DRN-5694139

The complaint

Mr F complains that Revolut Ltd won't refund transactions he didn't make or allow anyone else to make.

What happened

In June 2024, Mr F contacted Revolut and disputed several transactions totalling just under £20,000 which had debited his e-money account with it within the space of an hour. He said he hadn't made them or allowed anyone else to, but that he had received a suspicious call earlier that evening from someone claiming to be from Revolut. Mr F said he terminated the call when the caller started asking for his card details.

Revolut declined to reimburse Mr F on the basis that the transactions were made through Apple Pay, which was set up using Mr F's card details and a one-time passcode (OTP) that was sent to his registered device which was in his possession. It said the transactions couldn't be treated as fraudulent given how they were made and there were no grounds to raise a chargeback.

Unhappy with this outcome, Mr F complained to Revolut and subsequently referred the complaint to the Financial Ombudsman Service. In summary, he said he didn't authorise the addition of his card to an Apple device and Revolut hadn't provided evidence of this either. Mr F also questioned why Revolut didn't permanently block his card despite its records showing that several transactions were flagged as fraud and declined by its systems.

Our Investigator was satisfied that the Apple Pay token which was used for the disputed payments was created shortly after Revolut sent the associated OTP to Mr F's device. They noted that as the digital token could not have been created without the OTP, which only Mr F had access to given he'd confirmed that no one else had access to his device, then it must have been shared with a third-party. The Investigator concluded that as the evidence didn't support Mr F's submission – that he didn't disclose any details with a third-party – they couldn't rule out the possibility that Mr F gave his consent for someone else to complete the payments on his behalf.

The Investigator noted that Revolut did stop a payment and froze Mr F's card (including the digital token). But its records also showed that Mr F's device, which only he had access to, logged on to the Revolut app to confirm that the payment in question was recognised, and to unfreeze his card. Given that evidence from the time contradicts Mr F's position that he was not involved, the Investigator wasn't persuaded that Revolut could have prevented the payments.

Mr F disagreed with the Investigator's conclusions and asked for his complaint to be reviewed by an Ombudsman. In summary, he said no evidence had been provided to demonstrate that he approved the setting up of the Apple Pay token, or that he unfroze his card. While the complaint was awaiting an Ombudsman's review, the Investigator shared an extract of the technical audit data from Revolut's record with Mr F which they said showed that his card was unfrozen from his device.

After the complaint was passed to me, I contacted Mr F and said that based on the available information I was satisfied that he'd likely fallen victim to an impersonation scam. I also said that although I acknowledged Mr F's reservations about the technical evidence provided by Revolut, I was satisfied that the OTP that was needed for a third-party to set up Apple Pay on their device was sent to his phone. I noted from the account activity log that Mr F had accessed his account via the Revolut app on his phone at the time the OTP was sent. But, contrary to the Investigator's finding that it was accessed in-app, the OTP records showed that it was sent via SMS to Mr F's registered phone number. And as he'd told us that no one else had access to his phone, then the OTP must have been disclosed to the scammer. Otherwise, they wouldn't have been able to finish setting up Apple Pay on their device.

I also noted that Mr F's phone logged in after Revolut had frozen his card. And the activity log showed that it was his phone that reviewed the relevant screens which then led to the card being unfrozen.

Also, I highlighted to Mr F that in his email to Revolut – which was sent a couple of hours after the disputed payments were made – he said he was 'online' with Revolut and that his account was being 'recreated'. While he was checking that everything was above board, in my view, the email also indicated that he was in communication with the scammer even after the payments had been made, seemingly in relation to securing his account – which is consistent with the premise of an impersonation scam.

I explained to Mr F that I needed to understand why he took the steps he did, i.e., the sharing of the OTP, the unfreezing of the card, communicating with the scammer post payments, etc. I said that if I had a better understanding of what he thought was happening which led him to take those steps, I'd be able to properly assess how he would have likely reacted if I were to conclude that Revolut should have intervened again when the payments continued. I also said that without an explanation, I couldn't reasonably conclude that it would be unfair to hold him liable for the payments, or that Revolut could have prevented or limited his loss.

In his reply, Mr F said he terminated the call when the caller requested his card details. Suspecting that his account had been compromised, he moved funds to another account with a different provider. Subsequently, as nothing untoward had happened and he had several scheduled payments due to go out from his Revolut account, Mr F moved the funds back into his Revolut account. Mr F also said that while he accepted that Revolut's technical data shows an OTP was sent, it doesn't evidence how the code was obtained by the scammer. He said the conclusion that the code must therefore have been shared appears to be an inference rather than something directly evidenced by the logs themselves. Mr F also said that while he appreciates his device was logged in at the time the card status was changed from 'blocked' to 'active', the log only records the status change – it doesn't identify a specific user initiating that change.

In relation to still being in communication with the scammer after the payments were made, Mr F said that the timestamp of the email reflects when he eventually found a working email address for Revolut rather than the moment when he first attempted to notify it of his suspicions.

As I've had a reply from Mr F, it's appropriate for me to progress matters to the next stage.

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.

Under the relevant law – the Payment Services Regulations 2017 (PSRs) – the starting point is that Mr F is liable for payments he authorised, and Revolut is generally expected to reimburse unauthorised payments.

Where a payment is authorised, that will often be because the account holder has made the payment themselves. But there are other circumstances where a payment should fairly be considered authorised, such as where the account holder has given permission for someone else to make the payment on their behalf or they've told their payment service provider that they want the payment to go ahead.

