DRN-5601660

The complaint

Mr C complains that Revolut Ltd won't refund transactions he didn't make or otherwise authorise.

Mr C is being represented by solicitors in this complaint.

What happened

Mr C received a message on his mobile purportedly from Amazon notifying him of the annual Prime membership fee charge. As he pays for Prime membership monthly, he checked his bank account to see if the annual fee had been charged. Although it hadn't been, Mr C phoned the number in the message to look into the matter further.

The individual Mr C spoke with informed him that his Amazon account had been hacked, and fraudsters were in the process of making a purchase. Mr C logged on to his Amazon app and saw that an iPhone had been added to his basket of items. Around the same time, he also received an email from Amazon about a suspicious sign in from an overseas location. Mr C then noticed a second iPhone had been added to his basket.

Under the belief that the individual on the phone was assisting him in securing his Amazon account, Mr C followed their instructions and downloaded a remote access software. He states they then told him to delete all his stored payment methods before asking him to download the Revolut app. Mr C already had it on his mobile as he had an account with it, although he hadn't used it for some time.

Mr C states there was a lot of activity on his phone's screen which he couldn't keep up with. The individual spoke to him about fraudulent activity and showed him the sort of fraud alerts from Revolut he needed to look out for. Mr C was also given account numbers and sort codes, and he could see different transactions going in and out of his account.

Mr C states he didn't think much of it at first but soon realised something was odd. He logged on to the banking app for his main account provider and noticed that money had been transferred to his Revolut account. Mr C questioned the individual about the payments and was told not to worry as they would be reversed. But then the call disconnected, leading him to realise that he'd been scammed and lost just over £3,900.

In its final response to his complaint, Revolut said it hadn't received sufficient information from Mr C following the incident and so it hadn't investigated the scam claim. In its file submission to our service, Revolut said there had been no login attempts from any other device other than Mr C's own device. And it has controls in place which prevents third party remote control and view access to in-app screens with sensitive information, such as the payment screens. Therefore, it isn't possible for a third party to have initiated the payments on Mr C's behalf. Revolut also said several disputed transactions were detected as unusual, and it provided proportionate warnings.

Our investigator was satisfied on balance that the disputed transactions were authorised by Mr C and so he was deemed liable for them in the first instance. But they also thought that

Revolut didn't go far enough when the payments flagged as unusual. Given 'safe account' was selected as the payment purpose for the first payment, the investigator concluded that Revolut's intervention should have gone beyond the provision of a tailored scam warning during the payment journey; it warranted an intervention by a member of staff. Had that happened, the investigator was satisfied that the scam would have been uncovered and Mr C's losses prevented. To put this right, the investigator recommended Revolut to refund all the disputed payments in full.

Mr C accepted the investigator's recommendation, but Revolut didn't. In summary, it said the safe account payment option is not always indicative of fraud. Given the payment wasn't irregular yet its system worked as intended and still provided a strong warning, its actions were proportionate to the risk present. Revolut also said there was no way of knowing that the beneficiary wasn't in Mr C's name as set out in the payment instruction, given they went to an overseas account. The investigator's outcome remained unchanged and Revolut asked for a decision.

I issued my provisional decision last month and gave reasons for why I didn't intend upholding the complaint. I said:

