

The complaint

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

What happened

Miss M says that on 18 September 2023 she received a call from someone who said they were from Revolut. She didn't know at the time, but the caller was a scammer. The scammer told Miss M that an insurance company was trying to take funds from her account and asked her how much money she had in the account and about her latest transaction.

The scammer told Miss M that a new account would be opened to keep her money safe and to send funds to that account. Miss M authorised a card payment of £4,025 in the belief that the funds were going to her account. The scammer then told Miss M to delete the call log and hung up.

Miss M reported what had happened to Revolut.

Revolut didn't agree to reimburse Miss M. It said it couldn't raise a chargeback dispute as it was authenticated via the 3DS authentication system.

Miss M was unhappy with Revolut's response and brought a complaint to this service. She said she was the victim of a scam and should be reimbursed.

Our investigation so far

The investigator who considered this complaint recommended that it be upheld in part. He said that Revolut should have recognised that the payment was to a cryptocurrency provider and in view of the increased risk posed by such payments asked a series of questions to attempt to narrow down the scam risk. Once the scam risk had been identified, the investigator said that Revolut should have provided a warning that covered off the key features of the scam risk identified. If this had happened, and a safe account warning been provided, Miss M's loss could have been prevented. But the investigator said Miss M should share responsibility for her loss.

Revolut didn't agree with the investigator's findings. It said the transactions were 'self-to-self' and Revolut was only an intermediate link, so wasn't liable.

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 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.

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 in September 2023 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;
- 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;
- 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 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 Miss M was at risk of financial harm from fraud?

It isn’t in dispute that Miss M has fallen victim to a cruel scam here, nor that she authorised the payment via 3D secure authentication. The payment was made to a provider of cryptocurrency.

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 transaction Miss M made would be credited to a cryptocurrency account in her own name.

But by September 2023, when this payment was 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. They reached record levels in 2022. During that time, cryptocurrency was typically allowed to be purchased through many high street banks with few restrictions.

So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Mr C made in September 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.

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. And, as I've set out, the introduction of the FCA's Consumer Duty, on 31 July 2023, further supports this view. The Consumer Duty requires Revolut to avoid causing foreseeable harm to its customers by, among other things, having adequate systems in place to detect and prevent scams.

Taking all of the above into account, and in light of the increase in multi-stage fraud, particularly involving cryptocurrency, I don't think that the fact the payment in this case was likely going to an account held in Miss M's own name should have led Revolut to believe there wasn't a risk of fraud.

I think Revolut ought reasonably to have identified that the payment carried a heightened risk of harm given its size and that it was going to an identifiable provider of cryptocurrency.

What did Revolut do to warn Miss M?

Revolut didn't provide any warnings to Miss M.

What kind of warning should Revolut have provided?

I've thought carefully about 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.

As I've set out above, the FCA's Consumer Duty, which was in force at the time these payments were made, requires firms to act to deliver good outcomes for consumers including acting to avoid foreseeable harm. In practice this includes maintaining adequate systems to detect and prevent scams and to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers.

I'm mindful that firms like Revolut have had warnings in place for some time. It, along with other firms, has developed those warnings to recognise both the importance of identifying the specific scam risk in a payment journey and of ensuring that consumers interact with the warning.

In light of the above, I think that by September 2023, when this payment was made, Revolut should have had systems in place to identify, as far as possible, the actual scam that might be taking place and to provide tailored effective warnings relevant to that scam for both APP and card payments. I understand Revolut did have systems in place to identify scam risks associated with card payments which enabled it to ask some additional questions and/or provide a warning before allowing a consumer to make a card payment.

I accept that any such system relies on the accuracy of any information provided by the customer and cannot reasonably cover off every circumstance. But I consider a firm should by September 2023, on identifying a heightened scam risk, have taken reasonable steps to attempt to identify the specific scam risk – for example by seeking further information about the nature of the payment to enable it to provide more tailored warnings.

In this case, Revolut knew the payment was being made to a cryptocurrency provider and its systems ought to have factored that information into the warning it gave. Revolut should also have been mindful that cryptocurrency scams have become increasingly varied over the past

few years. Fraudsters have increasingly turned to cryptocurrency as their preferred way of receiving a victim's money across a range of different scam types, including 'romance', impersonation and investment scams.

Taking that into account, I am satisfied that, by September 2023, Revolut ought, fairly and reasonably, to have attempted to narrow down the potential risk further. I'm satisfied that when Miss M made the payment, Revolut should – for example by asking a series of automated questions designed to narrow down the type of cryptocurrency related scam risk associated with the payment she was making – have provided a scam warning tailored to the likely cryptocurrency related scam Miss M was at risk from.

In this case, Miss M was falling victim to an impersonation scam – she believed she had been contacted by Revolut and she was making a payment to keep her funds safe.

As such, I'd have expected Revolut to have asked a series of simple questions to establish that this was the risk the payment presented. Once that risk had been established, it should have provided a warning which was tailored to that risk and the answers Miss M gave. I'd expect any such warning to have covered off key features of such a scam, such as receiving out of the blue contact, a request to move funds to a 'safe' account or to help with an investigation, number spoofing and remote access.

I acknowledge that any such warning relies on the customer answering questions honestly and openly, but I've seen nothing to indicate that Miss M wouldn't have done so here.

If Revolut had provided a warning of the type described, would that have prevented the loss Miss M suffered?

I think that a warning of the type I've described would have resonated with Miss M and prevented her from making the payment. She believed that she was following Revolut's instructions so if Revolut told her it would never ask her to move her money Miss M would have had concerns about what she was being asked to do. She has explained that she wasn't given a cover story or told to lie.

Is it fair and reasonable for Revolut to be held responsible for Miss M's loss?

In reaching my decision about what is fair and reasonable, I have taken into account that Miss M purchased cryptocurrency which it appears credited an e-wallet held 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 payment 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 Miss M might have been at risk of financial harm from fraud, 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 Miss M suffered. The fact that the money wasn't lost at the point it was transferred to Miss M's own account does not alter that fact and I think Revolut can fairly be held responsible for Miss M'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.

For the reasons I have set out above, I am satisfied that it would be fair to hold Revolut responsible for Miss M's loss (subject to a deduction for Miss M's own contribution which I will consider below).

Should Mrs M bear any responsibility for her loss?

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.

Whilst I recognise that Miss M made the payment in the heat of the moment and because she feared for the safety of her funds, on balance, I consider a 50% deduction is fair and reasonable in all the circumstances of this case. Miss M received out of the blue contact with no caller ID from someone who said they were from Revolut. This person asked Miss M questions about her balance and recent transaction(s) – information that a member of staff at Revolut would know. And Miss M didn't take any steps to confirm that the caller really was from Revolut. I also can't see why Revolut would ask Miss M to make a card payment in the manner she did.

Overall, I consider it fair to reduce the amount Revolut pays Miss M to reflect the role she played in what happened.

My final decision

I uphold this complaint and require Revolut Ltd to:

- Pay Miss M £2,012.50; and
- Pay interest on the above amount at the rate of 8% simple per year from the date of the transaction to the date of settlement.

If Revolut Ltd considers that it is required by HM Revenue & Customs to deduct income tax from that interest, it should tell Miss M how much it has taken off. It should also give Miss M a tax deduction certificate if she asks for one, so she can reclaim the tax from HM Revenue & Customs if appropriate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss M to accept or reject my decision before 11 March 2025.

Jay Hadfield
Ombudsman