

The complaint

Ms B is unhappy that Revolut Ltd (“Revolut”) didn’t reimburse her after she fell victim to a scam.

Ms B has brought her complaint with the assistance of a professional representative. For ease of reading, I will refer to Ms B throughout this decision.

What happened

The background to this complaint is well known to both parties, so I won’t repeat it all in detail here, but in summary I understand it to be as follows.

During 2023, Ms B has said she had started to hear about investments and how friends had dabbled in cryptocurrency. In April 2023, she came across an advertisement that interested her, which was for an investment, but also included the opportunity to learn how to invest. Ms B has said she checked out the company and found mostly positive reviews and so she expressed an interest.

Ms B was then contacted by somebody, who claimed they were a financial adviser. Believing everything to be genuine, and after completing what she thought were genuine verification checks, Ms B decided to invest. But unknown to her at the time she was dealing with fraudsters.

Ms B made an initial payment of £250, from an account she held with another provider, which she was told was a start-up fee. She was then persuaded by the fraudsters to open a Revolut account, as well as accounts with different cryptocurrency platforms. Ms B moved money to her Revolut account, from accounts she held elsewhere to facilitate payments. She sent payments, totalling £101,780.76, from her Revolut account to the accounts she had set up with cryptocurrency platforms. These payments were subsequently converted into cryptocurrency and ultimately ended up in accounts that were controlled by the fraudsters.

Payment	Date	Type of transaction	Amount
1	05/06/23	Card Payment to Cryptocurrency Platform 1	£5,000
2	05/06/23	Card Payment to Cryptocurrency Platform 1	£5,000
3	20/07/23	Faster Payment to Cryptocurrency Platform 2	£9,780.76
4	13/09/23	Faster Payment to Cryptocurrency Platform 2	£5,000
5	13/09/23	Faster Payment to Cryptocurrency Platform 2	£4,000
	20/09/23	No loss, payment to Ms B’s own account	£10,000
	20/09/23	Failed transaction, to Cryptocurrency Platform 2	£25,000
6	20/09/23	Faster Payment to Cryptocurrency Platform 3	£1,000
7	20/09/23	Faster Payment to Cryptocurrency Platform 3	£47,000
8	21/09/23	Faster Payment to Cryptocurrency Platform 3	£25,000

Ms B realised she'd been scammed after Revolut contacted her on 21 September 2023, by way of its in-app chat, to discuss the activity on her account. Following this, she attempted to make a withdrawal from the investment and was told she couldn't make a withdrawal until she'd paid more money in.

Ms B raised the matter with Revolut, but it didn't agree to reimburse her the money she had lost.

Unhappy with Revolut's response, Ms B brought her complaint to this service. One of our Investigators looked into things and thought the complaint should be upheld in part. In summary, our Investigator thought when Ms B made her first payment, there was enough going on that Revolut should have intervened. It was our Investigator's view that had Revolut done so, by way of providing a tailored warning, it would have made a difference and the scam would have been prevented.

But our Investigator also thought Ms B should bear some responsibility for her loss. In summary, this was because she thought there was enough going on that ought to have led her to have some concerns about the legitimacy of the investment. Overall, our Investigator thought Revolut should refund Ms B 50% of her loss, along with interest.

Ms B agreed with our Investigator's view, but Revolut disagreed. In summary it said;

- Payments to a customer's own account don't meet the definition of an APP scam. It shouldn't be responsible for its customer's loss where it is only an intermediate link in a chain of transactions.
- The role of other financial businesses (including any interventions or warnings they might have provided) needs to be considered.
- The Financial Ombudsman should inform the complainant that it might be appropriate to make a complaint against another respondent.

As agreement couldn't be reached, the complaint has been passed to me for a decision.

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.

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 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. 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 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 Ms B was at risk of financial harm from fraud?

I'm aware that cryptocurrency exchanges, like the ones Ms B made her payments to here, 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. Revolut would likely have been aware of this fact too. So, it could have reasonably assumed that the payments would be credited to a cryptocurrency wallet held in Ms B's name.

By June 2023, when these transactions started, 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. They reached record levels in 2022. During that time, cryptocurrency was typically allowed to be purchased through many high street banks with few restrictions.

