

The complaint

Miss S complains that Revolut Ltd ('Revolut') did not reimburse the funds she says she lost to a scam.

What happened

In August 2025, Miss S was contacted on a well-known messaging service about a job opportunity by someone posing as recruiter. The job involved completing tasks for which she would receive commission but also involved having to pay to complete the tasks.

Miss S was guided through how to complete the tasks, given access to a professional looking platform and at one point was instructed to open a cryptocurrency wallet with a legitimate and well-known cryptocurrency provider.

I've set out the transactions Miss S sent from her Revolut account below:

Payment number	Date	Details	Amount
1	11 August 2025	Payment to M (an individual)	£30
2	12 August 2025	Payment to S (an individual)	£50
3	12 August 2025	Payment to S (an individual)	£50
4	12 August 2025	Payment to M (an individual)	£150
5	13 August 2025	Payment to Miss S's own crypto wallet	£380
6	13 August 2025	Payment to Miss S's own crypto wallet	£1,200

In total, Miss S sent £1,860 towards the scam. But Miss S also received several payments from M and S into her Revolut account, coming to a total of £239. So, Miss S's outstanding loss is £1,621.

Soon after the last payment, Miss S realised she'd been the victim of a scam and reported the payments to Revolut. Revolut investigated but didn't refund Miss S. It referred to a £100 excess it can apply, subject to certain conditions, to scam claims that fall under the Faster Payments Scheme (FPS) reimbursement rules – in this case, the first four payments. It also said the payments to Miss S's crypto wallet were not covered by the FPS reimbursement rules, that it had provided sufficient scam warnings and it had done everything to recover Miss S's funds. Unhappy with Revolut's response, Miss S referred her complaint to our service.

One of our Investigators looked at the complaint. They thought Revolut had acted reasonably in applying the excess and didn't think we'd have expected Revolut to have done anything further when Miss S made any of the payments. So, they didn't think Revolut should have to refund any of the money Miss S lost.

Miss S disagreed with our Investigator. In short, she doesn't think the excess should apply because her circumstances at the time meant she was vulnerable, the payments received from M and S shouldn't be included as part of her net loss, that Revolut's intervention wasn't sufficient given the risk indicators and that she should be reimbursed her outstanding loss.

As the complaint has not been resolved informally, it has been passed to me for a final 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.

I have summarised this complaint in less detail than the parties involved. I want to stress that no discourtesy is intended by this. If there is a submission I have not addressed, it is not because I have ignored the point. It is simply because my findings focus on what I consider to be the central issues in this complaint.

Having considered all the available evidence, I broadly agree with the conclusions reached by the Investigator. I'll explain why.

In deciding what's fair and reasonable in all the circumstances of a complaint, I'm required to take into account relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the time.

In broad terms, the starting position in law is that a firm is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. However, where the customer made the payment as a consequence of the actions of a fraudster, it may sometimes be fair and reasonable for the firm to reimburse the customer even though they authorised the payment.

The payments to "M" and to "S"

The Payment Systems Regulator (PSR) introduced the FPS reimbursement rules on 7 October 2024 to reimburse consumers who are the victims of Authorised Push Payment (APP) scams in certain circumstances. And it's not in dispute that the payments Miss S made to accounts held by M and by S are covered by these rules. So I've considered whether Revolut has fairly considered the claim under the FPS reimbursement rules.

There are limits on what firms are expected to refund under the rules, one of which is that firms can apply an optional excess of £100 per claim. The rules say that, where a claim satisfies the criteria for reimbursement:

"The value of the Reimbursable Amount to be credited to the Victim shall be the full value of all Reimbursable FPS APP scam payments, up to the maximum level of reimbursement and less any claim excess imposed."

And the PSR has confirmed that:

"Sending PSPs may apply an excess up to a maximum of £100 per claim."

In Miss S's case, she paid £280 in total to M and to S. These are the Reimbursable FPS APP scam payments as per the FPS reimbursement rules. But Miss S also received a total of £239 from M and S. I understand that the payments Miss S received were all part of the scam and a way of creating trust and ultimately getting her to send more funds. But the payments from M and S were received by Miss S, into her Revolut account and must be taken into account when considering the value of the Reimbursable Amount.

The FPS reimbursement rules only apply to the payments Miss S made to M and S. Because she received funds back from M and S, the full value of the reimbursable scam payments comes to £41. The excess Revolut applied was £100. Because the excess is larger than the value of the reimbursable payments, and it can be deducted from the reimbursable payments, the value of the reimbursable amount comes to £0.

With that in mind, I think Revolut has acted reasonably in interpreting the FPS reimbursement rules in this way and in saying it does not have to refund any money to Miss S under these rules.

But there is a further consideration when considering whether it is fair to apply the excess. The rules explain that the excess can't be applied if the consumer was vulnerable at the time of making at least one payment falling within the claim – and their vulnerability had a material impact on their ability to protect themselves from the scam. I've thought carefully about whether Miss S should be deemed a Vulnerable Consumer under the definition set by the rules, which defines this as:

“...someone who, due to their personal circumstances, is especially susceptible to harm – particularly when a firm is not acting with appropriate levels of care.”

