

The complaint

Ms C complains that Revolut Ltd (Revolut) won't refund the money she lost as a result of a scam.

Ms C has used a professional representative to bring this complaint to our service and they have made submissions on her behalf. For consistency, I'll refer to Ms C throughout.

What happened

I issued my provisional decision on this complaint on 26 July 2024. I wanted to give both sides a chance to provide any further evidence and arguments before I issued my final decision. That provisional decision forms part of this final decision and is copied below.

What happened

Ms C says she received a message which contained a link showing an online advertisement of a young man on a well-known breakfast TV show. He had supposedly doubled his money through an investment. Ms C can't recall what happened next, but she was in contact with a representative of a trading company (that I'll call T) via email.

Through discussions with T, Ms C understood she would be investing in commodities with varied returns expected. However, she says she was repeatedly guaranteed she would make a profit. She checked T's website, and says she saw positive reviews of T online, and saw nothing to indicate it was a scam. She later clarified, she saw both positive and negative reviews, but more positive. The fraudster also sent Ms C some literature for the investment, including the terms and conditions for the investment and an investment proposal.

Ms C opened a trading account with T through which she could monitor her investment and see her deposits in real time. The fraudster persuaded Ms C to download remote access software to her device, which enabled them to guide Ms C through opening accounts and investing.

Ms C started with a small initial investment from her account with another provider (Bank B). This was a £210 card payment on 23 August 2022 to a merchant which appears to be a trading academy based overseas. On 25 August 2022, Ms C opened a Revolut account under the instructions of the fraudster, for the purposes of making the payments. She told Revolut when she opened the account that the purpose for doing so was 'vaults, stocks, crypto'. She made the following payments as part of the scam:

<i>Date</i>	<i>Event</i>	<i>Amount</i>
<i>30 August 2022</i>	<i>Card payment to B*</i>	<i>-£2,581.45</i>
<i>21 September 2022</i>	<i>Transfer to F*</i>	<i>-£5</i>
<i>22 September 2022</i>	<i>Transfer to F</i>	<i>-£5</i>
<i>24 September 2022</i>	<i>Transfer to F</i>	<i>-£5</i>

28 September 2022	Credit from F	+£5
29 September 2022	Credit from F	+£5
5 October 2022	Credit from F	+£5
6 October 2022	International transfer to S*	-£5,275.33

**B, F and S are all legitimate cryptocurrency providers that Ms C sent funds to, in order to purchase cryptocurrency, and send this on to the fraudster.*

On 15 November 2022, Ms C received a return of £174.52 into her Bank B account. On 25 November 2022, she proceeded to send a further £10,000 from her Bank B account to the investment. That payment doesn't form part of her complaint about Revolut.

Ms C says when it came to withdrawing her investment funds, she was asked to pay multiple fees which she didn't pay. And when all communication stopped, she realised she had been scammed. Bank B says she reported the scam to them on 23 January 2023. However, Revolut says it was first made aware that Ms C had been scammed, when it received a letter of complaint dated 4 July 2023.

Revolut declined to reimburse Ms C for the following reasons:

- *The card payment of £2,581.45 could not have been completed without Ms C's authorisation, as 3DS verification was used to approve the payment. This required Ms C to log into her Revolut app and authorise the payment, so it rejected her chargeback claim.*
- *The transfers were authorised by Ms C, and she received a warning when making the first transfers to each new beneficiary. She could not have proceeded without acknowledging this warning. The given warning raised awareness about the risks of sending funds to unknown parties.*
- *Ms C didn't provide sufficient information for Revolut to consider her scam claim. It asked her to get back in touch with some specific evidence, but she did not respond.*
- *Ms C didn't do sufficient research into T, and there were several elements which ought to have concerned Ms C such as being pressured, cold-called, the use of a social media messenger service, and remote access software.*

Ms C referred her complaint to our service and our Investigator didn't uphold it. They didn't agree that Revolut missed an opportunity to prevent Ms C's loss as they didn't think Ms C would have positively engaged with the warning he'd recommended. They also noted as the funds were sent to cryptocurrency providers who provided a service, Revolut would not have been able to recover Ms C's funds.

Ms C didn't agree with this outcome. She said:

- *The reason for the account opening should be used to identify money laundering, not as a defence against authorised push payment (APP) fraud.*
- *If Revolut have used this to justify lack of intervention, they are knowingly allowing APP fraud providing the account opening reason is aligned with the fraudster's story.*
- *Had the payments been made through another account, they would have been considered out of character and warranted an intervention.*
- *The larger payment was an international payment, which doesn't carry less risk than a cryptocurrency payment. And this justified an intervention, as it was not in line with the account opening purpose.*
- *Revolut didn't ask probing questions or give an effective warning.*
- *There is no reason why Revolut should not have provided a warning that was suitable to the scam type, and no evidence to suggest Ms C wouldn't have heeded such a warning.*

As no agreement could be reached, this case was passed to me for a decision to be issued.

What I've provisionally 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 at the time of the scam, 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 including in relation to card payments);*
- 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.*

In light of the above, I've considered whether Revolut acted fairly and reasonably in its dealings with Ms C.

