DRN-4357656

The complaint

Miss S complains that Revolut Ltd failed to refund transactions made from her account that she didn't recognise.

What happened

What Miss S says

Miss S says she noticed her mobile phone had stopped working and believed this could have been because of an update to it. Miss S says it took some time to get her phone working again. She then had to re-load the Revolut app on her phone but found she couldn't log in to it.

About three days after the problem with her phone, Miss S eventually regained access to her Revolut account and found numerous transactions had been made from it which she didn't recognise. Some funds had been transferred to other accounts, some payments made using her card linked to the account and some exchanged for crypto currency.

Miss S informed Revolut about these payments and informed them about the problems she'd had with her phone and app. A few payments had been blocked (and later reinstated on Miss S's account) by Revolut because of concerns about the transfers and some card payments were later refunded by the merchants themselves.

The full list of transactions were produced by the investigator in her report to both parties so I don't intend to repeat them here.

Miss S told Revolut she'd lost several thousand pounds, and this was as a result of her phone/email and Revolut account being compromised by a hacker. Miss S provided details of an attempt to reset her security credentials for her phone and it's account.

Miss S confirmed to Revolut that she hadn't provided any of her banking/phone security information to anyone else and she was the sole user of her phone. She confirmed she hadn't been approached by anyone seeking her help or trying to obtain security information from her.

Miss S asked for her lost funds to be refunded, but Revolut declined, believing there was no compromise of her account. Miss S disagreed and after her complaint to Revolut was also declined, she brought it to the Financial Ombudsman Service for an independent review.

What Revolut says

Revolut received notice from Miss S that her account had been compromised and numerous payments made from it. They looked into the issue but couldn't determine where it had been compromised.

Revolut confirmed that Miss S had added a new device (phone) to her account several

weeks prior to the disputed transactions. This included changing the phone number attached to the account. The procedure for adding a new phone included a request for a photograph of Miss S, this was sent at the time and Revolut were satisfied it matched the one she'd provided when opening the account some months earlier.

The new device also used the same IP address which Miss S had used before, and this new phone was responsible for making the various disputed transactions. Based on this information, Revolut held her liable for the payments, believing she'd carried them out herself.

Note: IP addresses are a means to identify physical locations that online transactions are connected to and can be the actual physical location or other locations connected to the provider of the data services.

The investigation so far

Miss S's complaint was looked into by a senior investigator. She asked both parties for information about the complaint. Miss S provided an explanation of what happened and provided details of messages she'd received regarding her phones security.

Revolut provided audit data concerning the changes to Miss S's account (the addition of a new device) and information about the disputed transactions.

After reviewing the evidence, Miss S's complaint wasn't upheld. The investigator commented that:

- The data from Revolut showed it was Miss S who'd added another device to her account.
- The photos provided to add the phone matched the one already held by Revolut.
- A common IP address was used by both devices indicating that it was the same person who had access to them.
- Miss S hadn't given her device or account details to anyone else.
- There was no evidence of a compromise or a plausible explanation how a third party could have made the payments without Miss S's knowledge.

Miss S strongly disagreed with the report and, in summary, said:

- She wasn't responsible for the disputed transactions and reported them to Revolut herself.
- She's never owned the model phone added to her account.
- She believed Revolut were responsible for her details being compromised.
- Further details of her phone's account being compromised were provided and a notification concerning another payment method which had been stopped due to suspicions of fraud (dated after these disputed transactions).
- Miss S said she kept her security details on the notes app on her phone, which is how her account could have been compromised.

- She used public Wi-Fi which could account for the matching IP address.
- Miss S didn't accept she'd provided her photos to Revolut and they'd been obtained by the scammer.

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.

The relevant law surrounding authorisations are the Payment Service Regulations 2017. The basic position is that Revolut can hold Miss S liable for the disputed payments if the evidence suggests that it's more likely than not that she made them or authorised them.

Revolut can only refuse to refund unauthorised payments if it can prove Miss S authorised the transactions, but Revolut cannot say that the use of the card details or banking app conclusively proves that the payments were authorised.

Unless Revolut can show that consent has been given, it has no authority to make the payment or to debit Miss S's account and any such transaction must be regarded as unauthorised. To start with, I've seen the bank's technical evidence for the disputed transactions. It shows that the transactions were authenticated using the payment tools issued to Miss S. I'll now need to consider the information provided by both parties to determine whether there's sufficient evidence to hold Miss S responsible for the disputed transactions or not.

Miss S's version of events is that someone (unknown) took over her account, including her phone and made various transactions from her account. Revolut have a different version and believe their evidence points to Miss S being responsible for them.

Examining the evidence provided by both parties, it's apparent that Miss S had messages from her phone provider that showed her account details had been used and a later message to say that an attempt had been made to reset those details. This notice wasn't actioned (by the phone operator) at the time. That's because such requests are delayed to help protect the accounts owner. This notice showed the request wouldn't be actioned until well after these disputed transactions took place.

I accept that Miss S had some messages concerning her account ID (held with her phone provider), but there's nothing that indicates anyone was successful in taking over her account.

Revolut's information showed that when Miss S opened the account, she provided a photograph of herself, and this was later repeated when the second device was added to her account some weeks before the disputed transactions were made. Miss S has argued that these photographs were used by the scammer, and they weren't the type she would send to Revolut for the security check. Having looked at Revolut's records, they show the date and time of each photo when it was received by them. Both photos are of Miss S and the audit data linked to them indicates they were genuine and not subject to some form of manipulation. So, it's the case that if they were obtained by a scammer, then the account itself would be false – because it couldn't have been opened at all without them. Miss S hasn't raised this possibility and appeared to use the account normally from when it was opened. The other option is that the photos were uploaded by Miss S herself and that's supported by the audit evidence. I think that what Revolut have shown is that Miss S registered the second device after providing a photo of herself.

This is further supported by Revolut's evidence that a common IP address was used for both

the devices associated with Miss S's account. The pattern of use of those devices doesn't support Miss S's assertion that a scammer compromised her account on the same public network, it's far more likely it was linked to a regular location. So, the combination of Revolut's evidence doesn't support an unknown third party being responsible for these transactions.

I've also thought about the registration of the second device – it took place some three weeks or so before the disputed transactions took place and at the time, the account held a very healthy balance. If a scammer/fraudster had access to the account from the second device, I'd expect the account to be emptied at the time. There's no good reason for a criminal to wait if there are funds in the account as they're unlikely to know if they'll be spent or the compromise of the account identified. Generally, these types of compromise result in a fairly quick attempt to remove the funds, but that didn't happen here.

I've also considered the various blocks applied to some transactions and credits to the account, including the refund made by a merchant. I don't think that any of these show that the account was operated by anyone without Miss S's knowledge.

Overall, I'm not persuaded that Miss S's account was compromised as the evidence doesn't support that. What it does show is that Miss S registered a new device that was then used to make various disputed transactions, including some crypto currency exchanges which are also present on the account from some months earlier.

My objective assessment here is that I think Miss S was more likely than not responsible for these payments and it was reasonable for Revolut to hold her liable for them.

My final decision

My final decision is that I do not 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 14 December 2023.

David Perry
Ombudsman