Where evidence is incomplete, missing or contradictory, my role is to determine what I think is more likely than not to have happened. I do this by weighing up what I do have and making a finding on the balance of probabilities.

Here, Mr F says that he didn't set up Apple Pay with his card or allow someone else to, nor did he make the payments with that token or allow someone else to.

Revolut says the following steps were needed to set up Apple Pay on a device at the time:

- Entering Mr F's card information on that device.
- The set up required the use of an OTP to be entered on that device when prompted.

It's unclear how the scammer got hold of Mr F's card information. Unfortunately, it's not always possible to establish how card details were compromised. Usually, the customer is tricked into disclosing this information during the scam call or by clicking on phishing links which could happen in the days or weeks leading up to the call. But data breaches can and do also occur, where stored card information reaches the hands of a fraudster without the customer's direct involvement.

That said, for an Apple Pay token to be set up, the card details aren't enough on their own. And this is where scammers socially engineer victims into disclosing OTPs or taking steps within their mobile app.

Having reviewed the technical evidence Revolut has provided in this case, I'm satisfied that the OTP required to complete the Apple Pay set up was sent to Mr F's registered phone number. In his most recent response, Mr F appears to also accept that this is what the data shows. But his argument is that this data doesn't show how the scammer obtained the OTP. Mr F is right – it doesn't. But that's because the code wasn't required to be entered or forwarded from within Revolut's app such that this specific action would also be recorded. The OTP was entered on the device where Apple Pay was being set up.

The technical data shows that an OTP to set up Apple Pay was sent via SMS. Moments later, an Apple Pay token was successfully set up. As no other OTPs were sent in relation to this activity, then the only logical conclusion is that it was this OTP – sent to Mr F's phone – that was used for completing the set up. As for Mr F's comments regarding the inference that the code must have been shared, if he's told us that no one else had access to his phone, and he told Revolut that he wasn't asked to and didn't download any screen sharing software, then the only plausible explanation for how a third party could have obtained that code is that Mr F shared it with them – either knowingly or after being tricked into doing so.

I've considered Mr F's comments regarding card unblocking and status change. I can see he accepts that the technical data shows his device was logged in at the time. Given what he's said about no one else having access to his device, I'm satisfied that this means *he* was logged in at the time. I understand the point Mr F is trying to make about Revolut's evidence, specifically the 'author' of the card status change appearing as 'system'. But the transaction

activity log, which Mr F also received from Revolut and has since forwarded to our service, shows the app activity at the time. In addition to showing that Mr F was logged in at the relevant time, the log also shows that he viewed the notification relating to the card block – the transaction ID of the push notification that was sent to his device matches the ID of the screen that was viewed after logging in. The activity log also shows that in less than a minute, Mr F's card was unfrozen – ready to be used again.

I appreciate that Mr F has reservations about Revolut's technical evidence. The audit data might not be presented in the form he would expect. But as there was only one device logged in at the time, which belongs to him, I'm satisfied that Mr F was logged in and it was he who went through the in-app steps involved in reviewing the transaction which had flagged as suspicious (and which led to his card being frozen temporarily). This includes confirming that he recognised the transaction and wanted his card unfrozen.

Technical evidence aside, if the scammer didn't need Mr F to share any information with them or take any steps in his mobile app, then it's not clear why they would have phoned him at all. It's clear from Mr F's email to Revolut from later that day that he was led to believe (even if only at first) his account was being 'recreated'. He submits that the timestamp of that email doesn't reflect the point at which he intended to send it. Even if that is the case, it doesn't change the premise of the scam as it was presented to him. Namely, that his account was compromised and needed securing. I'm persuaded that Mr F was tricked into taking actions which resulted in the payments he's disputing. There are, unfortunately, several ways in which scammers are able to trick customers which result in payments. This includes both convincing the customer to allow payments, as well as to give them the ability to make payments without the customers' knowledge.

Prior to issuing this decision, I gave Mr F an opportunity to explain what exactly happened on the day in question. But he maintains that his involvement was only limited to answering the call and hanging up as soon as his card details were requested. Without knowing why Mr F shared the OTP, I can't reasonably conclude that it was unfair of Revolut to treat the payments are authorised. Similarly, without knowing why Mr F confirmed that he recognised the payment which had flagged as suspicious, and why he asked for his to be card unfrozen, I can't fairly conclude that Revolut would have been able to stop the subsequent payments if I were to make a finding that it should have intervened again when they continued.

Once the payments were processed, Revolut wouldn't have been able to stop the funds from leaving the account. As these were card payments, I've considered whether Revolut should have raised a chargeback, and the likelihood of it being successful, once it was notified of the scam. Revolut says it rejected the chargeback request because the payments were approved via Apple Pay which requires stronger authentication, i.e., biometric or passcode authentication. It's correct that a payment approved in this way doesn't have grounds for a chargeback on the basis that it was unauthorised. I've thought about whether any other grounds apply in the circumstances, but it's a common feature of the scam Mr F appears to have fall victim to that the goods or services paid for are provided, but to the scammer rather than the customer whose card was used. Here, it's more likely than not that the merchant would have successfully defended any claim made on the basis that goods or services weren't received. So, on balance, it's highly unlikely that Mr F could have recovered his funds in this way.

In summary, I'm sorry that Mr F has been the victim of a scam. But for the reasons I've set out, I don't think Revolut has acted unfairly in holding him liable for the payments. And because of this, I don't think it needs to take any action in relation to this complaint.

My final decision

For the reasons given, my final decision is that I don't 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 9 April 2026.

Gagandeep Singh
Ombudsman