DRN-4404052

The complaint

Ms I complains that Revolut Ltd failed to refund a transaction she didn't identify.

What happened

What Ms I has said

Ms I was out shopping and had difficulty with her Revolut account. After spending some time logging into it and answering various security questions, she noticed a large payment had left her account which she didn't recognise. This payment had been made to a crypto currency merchant and nearly emptied her account. The payment was for £2,500.

Ms I asked Revolut to refund this as she didn't make the transaction herself. She said that someone had "hacked" her email and been able to obtain the necessary details to register another device on her account which was responsible for stealing the funds. Ms I said that based on the timings of the transaction (very early in the morning), she was asleep and in a different part of the country to the new device registered to her account. Revolut declined the refund, believing she'd carried out the payment herself. Ms I complained to Revolut who again considered the circumstances but didn't change their position.

Ms I then brought her complaint to the Financial Ombudsman Service for an independent review where it was assigned to an investigator.

What Revolut have said

Revolut's system restricted the account after an automatic alert was created. Once they'd confirmed Ms I's identity, they considered whether they could use the chargeback system to challenge the payment, but after reviewing their information and based on what Ms I told them, they didn't think it would be successful.

Ms I had confirmed that she hadn't given her account details to anyone else or lent her phone to another person. Revolut didn't think that her account had been compromised. They did consider if the payment was the result of a scam, but Ms I said she knew nothing about the purchase of crypto currency. Revolut declined to make a refund, believing that Ms I was responsible for the payment.

The investigation so far

Both parties were asked to provide evidence and information about the disputed transaction. Ms I described how she'd noticed emails (from Revolut) in her account that she hadn't actioned. She believed that someone had hacked her email and removed the emails from her "inbox", but they'd failed to fully destroy the emails. She said that she'd seen notices from Revolut but hadn't acted on them as she often received "spam" from them.

Ms I denied any knowledge of the disputed transaction and remarked that the payment had caused her some distress as she'd had to obtain a loan from her employer.

Revolut provided technical information concerning how the payment was made and an audit

of actions carried out on the account. They explained that there was a new device registered to use the account around the time of the disputed transaction and location information indicated it was some distance from where Ms I was living at the time.

But, they said that the crypto currency merchant had requested an additional level of security when the payment was made known as 3DS. This meant that a message was sent to the primary device registered with Revolut – and that was the one used by Ms I. It wasn't the one that was newly registered that morning. That message required the user to open the app and confirm the payment was genuine before the crypto merchant would accept the payment.

After the investigator reviewed the evidence from both parties, he concluded that it was likely that Ms I made the payment herself. It was noted in his report that:

- No one else had access to the account apart from Ms I.
- Her primary device, which had been registered and used without issue, was responsible for confirming the 3DS message.
- There was another device, but Revolut's information stated it was registered after the disputed transaction had already happened.

Ms I strongly disagreed with the investigator's outcome, commenting that:

- She was asleep at the time and knew nothing about the transaction.
- The automatic restriction on her account (after the disputed transaction had already occurred) is evidence the account was compromised.
- Ms I recovered emails she believes were evidence of the "hacker" gaining access to Revolut codes used to defraud her and an email account she believes belonged to the "hacker".

As no agreement could be reached, the complaint has now been passed to me for a decision.

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.

This complaint has been considered based on the assertion by Ms I that she knew nothing about the payment. Essentially she's saying it was unauthorised. Revolut considered if Ms I was caught up in a scam which often involves payments to crypto currency merchants. Ms I told them this wasn't the case. The relevance of whether the payments were unauthorised or a scam is that they're treated slightly differently when assessing the merits of the situation and what we'd expect of either party. So here, as Ms I denied any involvement in the transaction, it's been treated as an "unauthorised complaint".

The relevant law surrounding authorisations are the Payment Service Regulations 2017. The basic position is that Revolut can hold Ms I 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 Ms I authorised the transactions, but Revolut cannot say that the use of the card details for an online payment 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 Ms I'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 Ms I. I'll now need to consider the information provided by both parties to determine whether there's sufficient evidence to hold Ms I responsible for the disputed transactions or not.

Whilst there's evidence of a new device recorded on Revolut's system, that device didn't receive the 3DS security message generated by the crypto merchant. Revolut have confirmed that only the primary device (here Ms I's own phone) would receive the 3DS message. In order to activate that confirmation, it required a log in to the app installed on Ms I's device (her mobile phone).

In order to do that, someone had to have access to her physical phone, know the security details to access it (biometric/or personal identification number (PIN)), then open the banking app and login with another set of security information, before confirming the message to authenticate the transaction with the merchant.

Each of those steps requires discreet information known only to Ms I. As she's confirmed no one else uses her phone or has access to the information about it or her Revolut account, it seems unlikely that an unknown "hacker" could obtain the entirety of that information.

I've also thought about the compromise of her email account. If someone had access to the account in order to intercept the messages about the new device logging into it, as Ms I stated, why would they then send those details (which weren't relevant to the disputed transaction) to another email account? They would have all the information they needed at the point the account was compromised because they would essentially be in control of it and could see the messages from Revolut. I've not seen anything that would persuade me the email account was linked to the disputed transaction.

Overall, there are a number of steps required in order to authenticate the 3DS message sent to Ms I's primary device, particularly the requirement to open the app on the device itself. If, as Ms I states, she was asleep and had the device with her, it seems unlikely to me that someone unknown to her could get hold of the phone, bypass several levels of security on the phone and the Revolut app itself, before authenticating the transaction, before returning the phone to Ms I at her home.

Based on an objective review of the evidence, I think it's more likely than not that Ms I was responsible for these transitions or allowing someone else to do them with her knowledge. In either case, I think it's both fair and reasonable that Revolut held her liable for the disputed transaction and I won't be asking them to do anything.

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 Ms I to accept or reject my decision before 1 December 2023.

David Perry
Ombudsman