DRN-5376060

The complaint

Miss S is unhappy that Revolut Ltd won't reimburse money she lost to a scam.

What happened

The background to this complaint is well known to both parties, so I won't repeat everything here. In summary, Miss S has explained that between October 2023 and November 2023 she made payments from her Revolut account towards an investment which she ultimately lost to a scam.

Miss S said she saw an advert on social media promoting the investment. She provided her details to the company and was called by the scammers shortly afterwards. She has told us she spoke to two scammers on the day. She highlighted to the first caller that she thought the investment was a scam. A few minutes later she was contacted by a different person who she says was professional and convinced her to invest. Miss S says she was given access to a platform and believing this was a legitimate investment she made the following payments.

Transaction number	Date	Type of Transaction	Amount
1	25 October 2023	Transfer to cryptocurrency exchange	£200
2	9 November 2023	Transfer to cryptocurrency exchange	£5,000
3	14 November 2023	Cryptocurrency exchange to EUR	£5,000
4	14 November 2023	Transfer to third party company	€ 5,677.01

Miss S sent her first two payments to a legitimate cryptocurrency firm – "P". From P, Miss S's funds were converted into cryptocurrency and sent to the scammers. Miss S also exchanged some funds before transferring the money to a third-party account provided by the scammer.

Miss S raised a complaint with Revolut. It investigated the complaint but didn't uphold it. It didn't think it had done anything wrong by allowing the payments to go through. So, Miss S brought her complaint to our service.

Our Investigator looked into the complaint but didn't uphold it. Our Investigator explained that Revolut had provided warnings to Miss S before releasing some of the payments, but she provided incorrect information when asked about one of the payments. He thought the actions taken by Revolut were proportionate to the risk it identified.

Miss S didn't agree, so her complaint has been passed to me for review and a final decision. Your text here

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'm sorry to disappoint Miss S, but I'm not upholding her complaint - for broadly the same reasons as the Investigator.

I've thought about the Contingent Reimbursement Model Code (CRM Code) which can offer a potential means of obtaining a refund following scams like this one. But as Revolut isn't a signatory of the CRM Code, these payments aren't covered under it. I've therefore considered whether Revolut should reimburse Miss S under any of its other obligations.

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 in October and November 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.

Given what Revolut knew about the payments, I've thought about at what point, if any, it ought to have identified that Miss S might be at a heightened risk of fraud.

Revolut says that when new payees were set up it provided Miss S with a warning that said:

"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."

Revolut didn't intervene on Transaction 1. I'm conscious that this payment was relatively modest so I can't see any reason for Revolut to have been particularly concerned about it. A payment of this size is unlikely to have appeared unusual to Revolut. So, I don't think this payment alone would have indicated that Miss S might be at risk of financial harm from

fraud, and I think the new payee warning it presented was proportionate in the circumstances of this payment.

However, when Miss S sent Transaction 2 to P Revolut recognised this was a high-risk payment and provided Miss S with advice and warnings to try and protect her from being scammed. I think Revolut was right to be suspicious of this payment given the amount and what it knew about the destination of the payment. So, I would have expected it to take additional steps, such as asking a series of questions through an automated warning in an attempt to narrow down a possible scam risk. And given Miss S was falling victim to a cryptocurrency investment scam, I consider that a warning highlighting some of the key aspects of such scams would have been an appropriate response here, without imposing a level of friction disproportionate to the payment risks presented.

As referred to by the Investigator, Revolut did take some steps to establish whether there was a possible scam risk on Transaction 2, so it could then provide a warning tailored to the risk identified.

Before this transaction was processed Miss S was asked a series of questions. Revolut stated that she should answer truthfully and that if she was being scammed the fraudster may ask her to hide the real reason for the transaction. I have set out below some of the questions Miss S was asked and the responses she provided:

