DRN-5667189

The complaint

Mr F complains that Revolut Ltd ('Revolut') debited his account with two payments totalling roughly £335 which he says he did not make or otherwise authorise.

What happened

In May 2025 I wrote to both parties to this complaint to explain my thoughts on the case. I had reached the same overall conclusion as our investigator had, but had gone into further details with regard to my reasoning. To be fair to both parties, I felt they ought to have the opportunity to respond with further comments or evidence should they wish to before I reached a final decision on this complaint. The following is an extract from that decision.

"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, Mr F complains that in April 2024 Revolut debited his account with two payments to an e-commerce site which were made via Apple Pay that he says he did not make or otherwise authorise.

Mr F said that he was working at the time the transactions were made, and not buying anything. He said the payments appeared to have been made in Hong Kong, which is somewhere he has never been to. He said that as soon as he saw the transactions he blocked the merchant and cancelled his card, then two further attempts were made to make payments to the same merchant. He complained that despite the four payments being made within five minutes, Revolut did not identify them as fraudulent nor conduct a chargeback for the transactions. Mr F said that he had not shared his security information or any two factor authorisation codes with anyone, and his Apple Pay devices were in his possession.

Revolut reviewed Mr F's disputed transaction claim but declined to refund the payments or raise a chargeback. In summary, they said this was because:

- *Mr F raised two chargeback claims through the VISA chargeback scheme. In Mr F's case, fraud chargebacks were raised which is applicable in cases where a payment is alleged to be unauthorised. Revolut did not have any dispute rights in this case as they had not found evidence of fraudulent activity on Mr F's account.*

- *Apple Pay requires either a passcode or biometric authentication. Therefore, it requires the physical presence of the device owner.*

- *For a card to be linked to Apple Pay, a verification code is sent to their phone number which clearly sets out what the code is for and not to share it with anyone else.*

- *As the transactions were authenticated this way, there was no valid chargeback under the card scheme rules and so Revolut were required to reject it.*

- *The terms and condition of Mr F's account stated that they would not refund any money lost if someone intentionally or carelessly failed to keep their security details or card safe.*

Unhappy with their response, Mr F escalated his concerns to our service. One of our investigators looked into what had happened and did not recommend that Mr F's complaint be upheld. They could not determine a point of compromise for Mr F's device, card details or security details such that someone other than Mr F or someone acting on his behalf could have completed the transactions.

Mr F remained dissatisfied. He said, in summary:

- *The investigator had shown a lack of understanding of security flaws and exploits;*
- *They had not considered cyber security exploitations that could happen such as sim clone and one time bypass attacks;*
- *They had said that it seemed strange that an unknown third party with access to Mr F's account would spend approximately £335 and stop spending when there were still funds remaining in the account. But Mr F explained he had cancelled the card and blocked the merchant which prevented them from emptying his account.*

As no agreement could be reached, the case has been passed to me to decide.

What I've provisionally 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 am minded to reach the same conclusion as our investigator, and for broadly the same reasons. But, as I have gone into more detail it is only fair to give both parties a chance to review my current thinking and provide any further information they may have. If nothing changes, my final decision will likely be as follows.

Generally, Revolut can hold Mr F liable for the disputed transactions if the evidence suggests that it is more likely than not that he authorised these payments or gave someone else consent to make them on his behalf. I am satisfied from my review of Revolut's technical evidence that the payments were authenticated utilising Apple Pay. But regulations relevant to this complaint state that authentication alone is not enough to enable Revolut to hold Mr F liable. So, I need to think about whether the evidence suggests that Mr F consented to these transactions – which could include allowing someone else to make them on his behalf. Having done so, on balance, I think that Mr F must have made or otherwise authorised these transactions.

The technical evidence provided by Revolut shows that Mr R's card had been 'tokenised' – that is added to Apple Pay – numerous times. Twice on one date in late January 2024, once more on another late January date, and once in early April 2024. There are two methods by which a card can be tokenised. The first, which was used on the first two times Mr F's card was tokenised, involves the customer signing into their Revolut account, opening the cards tab and selecting to add it to Apple Pay. The technical data shows that only one device was used to access Mr F's Revolut app during the period surrounding the disputed transactions, and Mr F has told us that no one else had access to his device. So it seems unlikely that either of these occasions of his card being tokenised by this method could have been completed by someone other than him.

The other way in which Mr F's card was tokenised involved using the wallet app within a phone. The customer would need to add their card details which includes all of the information including the card verification value 'CVV' code, which is then verified by a one-time passcode 'OTP' being sent to the registered phone number of the account holder. Mr F

has suggested that he did not disclose his OTP to anyone else, but that there could be a possible scenario that this was obtained through a cybersecurity flaw or exploit. He has suggested that a potential explanation would be that a sim swap fraud occurred. A sim swap fraud takes place when a fraudster tricks a mobile phone network provider into moving the phone number onto a sim or device controlled by the fraudster. But when this happens, the number would no longer remain on the sim or phone of the customer. And given that Mr F has given our service the same phone number that was registered with his Revolut account at the time of the disputed transactions, it does not seem this is most likely what happened here.

Mr F has also suggested it could be down to other cyber security exploits such as one time passcode bypass attacks. This can include malware infecting a device, phishing emails or websites, keystroke monitoring software or similar. But, considering the available evidence including Mr F's own testimony that he works in a cybersecurity role, that he has never clicked on any suspicious links or messages or handed over any of his details, this does not seem the most likely scenario here. I've not seen any evidence even within Mr F's testimony that explains how his device might have been compromised, such that someone would have been able to access his OTP. And I've thought more broadly about the kind of things customers with infected devices experience and have not seen any of the hallmarks of this here. Further, there was a gap of nine days between the last time Apple Pay was added for his card and whilst it is not impossible, it would seem strange that an unknown third party with access to Mr F's Apple Pay would wait to profit from this in some way. Though I would agree with Mr F that our investigator's remarks that an unknown third party with access to his card would have drained more of his available balance are not wholly true. I say this because further spending was prevented due to Mr F blocking the retailer and card.

I have to decide what is most likely, on the balance of probabilities, happened in the circumstances of this complaint. And my current thinking is that it is most likely that Mr F or someone acting on his behalf completed the payments to the e-commerce provider. I will review any further information submitted by the deadline prior to reaching any final decision.

My provisional decision

My provisional decision is that I do not uphold this complaint."

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.

Following on from my provisional decision, I did not receive any further evidence or comments from either party. So, for the reasons I explained in my provisional decision, I am unable to uphold this complaint and will not be asking Revolut to do anything further.

My final decision

I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr F to accept or reject my decision before 31 July 2025.

Katherine Jones
Ombudsman