> *"I appreciate that Mr C has struggled to recall how the conversation with the scammer moved from securing his Amazon account to accessing his Revolut account. My understanding of how the Amazon impersonation scams works is that in addition to helping the victim secure their Amazon account, the scammer also convinces them that the linked payment account has also been compromised. To keep their money safe, the victim is then tricked into accepting the scammer's help in securing their bank account. In the absence of any evidence to the contrary, I think this is what also happened here.*
>
> *When the complaint was initially referred to our service, Mr C said he didn't make the transactions he's disputing. In their assessment, the investigator concluded that it was fair and reasonable for Revolut to have treated the transactions as being authorised by Mr C. Although this finding hasn't been disputed by Mr C or his representative, for the sake of completeness, I've first considered whether the disputed transactions were authorised by Mr C.*
>
> *From what Revolut has told our service, it is my understanding that specific payment screens go black for both the customer and the third party when its app detects that screen sharing software is in use. This means there's no visibility over the screens, making it incredibly unlikely for a third party to be able to complete the steps involved in giving the payment instructions and reviewing and responding to any warnings.*
>
> *When our investigator sought further clarification from Mr C about what happened at the time of the payments, he recalled seeing transactions in and out of his Revolut account. He also said he saw alerts (from Revolut) which he thought the scammer was showing to him to highlight what they would look like when a payment flags as suspicious.*
>
> *Given Mr C was able to see some of the screens, which Revolut says would have been blacked out had remote access software been in use, on balance I think it's unlikely that screen sharing was in use at the time the transactions were made. Also, given Mr C remembers seeing warnings (albeit he claims he didn't realise they were real-time), and from the technical evidence provided a payment purpose selection was made on four occasions, I can't see how the disputed transactions were made without some form of involvement on his part. I note that Mr C also recalls the scammer giving him account number and sort codes.*

So, based on the information available, on balance, I'm satisfied that Mr C completed the steps involved in making the payments. And in the circumstances described, I also consider it fair and reasonable for Revolut to treat payments as having been authorised by Mr C.

What this also means is that in broad terms, the starting position at law is that Revolut is expected to process them in accordance with the Payment Service Regulations (in this case the 2017 regulations) and the terms and condition of Mr C's account. There are circumstances when it might be appropriate for Revolut to take additional steps before processing a payment. Such as when there are grounds to suspect that the payment presents a fraud risk. That might occur when a payment is significantly unusual or uncharacteristic compared to the normal use of the account.

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 at the time the transactions were made, 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; and*

- *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).*

Revolut recognised the first transaction as possibly scam related, and after notifying Mr C that the transaction could be a scam it asked him to select the payment purpose from a list of options. It then displayed a warning relevant to the option chosen. As I've set out in the background, 'safe account' was selected. From the information I've seen, Revolut provided a written warning covering the most common features of safe account scams.

While I understand that Mr C doesn't recall doing anything within his Revolut app, for the reasons I've given above, I'm persuaded that he completed the steps involved in making the payments. For the same reasons, I think the steps he completed also include selecting the payment purpose and confirming that he wanted to proceed with the payment after being presented with a warning.

Revolut states the warning it provided was proportionate to the risk identified. I don't discount Revolut's warning – which covered typical features of safe account scams – entirely. But having thought carefully about the risk the transaction presented, I don't consider displaying a scam warning on the screen and giving Mr C the option to cancel the payment or go ahead with it was a proportionate response to the risk identified. While I acknowledge Revolut's point that not all payments marked as 'safe account' are indicative of fraud, safe account scams are very common and it's rarely a legitimate reason for sending money to another account.

I consider a proportionate response to the risk the transaction presented would be for Revolut to have attempted to establish the circumstances surrounding the transaction before allowing it to debit Mr C's account. I think it should have done this by, for example, directing Mr C to its in-app chat to discuss the payment further.

The investigator's view was that had Revolut attempted to establish the circumstances around the transaction, Mr C would have been forthcoming that he'd been asked to download the remote access software and told to move his funds. And a scam warning by Revolut would have stopped him in his tracks.

This is where my findings differ from the investigator's. The challenge with this case is that Mr C's recollections and the evidence I've seen don't match. He's told us he didn't take any action within the Revolut app. What he recalls is watching the scammer perform actions on his screen and showing him warnings that he needed to look out for when fraudulent transactions are made on his Revolut account. But, for the reasons I've explained, it's unlikely that a third party could have performed actions on Mr C's Revolut app, let alone Mr C being able watch them do that. Also, the technical evidence I've seen shows multiple steps would need to have been completed by Mr C before the payment was executed. Mr C also remembers being given account numbers and sort codes. This ties in with the scammer likely tricking him into completing steps involved in making the payments.