Revolut	***"Is anyone telling you how to answer these questions?"*** ***"Is someone telling you which options to choose or telling you this is urgent?"***
Miss S	*"No, I am not being assisted through this questionnaire."*
Revolut	***"Why are you making this transfer?"*** ***"We'll only use this information to help protect your account."***
Miss S	*"As part of an investment."*
Revolut	***"What kind of investment?"*** ***"This helps us identify your level of risk."***
Miss S	*"Gains from cryptocurrency."*
Revolut	***"Have you been asked to install software?"*** ***"Scammers might ask you to install software (e.g. Any desk) to view your screen, spy on your personal details and help you to set up your investment account."***
Miss S	*"No, I was not asked to install any software."*
Revolut	***"How did you discover this opportunity?"***
Miss S	*"Friend or Family member."*
Revolut	***"Have you ever invested in crypto?"***
Miss S	*"Yes, I've invested in crypto before?"*
Revolut	***"Have you researched the company?***
Miss S	*"Yes- I checked if the firm is on the FCA Register."*
Revolut	***"Is the transfer to an account you control?"***
Miss S	*"Yes, it's my existing account."*

Following Miss S's responses Revolut then provided a number of warnings tailored to the answers Miss S provided which gave the option for her to pause and reflect on the transfer.

This included highlighting this could be a crypto scam, beware of social media promotions, don't give anyone remote access, do your crypto research and don't be rushed. Revolut took an additional step and put Miss S through to a 'live' agent who discussed the payment further. The agent made it clear to Miss S that her money might be at risk if she made the transfer and that it or another financial institution would never guide a customer to make a payment or ignore payment alerts, and that if someone was telling her to do this then it's likely to be a scam. I think these warnings highlighted several key features which applied to Miss S's payment so the information should have resonated with her.

Miss S has argued that had Revolut probed her further it's likely the scam would have been uncovered. Miss S would have preferred a call from Revolut, but it tends not to call its customers and deals instead through its in app chat which it did here. It's not for us to comment on how Revolut chooses to run its business, but I have thought about whether Revolut ought to have taken further steps for this payment and whether any further probing would have made a difference. When considering this, I've kept in mind that EMIs process high volumes of transactions each day. And that there is a balance for Revolut to find between allowing customers to be able to use their accounts and questioning transactions to confirm they're legitimate.

However, in the circumstances I think the actions Revolut took were proportionate to the risk identified at the time. Based on what Miss S has highlighted about the scam, even if Revolut had probed her further I don't think it would have made a difference here. This is because the scammer advised that Miss S shouldn't make Revolut aware that they were using remote access software. She's also explained that she was being guided by the scammer on how to answer questions at each step. And based on the evidence above it's clear that Miss S gave inaccurate information in order to get the payments processed. She's since confirmed that she hasn't invested in cryptocurrency before, she's also advised she found the opportunity on a social media platform and not through a friend or family member. She also told Revolut that she wasn't being told how to answer the above questions. It's clear that Miss S trusted what she was being told by the scammer so I don't think she would have revealed much about the circumstances around the payment, if probed further. So, although I appreciate that Miss S has advised the scammer was very convincing, I'm not persuaded Revolut ought reasonably to have known that Miss S wasn't revealing the true purpose behind her payment when making it. And, I think the actions Revolut took on this payment were proportionate to the risk it identified.

As explained above, I think that Miss S was under the spell of the scammer from the answers provided above so I don't think that further intervention from Revolut on Transaction 3 and 4 a few days later would have made a difference. I think it's clear that Miss S was willing to take direction from the scammer when making the payments, and although she was told she was answering general security questions, I can't ignore the fact that she was knowingly giving false information, despite the warnings being applicable to her circumstances. So, on balance, I don't have enough to say that if Revolut had intervened at any other stage and asked Miss S similar questions, that she would have provided the true purpose behind the payments.

So, I don't think there is anything further I would have expected Revolut to do before processing the payments.

Could Revolut have done anything to recover Miss S's money?

There are industry standards around attempting recovery of funds where a scam is reported.

Revolut attempted recovery of Miss S's payments. However, the payments to P were converted into cryptocurrency and paid to the scammer. Therefore, I don't think there was any realistic possibility of recovery.

Revolut also attempted recovery of the transfer to the third-party company. However, the receiving bank confirmed that the funds were no longer available. So, I don't think there was anything else Revolut could have done in the circumstances.

To summarise, I'm sorry Miss S was the victim of a cruel scam and about the impact the whole experience has had on her. I'm also sorry about the information she's shared with us about how the scam has impacted her. I'm conscious she's going through a particularly difficult time. But I can only direct Revolut to refund her losses if I'm satisfied any failings on its part made a material difference to what happened. On balance, I'm not convinced that it did.

My final decision

My final decision is that I don't 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 16 July 2025.

Aleya Khanom
Ombudsman