By the end of 2022, however, many of the high street banks had taken steps to either limit their customer's ability to purchase cryptocurrency using their bank accounts or increase friction in relation to cryptocurrency related payments, owing to the elevated risk associated with such transactions. And by June 2023, when these payments began, further restrictions were in place. This left a smaller number of payment service providers, including Revolut, who allowed customers to use their accounts to purchase cryptocurrency with few restrictions. These restrictions – and the reasons for them – would have been well known across the industry.

I recognise that, as a result of the actions of other PSPs, many customers who wish to purchase cryptocurrency for legitimate purposes will be more likely to use the services of an EMI, such as Revolut. And I'm also mindful that a significant majority of cryptocurrency purchases made using a Revolut account will be legitimate and not related to any kind of fraud (as Revolut has told our service). However, our service has also seen numerous examples of consumers being directed by fraudsters to use Revolut accounts in order to facilitate the movement of the victim's money from their high street bank account to a cryptocurrency provider, a fact that Revolut is aware of.

So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Ms B made from June 2023, 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.

To be clear, I'm not suggesting that, as a general principle, Revolut should have more concern about payments being made to a customer's own account than those which are being made to third party payees. As I've set out in some detail above, it is the specific risk associated with cryptocurrency in June 2023 that, in some circumstances, should have caused Revolut to consider transactions to cryptocurrency providers as carrying an increased risk of fraud and the associated harm. In those circumstances, as a matter of what I consider to have been fair and reasonable, good practice and to comply with regulatory requirements, Revolut should have had appropriate systems for making checks and delivering warnings before they processed such payments.

With all of this in mind, while I recognise this was a newly opened account and the purpose Ms B had given for opening the account was 'stocks, vaults and crypto', I think, on balance, given the value of the payment and that it was identifiably being made to a cryptocurrency platform, Revolut ought to have identified that Ms B might be at a heightened risk of fraud that merited its intervention from the point she made her first payment.

What did Revolut do to warn Ms B?

I'm aware that Revolut did carry out some interventions on payments Ms B made in July and September, which included chat interventions and presenting educational stories. But, my focus here is on what Revolut did to warn Ms B on the initial payment she made, given that's where, for reasons explained above, I think an intervention ought to have taken place.

Revolut has said that steps were taken as part of the 3DS authentication process for the card payment Ms B made. As well as this, it's said each time Ms B initiated a transfer to a new beneficiary, the following warning was displayed on the payment screen:

"Do you know and trust this payee? If you're unsure, don't pay them, as we may not be able to help you get your money back. Remember, fraudsters can impersonate others, and we will never ask you to make a payment."

What kind of warning should Revolut have provided Ms B?

I've gone on to consider what a proportionate warning in light of the risk presented would be in these circumstances. In doing so, I've taken into account that many payments that look very similar to this one will be entirely genuine. 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 this payment was made.

Taking that into account, I think Revolut ought, when Ms B attempted to make the first payment, knowing (or strongly suspecting) that the payment was going to a cryptocurrency provider, to have provided a warning (whether automated or in some other form) that was specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022. In doing so, I recognise that it would be difficult for such a warning to cover off every permutation and variation of cryptocurrency scams, without significantly losing impact.

So, at this point in time, 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 Revolut ought fairly and reasonably to have provided should have highlighted, in clear and understandable terms, the key features of common cryptocurrency investment scams, for example referring to: an advertisement on social media, promoted by a celebrity or public figure; an 'account manager', 'broker' or 'trader' acting on their behalf; the use of remote access software, visibility of what appeared to be a professional trading platform, the promise of high returns and a small initial deposit which quickly increases in value.

I recognise that a warning of that kind could not have covered off all scenarios. But I think it would have been a proportionate way for Revolut to minimise the risk of financial harm to Ms B by covering the key features of scams affecting many customers, but not imposing a level of friction disproportionate to the risk the payment presented.

If Revolut had provided a warning of the type described, would that have prevented the losses Ms B suffered from the first payment?

I've thought carefully about whether a specific warning covering off the key features of cryptocurrency investment scams would have likely prevented any further loss in this case. And on the balance of probabilities, I think it would have. There were several key hallmarks of common cryptocurrency investment scams present in the circumstances of Ms B's payments, such as finding the investment through an online advertisement, being assisted by an account manager, access to a trading platform, the promise of high returns and being asked to download remote access software.

From the evidence I've seen, I've not found anything that persuades me Ms B was asked, or agreed to, disregard any warning provided by Revolut. I've also seen no evidence that Ms B was provided with warnings by the firm she used to top up her Revolut account.