But because I don't have the full context of the scam as it happened or know why Mr C selected the safe account payment purpose and then confirm that he wanted to make the payment, I can't be sure that an in-app intervention by Revolut would have played out along the lines the investigator has suggested. Mr C engaged with the payment purpose screens and the subsequent scam warning, but thought the scammer was showing him examples of what a fraud alert from Revolut would look like. Had there been an in-app intervention, it seems possible, even likely, that the scammer could have persuaded Mr C that the more specific questions were part and parcel of the examples being given. If he was tricked into engaging with the automated warning thinking it was an example, I think it's also likely that Mr C would have been tricked into engaging with Revolut's agent.

Overall, in all the circumstances of this complaint, I can't fairly conclude that a direct intervention by Revolut at the suggested trigger point, as well as the later ones where the same payment purpose was selected, would have uncovered the scam. What this means is that I don't consider Revolut acted unfairly in executing Mr C's authorised instructions.

I've also thought about whether Revolut could have done more to recover the funds once it became aware of the situation, as in some circumstances the money can be recovered. It says it was first made aware of the dispute by Mr C's other account provider when it received a fraud report notification. Revolut contacted Mr C to ascertain what had happened and although he responded two days later and said he had been scammed, Revolut didn't hear back from him until a complaint was received from his representative months later.

Although Revolut didn't attempt to recovery when Mr C said he'd been scammed, in the circumstances where it didn't have a lot of information and two days had already passed since the payments were made, recovery is likely to have been unsuccessful."

I gave both parties an opportunity to provide further comments or evidence for my consideration.

Revolut replied and said it didn't have anything further to add.

Mr C's representative said a human intervention should have taken place in this instance and a direct conversation with a Revolut representative could have potentially prevented the scam. Mr C's representative also added that Revolut should have taken appropriate action to limit account functions if screen-sharing software was detected. Given the failings, Revolut should be expected to take partial responsibility.

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 thank both parties for their response to my provisional decision. I've carefully considered the appeal submitted by Mr C's representative. But it hasn't persuaded me to change the outcome reached in my provisional decision. I'll explain why.

The representative states that a direct human intervention should have taken place in this instance. I should clarify, it if was unclear, that this is what I meant when I wrote 'directing Mr C to its in-app chat to discuss the payment further' in my provisional decision. Namely, that an agent should have made further enquiries of Mr C when the 'safe account' payment purpose was selected during the payment flow.

What this is means is that in reaching my provisional findings, I had already considered whether a direct or human intervention would likely have led to a different outcome. My finding that I can't fairly conclude that such an intervention would have uncovered the scam remains unchanged for the reasons set out in the provisional decision.

I can see Mr C's representative states that a phone call warning would have resonated with him. I appreciate the representative's strength of feelings on the matter. While our service does assess what a proportionate intervention should look like, generally it doesn't set specific expectations on how that proportionate intervention should take place.

I've also considered the comments made about expectations from Revolut when screen sharing software is detected. But as I set out in my provisional decision, based on the information Mr C and Revolut have provided, I think it's unlikely that screen sharing was in use at the time of the payments. So, I consider these comments have no bearing on the outcome I previously reached.

In conclusion, I know that Mr C and his representative will be disappointed with this outcome. Not least because of how long the matter has been ongoing and our investigator previously upheld this complaint. Despite my natural sympathy for the situation in which Mr C finds himself due to the scammer's actions, for the reasons given, I remain satisfied that it wouldn't be fair of me to hold Revolut responsible for his loss.

My final decision

For the reasons given, my final decision is that I'm not upholding this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr C to accept or reject my decision before 2 July 2025.

Gagandeep Singh
Ombudsman