DRN-5226303

The complaint

Miss B is the director of a company which I'll refer to as C. Miss B complains on C's behalf that Revolut Ltd is holding C liable for payments which she says were unauthorised.

What happened

The details of this complaint are well known to both parties. So, rather than repeat them all here, I've summarised the key events.

In February 2024, C's Revolut account was accessed from a new device and several payments, totalling just over £4,000, were sent to a new payee. Miss B was travelling and without internet access at the time. When she regained signal, she saw the payment notifications and reported them as fraudulent. When Revolut didn't agree to refund C, she referred the matter on to our service.

Revolut provided records showing the new device had been added to the account by selecting a link in an email sent to a colleague of Miss B, Mr M, who was involved with C. His password had then been reset using a code sent to his phone number. A further code, also sent to his number, was also required to make the first payment to the new payee. Revolut said it accepted a third party completed the payments – but the actions taken by Mr M (who was registered on the account) amounted to authorising them to do so. However, the parties connected to C's account say they didn't share anything or complete any of these steps.

Our investigator didn't uphold C's complaint. He didn't think it was likely the account could have been accessed, and the payments made, without the involvement of someone registered on C's account. In the absence of an explanation for this, he considered it fair for Revolut to treat the payments as authorised. He also didn't think Revolut could fairly be held at fault for not preventing or recovering the payments.

Miss B has appealed the investigator's outcome. In summary, she maintains no one acting for C consented to any payments or shared any details with a third party/scammer; Revolut should have identified the payments as suspicious and intervened, which would have prevented the loss; and Revolut has been negligent in safeguarding against fraud – noting there appears to have been a targeted scam, requiring knowledge of its customers' data.

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 cases like this, I can't be certain about what happened. So, I must make my decision on the balance of probabilities. I've weighed up all the information provided to determine what is more likely to have happened. Having done so, I've decided not to uphold C's complaint.

Under the relevant regulations – the Payment Services Regulations 2017 – the starting position is that the customer is liable for authorised payments, whereas the payment service provider would generally be expected to refund unauthorised payments.

In most circumstances, a payment is authorised because the customer completed the steps to make it (such as entering the payment details in the Revolut app and inputting any security codes required to confirm it). But there are other circumstances where I'd consider it fair for a payment to be deemed authorised – such as if the customer effectively gave permission for someone else (an agent) to make a payment, or told their payment service provider they wanted a payment to go ahead.

From what I've seen, I consider it unlikely the payments were made by any of the parties directly connected to C's account. However, for a third party to have made these payments, they would have needed access to information contained in several messages sent to parties who did act for C – such as Mr M. That includes the login link, which had to be selected to confirm the new device could access the account, as well as the codes used to reset the password and confirm the first payment. The email address and phone number these messages were sent to match those stored on Mr M's profile for this account.

Mr M says he did receive some messages; I can see, for example, that when reporting the dispute to Revolut he shared the text containing the code used to make the first payment. But he says he didn't see these at the time and didn't receive any contact from a scammer. Mr M says he did later share the texts with a colleague, who confirms receiving a call from a scammer. However, the colleague says he also didn't share anything, and believes it was another Revolut account he held, rather than C's account, which was being targeted.

Given this explanation, I can't see how a third party could have accessed the login link and codes needed to access the account and make these payments. So, on balance, I think these details were likely shared via the involvement of someone registered on C's account. And in the absence of an explanation for what they did and why, I do consider it reasonable for Revolut to treat these payments as authorised.

In saying this, I do accept it's likely a scammer directly made these payments. But without knowing how any representatives for C may have been tricked or scammed, I can't know what they understood or agreed to. In the circumstances, I don't think it's unreasonable for Revolut to conclude the actions of C's representatives amounted to effectively authorising a third party to act on their behalf.

However, given the likelihood of a scam, I have considered if there are any wider reasons why Revolut should fairly hold liability for C's loss. I understand Miss B's point that some Revolut customer data (such as phone numbers) appears to have been used to perpetrate this scam. But I've seen insufficient evidence to support that C's details were obtained due to a failing by Revolut. As is often the case, it's unclear how these details were obtained.

Miss B argues Revolut should have identified the payments as suspicious and completed further checks. But even if Revolut had done this, I'm not persuaded it's likely this would have prevented them from being made.

The access gained by the scammers means they would have had access to Revolut's in-app chat, to intercept any intervention. And it's likely they would have responded in a way to alleviate any potential fraud concerns.

I'm also conscious the payments were made on Mr M's profile. As I've explained, I consider it likely he (or another representative for C) shared details with the scammer. Without knowing what they shared and why, I can't reasonably conclude any direct contact made with them was likely to have prevented the payments from being made.

I've also considered Revolut's actions when the scam was reported. As the investigator explained, it wanted to speak to Mr M before attempting to recall the funds due to the payments being made using his details – to understand whether it had grounds to attempt to recall them. In any event, I've seen evidence that the funds were sent on before the payments were reported as fraudulent. Unfortunately, that meant Revolut couldn't successfully recall them.

I do appreciate this will be disappointing for Miss B, as I accept C has likely incurred a loss due to a scam. However, looking at Revolut's role in what happened, I'm not persuaded it would be fair to direct it to accept liability for this loss.

My final decision

For the reasons given above, my final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask C to accept or reject my decision before 20 March 2026.

Rachel Loughlin
Ombudsman