Miss S has kindly told us about some difficult personal circumstances affecting her at the time of the scam which she says made her especially susceptible to harm, and in particular the type of scam she fell victim to. I'm sorry that Miss S was experiencing a very difficult time personally and financially at the time of the scam. And I acknowledge the negative impact the scam has had on Miss S since. But having carefully considered the information available to me, I agree with the investigator that her circumstances didn't materially impact her ability to protect herself from the scam she fell victim to. For example, Miss S confirmed she was able to complete some checks on the company and the materials she'd been sent and checked online and found similar job-task opportunities being discussed. This indicates she was able to take steps to try and protect herself. It's just that unfortunately, those checks didn't make it clear it was a scam. Overall, while I'm sorry to hear about the difficulties Miss S was experiencing, I'm not persuaded Miss S was vulnerable in a way that materially affected her ability to protect herself from the scam. I'm therefore satisfied it's fair for Revolut to apply the excess to her claim.

I've also thought about whether Revolut should reasonably have been able to prevent the scam from occurring. There are some situations where I'd reasonably expect a firm to make further enquiries about a payment before deciding whether to process it – such as where there are grounds to suspect it presented a fraud risk. If a firm failed to respond proportionately to such a risk, and doing so would have prevented the consumer from incurring a fraudulent loss, it may be fair to hold it liable.

In this case, I don't think the payments to M and to S would reasonably have looked particularly suspicious to Revolut. The payments weren't for especially large amounts, were being sent to individuals and weren't out of character when compared to Miss S's usual account activity. Miss S also received payments from both recipients before she made payments to them, and in between the payments to them – making the outward payments look less likely to be a risk of fraud. I therefore consider it reasonable that Revolut processed the payments in line with Miss S's authorised instructions without completing further checks.

I also don't think anything I would reasonably have expected Revolut to have done would have led to any of Miss S's funds being recovered from the accounts they were sent to. Miss S received more money from M's account than she sent to it so there wouldn't have been anything more to recover from that account. And I've seen evidence that the funds she sent

to S were promptly moved on from the account paid, and before Miss S reported the matter to Revolut. So I don't think Revolut missed an opportunity to recover Miss S's losses.

The payments to Miss S's crypto wallet

The FPS reimbursement rules only apply to faster payments or CHAPS payments, sent to an account that the victim does not control. Payments five and six were transfers to Miss S's own crypto wallet. From there, Miss S converted her funds into cryptocurrency which was then sent to an external wallet held by the scammer. I appreciate that Miss S was following the instructions of the scammer when she opened the wallet and transferred crypto to them. But Miss S has confirmed that she opened the crypto wallet herself, didn't share the login details with anyone else and had full control of the wallet. So the two payments made to her crypto wallet aren't covered by the FPS reimbursement rules.

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;
- 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 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

So I've considered whether Revolut should have identified that Miss S was at heightened risk of financial harm from fraud as a result of the transfers to her own crypto wallet.

In this case, I'm not convinced there was enough about the first payment, looking at its value and what Revolut would have known about the payee, for it to have intervened on suspicion that Miss S was at a heightened risk of financial harm from fraud.

I realise the Revolut account was not newly opened and that Miss S hadn't made payments to a cryptocurrency provider before. But the recipient was a genuine and well-known cryptocurrency provider and it's not uncommon for consumers to make one-off and relatively small payments to cryptocurrency providers from time to time. And, in the absence of other significant factors, I don't think it was unreasonable for Revolut to have processed the payment after providing Miss S with a 'new payee' warning which said "*Do you know and trust this payee? If you're unsure don't pay them. As we may not be able to help get your money back. Remember, fraudsters can impersonate others and we will never ask you to make a payment*".

For the second payment to Miss S's crypto wallet, Revolut has sent us evidence to show that it did intervene. Miss S was told that it was important to answer Revolut's questions honestly and that if she was being told what to say, or to act quickly then the transaction may be a scam. Miss S was asked, in the automated payment flow, to provide a 'payment purpose' before it was processed. Miss S selected 'Investment'. In turn, she was asked further questions and shown warnings about investment scams. Though the warnings weren't specific to the job task scam Miss S was falling victim to, parts of the warnings were relevant and I can see from the chats with the scammer that Miss S challenged the scammer about some of the information Revolut gave her. Miss S was also asked questions and given warnings related to being given instructions by somebody else, how she found out about the opportunity and what checks she'd carried out.

I understand Miss S selected the "investment" option as the purpose of the payment and answered Revolut's questions following the instructions of the scammer throughout. But I don't think the steps Revolut took in trying to establish if a possible scam might be taking place, were disproportionate to the payment risk presented. And I can't overlook Miss S's replies to the automated questions in the payment flow didn't lead naturally to Revolut being able to provide her with a warning relevant to the exact situation at the time. With that in mind, I don't think it would be fair and reasonable to hold Revolut liable for the payments made to Miss S's crypto wallet.

Because the funds were sent to Miss S's own crypto wallet and then sent onwards from there, there weren't any funds to recover from the wallet. So, I don't think Revolut missed an opportunity to recover Miss S's funds.

I know Miss S feels strongly about this matter. She has explained how her personal circumstances have been affected in the aftermath of this scam and I'm truly sorry to hear about the effect it's had on her. While I appreciate it will have been difficult to have pursued this matter, it is ultimately the cruel actions of the scammer, rather than any failings by Revolut, that is the main cause of this. In the circumstances, I'm not persuaded it would be fair to require Revolut to do more to resolve her complaint.

My final decision

For the reasons set out above I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss S to accept or reject my decision before 21 May 2026.

Mike Southgate
Ombudsman