DRN-4739059

The complaint

Miss S complains that Revolut Ltd won't refund money she lost when she fell victim to an employment scam.

Miss S is being represented by solicitors in this complaint.

What happened

The detailed background to this complaint is well known to both parties and has also been set out previously by the investigator. The facts about what happened aren't in dispute, so I'll focus on giving my reasons for my decision.

The complaint concerns several transactions totalling approximately £3,500 which Miss S made in October 2023 from her Revolut account. These were made in connection with a job opportunity which involved completing a set of tasks to boost ratings for products for two stores. Miss S subsequently discovered that she'd fallen victim to a scam.

Miss S's Revolut account was opened as part of the scam. It was explained to her that she needed to make deposits in cryptocurrency to complete some of the tasks. To facilitate this, Miss S transferred money from her account with another business to Revolut, before sending them on to third-party individuals to purchase cryptocurrency through peer-to-peer trading.

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 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 be good industry practice at the time, I consider it fair and reasonable in October 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 – (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.

Where there's no previous account history, as was the case here, what should reasonably strike Revolut as concerning for a first payment isn't down solely to the transaction amount involved. I haven't seen any other factors at play here such that, in my view, Revolut should have been concerned and ought to have questioned Miss S when she authorised the first disputed transaction of £162 on 13 October.

The next few transactions – to a cryptocurrency exchange – didn't go through. It isn't clear why the transactions were unsuccessful but reading through the chat messages between Miss S and the scammer from that time, it looks like there was a problem at the merchant's end and the scammer instructed Miss S to buy cryptocurrency through peer-to-peer purchase. But that transaction flagged as suspicious on Revolut's fraud detection system.

After providing a general scam warning, Revolut asked Miss S to select the payment purpose from a list of options. She was then provided a warning specific to the option selected before being transferred to Revolut's in-app chat feature so that an agent could discuss the transaction further. Based on Miss S's chat with Revolut, it looks like she selected the payment purpose as 'buy or rent goods or services'. When prompted to narrow down the payment purpose further, Miss S appears to have selected 'something from social media/online marketplace/online retailer'.

During the live chat, the agent informed Miss S that based on her answers there was a high chance her money was at risk if she went ahead with the transfer. They went on to provide further scam education, including informing Miss S that scammers often tell customers to ignore payment alerts. The agent reiterated that the transaction had flagged as high risk and asked Miss S if she wanted to cancel the payment. But Miss S said she wanted to proceed, and the agent informed her she could return to the app to review the details and go ahead if she wanted to.

I've seen the chat messages between Miss S and the scammer from that same time. She referenced Revolut's intervention to them, including telling them that it had said this was a scam. The scammer reassured Miss S that Revolut's warning was a normal reminder to customers to protect their money, and that she just needed to reply to them and say she wanted to proceed. We know from her chat with Revolut that this is exactly what Miss S did.

I've thought very carefully about what happened when the transaction in question flagged. Miss S's response to the payment purpose wasn't accurate. Given that the transaction wasn't identifiably cryptocurrency related, Revolut couldn't reasonably have known that Miss S's response didn't match the payment type. Even when Miss S was directed to the in-app chat, she wasn't forthcoming with what she was doing. In the circumstances, I can't fairly say that Revolut failed to identify the type of scam Miss S had fallen victim to.

The transaction didn't go through in the end as it looks as though the individual Miss S was attempting to purchase the cryptocurrency from had declined it. Under the scammer's instructions, Miss S went ahead with purchasing cryptocurrency from a different third-party. Some of the subsequent transactions in the days that followed also triggered Revolut's fraud detection system. Again, Miss S mislead the EMI about the payment purpose. As such the warning provided wasn't specific to the scam Miss S had fallen victim to.

It isn't clear why Miss S didn't answer the payment purpose question honestly each time she was asked to. Having reviewed the entire chat correspondence with the scammer, earlier on the scammer had instructed Miss S not to mention cryptocurrency as that could cause problems. It seems to me that Miss S had been coached to lie if questioned about why she was making the transactions in connection to the scam.

I've considered whether further probing by Revolut at the times it directed her to an in-app chat with one of its agents would have led to a different outcome. But I'm not convinced that a better intervention would have stopped Miss S from going ahead. Chat messages with the scammer show that Miss S had doubts on several occasions over the course of the scam. Yet, despite sharing her concerns that she was being scammed, each time Miss S continued following their instructions. I'm not persuaded that any further questioning from Revolut would have made Miss S stop in her tracks. Given what I've seen, on balance, I think it's more likely than not that any further doubts or concerns she might have had following further Revolut's intervention would have been alleviated by the scammer who she was in constant contact with.

Miss S's representatives submit that Revolut ought to have taken notice of Miss S's vulnerability. But this was a newly opened account, set up without any direct interaction with one of Revolut's agents. I've also reviewed the chat correspondence between Miss S and Revolut and I haven't seen anything that leads me to conclude that Revolut ought to have picked up on Miss S's vulnerability from her responses. Ultimately, transactions did trigger an alert and Revolut asked questions to establish the risk involved. But Miss S wasn't honest as she was being coached. In the circumstances, I can't fairly say Revolut acted unreasonably in executing her authorised instructions.

I've also thought about the recovery of payments when Revolut because aware of the situation. For the peer-to-peer payments, recovery wouldn't have been successful as Miss S did receive the cryptocurrency from the individuals who were not involved in the scam. It's unfortunate that the cryptocurrency was then lost when it was sent on to the scammer's wallet. For the remaining transactions which were transfers, I can see Revolut contacted the beneficiary account providers. It either didn't hear back from the beneficiary account providers, or they confirmed that funds had already left the beneficiary's account.

In summary, I know that Miss S will be disappointed with this outcome. I fully acknowledge that there's a considerable amount of money involved here. Despite my natural sympathy for the situation in which she finds herself, for the reasons given, it wouldn't be fair of me to hold Revolut responsible for her loss.

My final decision

For the reasons given, 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 29 July 2024.

Gagandeep Singh
Ombudsman