of the scammer as a friend. All this makes it less likely, in my view, that Revolut would have been able to uncover the scam, even if it had intervened in person, for example through in-app messaging and has asked more probing questions. I think it likely Miss B would have sought assistance from the scammer about how to answer, just as she did when her cryptocurrency exchange asked her questions. I also think any warnings Revolut might have given her are unlikely to have convinced Miss B she was falling victim to a scam, based on the warnings she received from Revolut and her cryptocurrency exchange, which don't seem to have resonated with her.

Recovery

I can see from Revolut's records that it contacted the payees to try and recover Miss B's money on 30 October 2024, the same day she reported the scam to Revolut. Revolut contacted one of the payees around five hours after it contacted the first. I would expect Revolut to act promptly to try and recover its customers' money and I can see no good reason for that delay. However, the payments were made by Miss B to other accounts in her name and which she controlled. By her own account, money was moved on from these accounts swiftly and since Miss B reported the scam two months after the last payment from Revolut, I don't see that any delay of several hours in contacting the payees can have caused Miss B any loss.

Overall, while I'm very sorry Miss B has been the victim of a sophisticated scam and has lost her money and I don't doubt the impact this has had on her, and while I don't think Revolut did all it could have done, I'm not persuaded Revolut could reasonably have prevented Miss B's losses even if it had intervened further.

Miss B responded to my provisional decision and said:

- Her loss is £88,461.94 and there hasn't been any element of double-counting, as I had suggested. She provided a number of documents and an explanation to show how money had been moved round her various accounts before being sent to the scammer;

- Revolut didn't implement checks on every transaction. Only a few triggered in-app prompts. She followed the adviser's guidance, thinking these were standard banking procedure;

- She didn't knowingly provide inaccurate answers. She genuinely believed the adviser was a friend. He convinced her to say she had heard about the investment through family and friend recommendation and convinced her this was true. She had checked the FCA register before investing and hadn't downloaded any software;

- She provided further evidence she feels shows she did not have control of the cryptocurrency account;

- Revolut should have intervened with a phone call and if it had done so, she would have realised something was wrong. A call wouldn't have allowed the adviser time to coach her responses. She doesn't think it's fair for me to conclude she would have moved money elsewhere if Revolut had blocked the payments.

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.

Miss B has provided a detailed response to my provisional decision, along with various supporting documents, which I've necessarily had to summarise, but I have considered all the points she's made and the documents she's sent me. I haven't included all the points because some of them are not directly relevant to the outcome, for example her comments on the date she became aware of the scam. Having considered everything Miss B has provided, I've reached the same overall conclusion and for largely the same reasons. I'll explain why.

The documents Miss B has sent provide greater clarity on the movement of Miss B's money and they do provide good evidence of the amount that was sent on to the scammers through two cryptocurrency accounts.

While the flow of funds in this case is complicated, the further evidence Miss B has provided supports my point that some of the money she is claiming has effectively been double-counted. I'm not suggesting this is intentional, I think it's simply due to the complicated flow of funds. In summary Miss B paid £16,500 from her Revolut account to her account with a cryptocurrency exchange I'll call S. The first payment to S from her Revolut account, for £3,000 made on 1 August 2024, appears to have been converted into cryptocurrency and sent on from S to an account with another cryptocurrency exchange I'll call A. The money she sent to S from her Revolut account on 3 and 4 August, totalling £13,500, was converted into cryptocurrency on 5 August, then converted back into sterling and withdrawn to her account with a bank I'll call M. So, the two payments totalling £13,500 were not sent on to the scammer, they went back to Miss B's bank account with M and Miss B then sent money on from M *back to Revolut*, and then on from Revolut to another cryptocurrency exchange I'll call X, and those payments from Revolut to X also form part of Miss B's claim. So, I'm satisfied that the amount she is claiming from Revolut ought to be £13,500 lower.

I remain satisfied Miss B had control of her cryptocurrency account with X and she made the payments from it, for the reasons given in my provisional decision. The additional evidence she sent me includes an email from X in which it says that at the time the transactions were made, the process for making transactions, such as purchasing and exchanging cryptocurrency, was to send instructions by email from the verified user email address. So while Miss B says that she didn't control the cryptocurrency account with X, she appears to

have been the only one who could actually buy, sell or transfer cryptocurrency from that account by sending emailed instructions from her email account. Indeed, she has confirmed she sent the emails instructing X to make payments.

Most of the points Miss B made in response to my provisional decision concern whether Revolut's interventions were sufficient and whether further and better intervention would have made a difference.

In my provisional decision, I said that I considered Revolut ought to have intervened on further occasions and that on at least one occasion it didn't ask sufficiently probing questions, in my view. However, I considered it unlikely further and better intervention would have uncovered the scam because Miss B hadn't been open with Revolut nor with cryptocurrency exchange S.

Miss B says further intervention, particularly a phone call, would have prevented her losses and uncovered the scam and she says she didn't intentionally mislead Revolut or S. While I've considered this very carefully, I'm not persuaded the evidence suggests it's more likely than not that such intervention would have been effective at stopping this scam.

In my provisional decision, I set out several instances of Miss B giving S inaccurate information when it asked probing questions. I think it's likely Miss B knew that information was inaccurate, for example when S asked whether Miss B was receiving advice from an adviser or broker and she said she was not. While I've considered her comment that she also thought of the adviser as a friend, he was first and foremost an adviser, advising her on her investment. She was also asked by S how she had heard about S and she said she had found it using her own research, but her messages with the scammer show that he found it and recommended she use it.

On 29 July 2024, S asked a series of questions, probing into the payments. It asked Miss B about her general investment strategy and what she intended to do when she withdrew her cryptocurrency to A. She said she was just going to hold onto it in that wallet with A but in fact she had sent previous amounts on to her investment account and it seems fairly clear that was the intention again. Some days later when S asked to see a screenshot from A, the adviser told Miss B to send him the screenshots of her wallet with A so that he could see if he could hide the transactions that had been sent to the investment account. Overall, I think the evidence suggests Miss B ought to have known that much of the information she was providing wasn't accurate.

It's clear the adviser was guiding Miss B throughout. The emails she has provided show the adviser taking her through how to respond to questions from Revolut and S, for example and really leading her step by step. Miss B mentions having no investment experience, a very high degree of trust in the adviser and trust in what she was being told. I've read her comments about how vulnerable she was at the time and I think the adviser was aware of this and cruelly used that to his advantage. I don't doubt that he took time to build a friendship and a sense of trust in Miss B. All the evidence suggests she was deeply taken-in by this scam and I do sympathise with Miss B, who has been the victim of a particularly distressing scam here, but I do consider this makes it less likely, in my view, that any intervention would have been successful.

While it's possible a phone call with Revolut might have made it more difficult for the scammer to coach Miss B on how to respond, I'm not persuaded I can safely conclude that it would have been effective. I think it's more likely, based on the evidence I've seen, given the degree of influence the scammer appears to have had over Miss B, the number of interventions that did take place, the level of coaching and the inaccurate answers that Miss B gave, that any intervention is unlikely to have succeeded.

For those reasons and for those set out in my provisional decision, I don't uphold Miss B's complaint.

My final decision

I don't uphold Miss B's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss B to accept or reject my decision before 31 December 2025.

Greg Barham
Ombudsman