Firstly, I've thought about whether the payments identified Ms C might be at a heightened risk of financial harm due to fraud or a scam. I note the following:

- The account was newly opened so Revolut didn't know what would constitute as 'typical account usage' for Ms C. But the nature of the disputed activity aligned with what Ms C told the account would be used for, when she opened it. I think that this might have reasonably given Revolut some re-assurances.*
- Ms C's statements also shown cryptocurrency related transactions amongst the disputed payments, through Revolut's own cryptocurrency facility. Ms C has no recollection of what these relate to, and they don't form part of her complaint. But I can see why this activity, and the payments made to B and F, appeared to be consistent with the declared purpose of the account.*
- The values of the first four payments were not remarkable enough to have caused Revolut any concern. Nor do I consider enough of a pattern formed here to suggest Ms C might be at a heightened risk of financial harm due to fraud or a scam. I'm not persuaded Revolut reasonably ought to have been concerned about payments 1-4.*
- The final payment was an international transfer, which carries an enhanced risk due to the difficulty in recovering funds overseas. In combination with the payment value, I think, at this point, Revolut ought to have taken steps to provide Ms C with a written*

warning about the payment she was making, before allowing it to be made. In doing so, it should have attempted to tailor the warning to a particular scam risk, such as by asking Ms C to provide a payment purpose for the transaction she was making.

However, whilst I think Revolut ought to have given Ms C a more specific warning, I don't think any proportionate intervention by Revolut would have prevented Ms C's loss. I'll explain why.

I've reviewed evidence of a phone call Ms C had with Bank B when she attempted to make a £10,000 payment towards the scam from her Bank B account. Ms C told Bank B the payment was for 'investment or crypto-currency' when she created the payee on her online banking, and she'd received an online written warning relevant to this scam risk. The payment was flagged by Bank B's fraud monitoring systems and Ms C had to discuss this with Bank B before the payment could be released.

During this phone call, Ms C told Bank B the following:

- She was investing in bitcoin and was quite happy as it had been going well.*
- She had full faith in what she was doing and had been advised about the investment by her father. She was relying on his advice rather than her own research.*
- No one, other than her father, helped her open the account with a cryptocurrency provider so she could access her bitcoin.*
- No one had instructed her to open the account, and she didn't give remote access to her device, nor had she shared access to her account with anyone else.*
- She wasn't dealing with a third party, such as a broker, to make the investment.*
- She had friends who had invested this way too, and she hadn't been rushed into the decision.*
- She was aware of the risks involved in the investment and she could afford to lose the money should the investment not work out.*

Not all of the information Ms C gave Bank B was accurate, based on what Ms C has told our service. This is also supported by the evidence of her correspondence with the fraudster, which shows she had been pre-warned about such calls from the bank. And she was told to say she was using software her family recommended and helped her install.

In this call, Bank B attempted to highlight some of the risks associated with the payment, such as the beneficiary (F) not being regulated in the UK and that her money was not protected. However it's clear from listening to the call that Ms C thought that Bank B's real reason for intervening was because they didn't want customers involved in bitcoin investments as they didn't want people to make money. This is what she had been led to believe that by the fraudster.

Bank B did also give context to the questions and explained it was to prevent her being scammed. It also warned her of the consequences of proceeding and highlighted the importance of checking that it was a legitimate investment. However, Ms C confirmed she was happy in her trust in the investment company and asked Bank B to release the payment.

Taking these things into account, I think it's highly unlikely that a written warning from Revolut, which is the most I'd have expected it to do when Ms C made the final payment, would have made any difference to Ms C's decision to proceed with the payment. In fact, I can see that despite Ms C reporting the scam to Bank B in January 2023, she continued communicating with the scammers until March 2023, as she was still hoping she would be able to withdraw her money. In her own words, Ms C had 'full faith that her money was in good hands', so I don't believe Revolut's failure to provide a more in-depth written

warning about investment scams, had a material impact on preventing Ms C's loss. And so, I can't fairly or reasonably hold Revolut liable for Ms C's loss.

Recovery of funds

I'm not persuaded Revolut could have done more to recover Ms C's funds sent to B and S. The card payment to B went to a legitimate cryptocurrency exchange – not the fraudster. B provided the goods and services Ms C paid for – namely the transfer of funds and/or provision of cryptocurrency. So, I'm not persuaded there was any reasonable prospect of a chargeback succeeding in these circumstances.

The transfer Ms C made to S – another legitimate cryptocurrency exchange - went overseas, which makes it much more difficult to recover funds. International banks aren't obliged to follow UK rules, regulations and best practice on recovery of funds. And recovery attempts are often subject to local laws and rules. Ms C has also confirmed she made the transfer to purchase cryptocurrency which she sent to what she thought was her trading wallet, confirming she received what she paid S for. So again, there wasn't any realistic prospect of recovering Ms C's money.

My provisional decision

For the reasons I've explained above, I do not intend to uphold this complaint.

Ms C did not accept my provisional decision; however she had nothing further to add. Revolut did not respond.

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.

As neither party have provided any new comments or evidence for me to consider, my final decision is unchanged from the provisional findings I've set out above.

My final decision

For the reasons I've explained above, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms C to accept or reject my decision before 27 September 2024.

Meghan Gilligan
Ombudsman