DRN-4223971

The complaint

Ms S complains that Revolut Ltd failed to refund transactions that she didn't recognise.

What happened

What Ms S says

Ms S was in a meeting when she received an alert from Revolut. Her payment card used on the account had been frozen and Ms S noticed several transactions had been made from her account that she didn't recognise.

Ms S asked Revolut about them and sought a refund. She said she wasn't aware of the payments or the merchant (offering multi-currency accounts) who had received them. After looking into the matter, Revolut declined to make a full refund, although one of the payments was later paid back to Ms S. The loss was also reported to the police.

What Revolut says

Revolut's security system froze her card after repeated transactions to the same merchant. After Ms S contacted them, they considered whether they could approach the merchant using a chargeback process. Due to the specific circumstances of these payments, Revolut decided they couldn't use a chargeback because their records showed the payments were made with Ms S's registered card through the use of Apple Pay.

The process for authorising Apple Pay linked to Ms S's account (and card) was completed just prior to the start of the disputed transactions. Revolut said this could only have been done by Ms S. They said the one refund received by Ms S was a gesture of goodwill.

The investigation so far

After Revolut declined to refund the complete set of disputed transactions, Ms S complained to the Financial Ombudsman Service and sought an independent review of the complaint.

An investigator was assigned to look into the situation and both parties were asked to provide whatever evidence they could. Ms S explained how she was in the office when she received an alert and hadn't authorised these transactions. She confirmed she had Apple Pay on her phone(s) but wasn't responsible for these transactions.

Ms S also confirmed she retained possession of her phone(s) and no one else knew the details of her Revolut account or the payment card attached to it. She also confirmed that she hadn't received any unusual messages or requests for information from anyone.

Revolut provided details about the payments and records from their system about Ms S's account. After reviewing the evidence, the investigator didn't uphold it, believing the evidence pointed to Ms S being responsible or enabling someone else to use her account due to the information needed for Apple Pay to be authorised. The investigator didn't think that Revolut's decision to decline the chargeback application was unreasonable as it was likely to fail based on their understanding of what had happened.

Ms S disagreed what the investigator's outcome and asked for it to be reinvestigated. A second investigator looked at the complaint who asked Revolut for further information about the circumstances, including the specific audit data concerning the use of Apple Pay.

Revolut supplied that data and it was confirmed that a message with a specific code was sent to Ms S's registered phone to enable Apple Pay to be linked to her card. Revolut said the system is designed to prevent anyone adding this type of payment system without the owner of the account being aware.

Considering this additional information, coupled with:

- Ms S's confirmation that she hadn't provided her account details to anyone else; and
- there was no evidence of a second phone being added to her account.

The second investigator didn't think there was a plausible explanation of how Apple Pay could have been authorised without Ms S's knowledge.

Ms S's assertion that she hadn't made them herself was acknowledged, but the evidence couldn't explain how an unauthorised third party could have carried them out.

The investigator considered whether Revolut should have intervened at the time but based on the how they were made and for how much, she didn't think Revolut could have reasonably prevented the loss.

Ms S again disagreed with the second outcome and said:

- Apple Pay was already authorised on her two phones that were in her possession.
- She didn't receive any codes the day of the disputed transaction and didn't carry them out.
- Ms S usually received notification for larger payments but didn't in this case. She also said these payments were much higher than she usually used the account for.

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.

The complaint brought by Ms S is that she wasn't responsible for adding Apple Pay or making the disputed transactions. Revolut's case is that she had to be responsible because their records showed she used a code sent to her mobile phone, which enabled Apple Pay to be added to a device. Where there is a dispute about what happened, as it is here, and the evidence is incomplete or contradictory, I must reach my decision on the balance of probabilities – in other words, on what I consider is most likely to have happened in light of the available evidence.

The relevant law surrounding authorisations are the Payment Service Regulations 2017. The basic position is that Revolut can hold Ms 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 Ms S authorised the

transactions, but Revolut cannot say that the use of Apple Pay 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 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 Ms S. I'll now need to consider the information provided by both parties to determine whether there's sufficient evidence to hold Ms S responsible for the disputed transactions or not.

Revolut's audit evidence shows that just prior to the disputed transactions took place, a new request for Apple Pay was made and authorised after the successful completion of the passcode sent to Ms S's phone. Ms S denies ever receiving the code on that day and said that Apple Pay was already set up on her two devices. Their records also show that two other devices had already been set up to use Apple Pay.

The payments themselves do show the type of transaction you'd expect to see from someone emptying the account as soon as possible (often how hijacked accounts are exploited), that is quick payments over a short period of time. None of them are particularly large payments, so I can see why they didn't alert Revolut, but there are several declined attempts made – supporting the case that whoever made them wasn't aware of what the balance was in the account.

The timeline of the Apple Pay authorisation and the following disputed transactions suggests that the account with the merchant that received the payments was already set up. That's because the account the funds were paid to required an application supported by identification. It's unlikely such an account was set up on the spur of the moment. What that indicates is that the payments made from Ms S's account had an element of planning involved.

It doesn't appear likely that these payments were made as the result of a scam because Ms S confirmed she hadn't been asked to provide any details to anyone or received unusual requests for information. So, whoever made them had access to Ms S's phone, because otherwise the passcode issued by Revolut couldn't have been used to create the Apple Pay facility on another phone. There's no evidence of compromise of Ms S's account or anything that would point to how someone could have obtained the necessary information to set up Apple Pay.

I do recognise there are some aspects of this complaint that supports the notion that Ms S's account was used by someone without her permission. But, without a plausible and realistic explanation for how the code sent to her phone was somehow obtained by a third party, I can't uphold this complaint.

Whilst I'm sure Ms S will disagree with me, I think it's implausible to conclude they weren't authorised without stronger evidence to the contrary. That means I think it's more likely than not that Ms S carried out these transactions herself – or that someone else with consent did so.

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 S to accept or reject my decision before 1 December 2023.

David Perry
Ombudsman