

The complaint

Miss B complains that Revolut Ltd ('Revolut') won't refund the money she lost after falling victim to a scam.

What happened

The details of this complaint are well known to both parties, so I won't repeat them again here. Instead, I'll focus on giving my reasons for my decision.

In summary, Miss B fell victim to a job scam. She found a job opportunity online that involved the completion of tasks. When Miss B couldn't afford to send any more money, she was unable to withdraw her earnings, and realised it was a scam.

These are the payments Miss B made as part of the scam from her Revolut account.

Date	Details of transaction	Amount
17.6.2025	Card payment to C – a cryptocurrency exchange	£259
18.6.2025	Faster payment to C1 – a cryptocurrency exchange	£500
18.6.2025	Card payment to C – a cryptocurrency exchange	£1,314
18.6.2025	Faster payment to C1 – a cryptocurrency exchange	£980
19.6.2025	Card payment to C – a cryptocurrency exchange	£2,340

Miss B raised a fraud claim with Revolut, asking that they refund her. Revolut declined to refund Miss B saying the payments were made to accounts in her own name, so they aren't liable for her loss. Also, Miss B isn't eligible for chargeback on the card payments as they were authorised.

Miss B wasn't happy with Revolut's response, so she brought a complaint to our service.

An investigator looked into Miss B's complaint but didn't recommend that Revolut refund her. The investigator felt Revolut's intervention on the first two payments was proportionate, in providing onscreen warnings based on the payment purpose Miss B selected. However, the investigator felt Revolut should've identified that the payments were related to cryptocurrency and provided a warning tailored to cryptocurrency scams. The investigator highlighted that Miss B was coached by the scammer in selecting the payment purpose and in answering the onscreen questions Revolut asked, so they thought it was unlikely Revolut could've uncovered the actual scam type Miss B had fallen victim to.

Miss B disagreed with the investigator's opinion and asked for an ombudsman to review her case. Miss B raised the following points:

- She was manipulated by an organised criminal network who used coercion and impersonation tactics to gain her trust.
- She only made the payments as she was desperate to regain the funds.

- Miss B doesn't agree that automated warnings meet the duty of care Revolut owes to its customers.

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; codes of practice and, where appropriate, what I consider to have been good industry practice at the time.

Where there is a dispute about what happened, and the evidence is incomplete or contradictory, I've reached my decision on the balance of probabilities. In other words, on what I consider is more likely than not to have happened in light of the available evidence.

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.

I'm really sorry that Miss B fell victim to such a cruel scam and that she's lost her life savings. And, while I sympathise with Miss B's position, being the victim of a scam doesn't necessarily mean that Revolut are liable for her loss.

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 June 2025 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.

By June 2025, Revolut should've recognised that there was a significantly elevated risk of fraud with payments related to cryptocurrency. And, in response to identifying a potential risk of fraud, Revolut should've asked a series of questions to establish the specific type of scam. Revolut say they had concerns about payments one and two and, based on answers

Miss B gave, they provided onscreen warnings.

Taking into account the size of the payments, the total number of payments, and that the payments were spread out over a couple of days, I'm satisfied that it was appropriate for Revolut's intervention to be onscreen warnings tailored to the scam type identified in response to their questions.

However, Miss B has told us that the scammer was coaching her in how to answer Revolut's questions, which is more likely than not why she chose the payment purposes related to "sending money to her own account" (for payment one) and "paying a family member or friend (for payment two). There was a more relevant purpose relating to paying for a job, but Miss B didn't select this.

Because of the payment purposes Miss B selected, the onscreen warnings she was shown weren't relevant to her circumstances. However, both onscreen warnings included a warning that "the fraudster may ask you to hide the real reason for this payment".

Even if I was satisfied that Revolut should've intervened on other payments Miss B made, besides payment one and two, I'm not satisfied that I can fairly say the scam would've been uncovered or Miss B's loss prevented. I say this because it's more likely than not the scammer would've guided Miss B on what payment purpose to select in order to circumvent Revolut's system from identifying the correct scam type. So, I'm not persuaded that Revolut asking onscreen questions would've identified that Miss B was the victim of a job scam and allowed them to provide a more relevant warning.

I appreciate that Miss B feels onscreen warnings aren't appropriate and don't meet Revolut's duty of care. But, in some circumstances, onscreen warnings are proportionate and appropriate. In this case, I'm not satisfied that I can't fairly say Revolut's intervention should've gone beyond onscreen warnings.

I appreciate that this was a lot of money for Miss B, but Revolut has to find a balance between identifying payments which could be fraudulent and then responding appropriately to their concerns - while ensuring minimal disruption to legitimate payments.

Having carefully considered all of the evidence, I'm not satisfied that I can fairly hold Revolut liable for Miss B's loss or ask them to refund her.

My final decision

My final decision is that I don't uphold this complaint against Revolut Ltd.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss B to accept or reject my decision before 3 March 2026.

Lisa Lowe
Ombudsman