

The complaint

Mrs V complains that Revolut Ltd ('Revolut') debited her account with a series of payments totalling nearly £800 which she says she did not make or otherwise authorise.

What happened

The details of this complaint are well-known to both parties, so I will not go into every detail of what happened here. But in summary, Mrs V says that in May 2024 she logged into her Revolut account to discover a series of payments to a popular online auction website which were made via Apple Pay. Mrs V says she did not make these payments, had never set up Apple Pay for her Revolut account, and did not authorise anyone to do either of these things on her behalf.

Mrs V said when she noticed the payments she contacted Revolut who said they could not raise a chargeback for her as the payments were made using Apple Pay. Mrs V maintains that she has never set up or used Apple Pay, and says that Apple Pay confirmed her Revolut card hadn't been added to their service. She said when the transactions took place she was on holiday but the payments took place in a different country. When she was not using her Revolut card, she said that it was kept in a cupboard at home in her gated apartments where she lives with her husband. She said that nobody else could access her card details.

Revolut reviewed Mrs V's disputed transactions, but declined to refund the loss or raise a chargeback. In summary, they said this was because:

- Mrs V's card had been added to Apple Pay in March 2024;
- Neither Mrs V's card nor her mobile had been reported lost or stolen;
- A one time password ('OTP') had been sent to Mrs V's phone in order to set up Apple Pay;
- An alert was sent to Mrs V's mobile to verify that Apple Pay had been set up; and
- No new or unrecognised phones were registered on her account.

Unhappy with their decision, Mrs V escalated her concerns to our service. One of our investigators looked into what happened and did not recommend that Mrs V's complaint be upheld. They felt that on balance it was more likely than not that the payments were authorised and so did not think it would be fair to ask Revolut to refund them.

Mrs V remained dissatisfied. She said, in summary, that she:

- Had received an email from Apple Pay which confirmed that her card had never been added to her Apple wallet. She provided a screenshot which she said showed the previous cards she had added to Apple Pay, which showed just one card from an account she holds with a different business.
- The transactions appeared to be made in a completely different part of the country from where she was at the time, or another country entirely.
- She had contacted the auction website and the addresses on orders was different from that on the statements. The website claimed that the transactions were done

from China. They had suspended both the buyer and seller from using their platform. Our investigator still could not see where there was a point of compromise for the OTP needed to activate the card on Apple Pay. As no agreement could be reached, the case was passed to me to decide.

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.

Having done so, I have reached the same conclusion as our investigator, and broadly for the same reasons. I know this will come as a disappointment to Mrs V, and I am sorry for this. I will explain how I have reached this conclusion.

Generally, Revolut can hold Mrs V liable for the disputed transactions if the evidence suggests that it is more likely than not that she authorised these payments or gave someone else consent to make them on her behalf. I am satisfied from my review of Revolut's technical evidence that the payments were properly authenticated utilising Apple Pay, which had been set up using an OTP. But regulations relevant to this case state that authentication alone is not enough to enable Revolut to hold Mrs V liable. So, I need to think about whether the evidence suggests that it is more likely than not that Mrs V consented to these transactions being made. This could include allowing someone else to complete these transactions on her behalf. Having done so, on balance, I think that Mrs V must have made or otherwise authorised these transactions. I will explain why.

I think it is more likely than not that whoever set up the Apple Pay also made or authorised the disputed transactions. I say this because Apple Pay was only used on Mrs V's Revolut account for the disputed transactions, and Mrs V denies adding the account to Apple Pay as well as disputing these transactions. So, I think it follows that the setup of Apple Pay and the disputed transactions are intrinsically linked.

I have carefully considered how Apple Pay could have been set up for Mrs V's Revolut account. Whilst Mrs V says she didn't set up Apple Pay for her Revolut card, it is clear from the technical evidence that Apple Pay was set up using an OTP which was sent to Mrs V's genuine phone number. Mrs V has told us that she did receive this text to her phone. So, I have thought about the different ways in which an OTP can be used to set up Apple Pay. Having done so, I have not been able to find any point of compromise for the OTP, so I think it is most likely that Mrs V set up or otherwise allowed for the setting up of Apple Pay. I say this because:

- I have considered the most common ways in which an OTP can be compromised. And having done so, the evidence does not support Mrs V's account.
- I thought about whether Mrs V could have been the victim of a SIM swap. SIM swapping is what happens when a fraudster contacts a customer's mobile phone service provider and tricks them into activating a SIM card that the fraudsters have. Once this occurs, the scammers have control over your phone number, as it is transferred to the new SIM card. This means that if anyone calls or texts the customer's genuine number, it is sent to the new SIM card and so is received on the fraudster's phone, rather than that of the genuine customer. I do not think this is most likely what happened here. I say this because by Mrs V's own admission, she received the OTP on her phone. If a SIM swap had occurred, it would have only been sent to the new SIM card, so only would have appeared on the fraudster's phone.
- Mrs V was working from home alone when the OTP came through on her phone. So it seems unlikely that someone was able to physically gain access to her phone to read the OTP.

- Our investigator also explored the prospect that someone could have tricked Mrs V into handing over her OTP. Fraudsters can be very skilled in gaining information from unwitting victims, so our investigator even explored any phone calls Mrs V had that day to see if she could ensure that there were no suspicious calls. Mrs V was able to explain the phone calls she had that day, and it does not appear there were any unexpected or suspicious calls. Mrs V has not reported any other suspicious communications around that day, and has been clear that she did not hand over the OTP to anyone. So, there is nothing to suggest Mrs V was tricked into handing over the OTP.
- I have also thought about less common methods which fraudsters use to obtain personal information and OTPs, but based on the available evidence, I cannot see how an unknown third party could have compromised Mrs V's OTP.
- I also have thought about what other details the person who set up the Apple Pay would need. This would have included the card details, which Mrs V said she did not give out to anyone, nor is there a plausible explanation as to how someone could have gained access to these without her permission.
- And so, it follows that it is more likely than not that Mrs V or someone acting on her behalf set up the Apple Pay using the OTP. I appreciate Mrs V has shared a screenshot of the previous cards she had on Apple Pay which did not include the Revolut card, and information from Apple Pay to say she had not added it. However, the technical evidence which Revolut provided shows that her Revolut card was added to an Apple Pay, and then utilized for the disputed transactions.

I also think that the available evidence shows it was most likely that Mrs V, or someone acting on her behalf, authorised the disputed transactions. I say this because:

- Mrs V topped up £500 prior to the disputed transactions. She has said this was to set up her account and not leave it empty, but she had already topped up her account previously. Whilst this is not impossible, it seems unusual that she topped up an account that she had not really used.
- No unknown devices were added to her account at the time Apple Pay was set up, or at the time of the disputed transactions.
- The technical evidence shows that not only did Mrs V get sent the OTP, but would have also received a notification to say her Apple Pay was set up. It is plausible that she did not really question these – she said she did not see any notification and thought the text was to do with setting up her account. But it does seem unusual that she did not question why she was being sent a code if she did not request it or see a use for it.
- The Apple Pay was set up in March, and the disputed transactions did not take place until May. One would assume an unknown third party who had access to her account, who would have presumably known that Mrs V had received an OTP via text which she could question, would not wait this prolonged period of time before making the disputed transactions.

I do appreciate that Mrs V may have fallen victim to a fraud or scam – I am not saying this is impossible here. But my role is to assess the evidence available to me and determine what most likely happened here. And having done so, I cannot see how Mrs V's OTP would have been compromised in order to set up the Apple Pay, and it follows that I cannot see how an unknown third party could have done this or completed the disputed transactions.

Mrs V has queried the location of the payments when she was in another country, and they appeared to be in London on her statements and the online auction site told her they were made in China. But the London address was an address for the online auction company.

And for the purposes of the relevant regulations, Mrs V did not have to complete the transactions herself in order to authorise them. So, she can still have authorised them even if she did not physically make the transactions herself, so the location they took place in does not alter my decision here.

I have also thought about Revolut's decision not to raise a chargeback here. Revolut are not obligated to raise a chargeback. Whilst in some cases it would be regarded as good practice, they have said that their processes mean that as Apple Pay is set up with the authorisation of the account holder by using the OTP sent to their registered phone, it would mean that payments then made using Apple Pay are authorised by the account holder. I do not think that Revolut acted unfairly by not raising a chargeback here.

My final decision

I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs V to accept or reject my decision before 23 May 2025.

Katherine Jones
Ombudsman