I'm also satisfied that Ms B wasn't being coached by the fraudster or guided as to how to circumvent any attempts by Revolut to protect her. I say that especially as at one point Ms B tells Revolut that the purpose of one of the later payments (in July) was for 'transfer to a safe account'. I think it's highly unlikely that a fraudster would coach one of their victims to select this purpose for a payment, given this would be such a stark indicator of potential fraud.

I'm mindful that Revolut has said that Ms B chose to give it inaccurate information (in choosing safe account for this later payment). However, I'm not persuaded that Ms B *chose* to give inaccurate information, rather I think she made a genuine choice based on what she thought was right, albeit I accept that there was a better choice available ('investment') to her. But, and importantly, I can't see that Ms B was asked to provide a purpose for the first payment. So, for reasons explained, the most identifiable fraud risk based on what Revolut knew, would have been a cryptocurrency investment scam.

The evidence I've seen, of the in-app chat's that Revolut has had with Ms B satisfy me that when probed she spoke freely about what she was doing, explaining the money was towards crypto. But most importantly, on being presented by Revolut with warnings about investment scams it is evident that it didn't take much, by way of these warnings, for Ms B to heed its advice and to confirm that she would not be sending any more money.

Therefore, on the balance of probabilities, had Revolut provided Ms B with an impactful warning, at the time she made this first payment, that gave details about cryptocurrency investment scams and how she could protect herself from the risk of fraud, I believe it would have resonated with her, as it did later when she was presented with warnings about investment scams. She could have paused and looked more closely into the firm before proceeding, as well as making further enquiries into cryptocurrency scams. I'm satisfied that a timely warning to Ms B from Revolut would very likely have caused her to be more cautious and would have prevented the scam.

Is it fair and reasonable for Revolut to be held responsible for Ms B's loss?

I have taken into account that Ms B seemingly remained in control of her money after making the payments from Revolut. It wasn't lost until she took further steps. But Revolut should still have recognised that Ms B was at risk of financial harm from fraud at the point

she made the first payment, and had it have warned Ms B, in the manner described above, I think it would have ultimately prevented Ms B's loss from that point. I think Revolut can fairly be held responsible for Ms B's loss in such circumstances.

While I have considered all of the facts of the case, including the role of other financial institutions involved, Ms B has chosen not to complain about another firm, and I can't compel her to do so. And I do not think it would be fair to reduce Ms B's compensation because she's only complained about one firm, as I consider that Revolut should have prevented the loss.

Should Ms B 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. Ms B has already accepted the Investigator's opinion that any refund provided should be reduced to account for her own actions as part of the scam. And as I agree with this point, I won't dwell on it.

Except to say that I think the returns being offered, of expecting a profit of double the amount invested, were simply too good to be true, to the point of being implausible. I can't see that Ms B was given, nor sought, clarification of how this was achievable. Alongside this I can't see that there was any formalisation of the agreement, such as any paperwork, which you would reasonably expect to see with a legitimate investment.

Overall, I think it's fair and reasonable for Revolut to make a 50% deduction from the redress payable to Ms B.

Could Revolut have done anything else to recover Ms B's money?

I've also thought about whether Revolut could have done more to recover the funds after Ms B reported the fraud. The first two payments were made by card to a cryptocurrency provider, and that cryptocurrency was sent on to the fraudsters. So, Revolut would not have been able to recover the funds.

In addition, I don't consider, for these card payments, that a chargeback would have had any prospect of success given there's no dispute that the cryptocurrency platform performed its given role in providing cryptocurrency in return for payment.

Similarly, the remainder of the payments were made by faster payment to cryptocurrency providers, before the funds subsequently ended up in the control of the fraudsters. So, there would have been little prospect of Revolut being able to recover any of the money Ms B had sent.

Putting things right

For the reasons explained above, I now direct Revolut Ltd to:

- pay Ms B £50,890.38 (being 50% of the total loss of £101,780.80).
- Apply 8% simple interest per year on that amount from the date of each payment to the date of settlement (if Revolut Ltd deducts tax from this interest, it should provide Ms B with the appropriate tax deduction certificate).

My final decision

My final decision is that I uphold this complaint in part.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms B to accept or reject my decision before 26 September 2025.

Stephen Wise
Ombudsman