

The complaint

Miss I complains that Revolut Ltd (Revolut) won't refund transactions totalling £420 which she says she didn't authorise.

What happened

The background to this complaint is well known to both parties, so I won't repeat everything here. In summary, Miss I says there were 12 transactions, each totalling £35, which were taken from her account while she was on holiday. This resulted in £420 leaving her account which she says she didn't approve.

The transactions occurred in the early hours of the morning. Revolut says that these were authorised using Apple Pay and this was set up using a code that was sent by text to Miss I prior to the transactions occurring. As Miss I said that her phone remained in her possession, Revolut is persuaded that Miss I authorised the transactions or provided details which enabled somebody else to complete the transactions. Because of this they are not refunding the amount taken from her account.

The investigator concluded that Revolut acted fairly by not refunding Miss I the payments she's disputing. As Miss I disagrees this complaint has 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.

While I might not comment on everything (only what I consider key) this is not meant as a discourtesy to either party – it reflects my role resolving disputes with minimum formality. I'd like to assure both parties I've considered everything they have sent.

Having done so, I don't uphold this complaint.

Generally speaking, Revolut is required to refund any unauthorised payments made from Miss I's account, and Miss I should only be responsible for transactions made on her account that she has authorised. Those rules are set out in The Payment Services Regulations 2017. Miss I says she didn't authorise the transactions she's disputed. So, I have to decide whether or not I think Miss I authorised them.

Revolut's internal notes show that the disputed transactions took place using Apple Pay. I've therefore looked into how this was set up.

Revolut's internal notes show that a text was sent to Miss I around 20 days before the disputed transactions occurred and that following this Apple Pay was set up. Based on Revolut's internal notes I'm satisfied that the text was correctly sent to Miss I (and I've noted to the same number our service has for her). This text contained a code for Miss I to set up

Apple Pay. Revolut confirmed it read “this code will be used to add your card to another Apple Pay device. Don’t enter it anywhere unless you want to add your card to a new device. Don’t share this code with anyone, even if they claim to be from Revolut. Revolut verification code for Apple Pay: XXXXXX”. So I’m satisfied Miss I received a code to set up Apple Pay.

Miss I provided a screenshot showing funds being added to an account via Apple Pay but it’s unclear what account this relates to. Revolut also provided internal notes showing that Apple Pay was set up previously for Miss I. But I haven’t seen anything to show that the fact Apple Pay was added to a previous device means that it couldn’t have been added to a new device. Apple’s website says that this is possible. For these reasons, I’m persuaded that it is possible to set up Apple Pay for the same card on multiple devices.

Miss I has told our service that she had her phone in her possession. Her card details would also have needed to be provided for her to set up Apple Pay – and I’ve not been provided with any information to show how a potential fraudster would have had access to Miss I’s card details *and* her phone so they could access the code. The transactions she has referenced as potentially suspicious don’t explain how a third party could have had access to the code sent to her phone in order to set up Apple Pay. Miss I has said that everything, everywhere can be hacked by cybercriminals, but based on what I’ve seen I can’t see how this happened here. And there isn’t enough here for me to say on balance this is likely what happened here.

As such, I’m satisfied after reviewing the information given that the disputed transactions were made and authenticated using Apple Pay which would have needed to have been set up using a code sent to Miss I’s phone. And I haven’t been provided with a plausible explanation as to how anyone but Miss I could have authenticated the transaction.

In order to decide Miss I most likely authorised the disputed transactions, I not only need to be satisfied the transactions were authenticated (as I’ve said above, I think they were), but I also need to be persuaded Miss I most likely consented to them.

Below are three possible scenarios regarding consent:

- a) Miss I consented to the disputed payment transactions herself. That is, she used Apple Pay to make the disputed payment transactions herself.
- b) Miss I provided authority to a third-party to consent to the disputed payment transactions.
- c) A third-party, without Miss I’s authority, gave consent to the payment transactions. That is, a third-party used Apple Pay to make the disputed payment transactions without her authority.

In scenarios (a) and (b), Miss I authorised the disputed payment transactions, so redress would not be available to her. In scenario (c), Miss I did not authorise the transactions, so redress could potentially be available.

Miss I denies making the transactions herself, and said she didn’t provide authority to a third-party to make them on her behalf. Therefore, I have reflected on whether it is more likely than not that scenario (c) applies, rather than (a) or (b). Having done so, I am not persuaded that scenario (c) is more likely.

For a fraudster to have made the disputed payment transactions – they would have required access to Miss I’s card details *and* her phone so they could access the code and set up

Apple Pay on a device other than Miss I's. And after carefully considering all the information given I'm unable to say on balance, that both layers of security were compromised.

Miss I says that she was asleep and her phone switched off at the time the transactions occurred; and it was only when she woke up and checked her phone that she was aware of the transactions. In this case, given the evidence I've seen and given the level of security that would have needed to have been completed to set up Apple Pay, I think it's unlikely and I can't see a plausible explanation of how Apple Pay could have been set up, and how the transactions could have been authorised without Miss I's consent. For these reasons, I am not satisfied, on balance, that a third-party was responsible for the transactions.

Miss I also provided copies of emails from what looks to be from the business the funds were sent to. In these emails the business says that it appears that someone accessed Miss I's card details and used them to make unauthorised transactions. But these conclusions look like to be based on what Miss I has said and not as a result of an in-depth investigation at their end. The business explained that as the transactions have already been processed, they can't offer a refund and direct Miss I to contact Revolut. While I've carefully considered the emails alongside all the information given, they aren't enough for me to fairly ask Revolut to refund the disputed transactions.

I appreciate that Miss I will be disappointed. But for the reasons I've explained I'm not persuaded it was unreasonable for Revolut to treat these transactions as authorised and to therefore not refund them.

My final decision

For the reasons set out 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 Miss I to accept or reject my decision before 25 April 2025.

Sureeni Weerasinghe
Ombudsman