DRN-4863095

The complaint

Miss D is unhappy that Revolut Ltd ("Revolut") won't refund payments she says she didn't authorise.

What happened

Miss D says she fell victim to a safe account scam. She says she received a call from someone who said they were her other bank (Bank N) saying her account had been compromised. The scammers explained she needed to open a Revolut account and move her money to there to keep it safe. Miss D says she then realised her money was leaving the account with Revolut and soon after realised she'd been the victim of a scam.

Our investigator did not uphold the complaint.

Miss D did not agree so the case has been passed to me for a decision.

I am sorry it has taken so long to reach this 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.

In deciding what's fair and reasonable, I'm required to take into account relevant law and regulations; regulatory rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the time.

Where the evidence is contradictory, I reach my decision on the balance of probabilities – in other words, on what I consider is more likely to have happened in light of the available evidence and the wider circumstances.

The Payment Services Regulation 2017 (PSRs), which apply to transactions like the ones made from Miss D's account, set out when a customer should be held liable for transactions which happen on their account and when they shouldn't.

The starting position is that a customer is liable for transactions they've authorised. But Miss D says she didn't authorise the payments. Revolut says its evidence indicates that she did authorise the payments. So I first need to consider whether I think it is more likely than not that Miss D authorised the payments.

The PSRs explain that authorisation depends on whether the payment transactions were authenticated correctly and whether the customer consented to them. So, in order to establish whether the transactions were authorised, I need to consider whether the payment transactions were authenticated and whether Miss D gave her consent to them.

To establish the agreed form and procedure, I've reviewed the terms and conditions Revolut

has referred us to. Specifically with reference to card payments (which was the method used here) “we will consider the payment to be authorised by you unless: you let us know that the money has been stolen from your account; or you don't think we've carried out your instructions correctly.”

In this instance, the disputed transactions were authenticated through Revolut’s app on Miss D’s mobile phone. This was accessed through PIN/access code or facial recognition biometrics. All the transactions took place on 21 November 2023 – the same day the account was opened and the same day the fraud was reported in the in-app chat to Revolut. These actions were all done on the same mobile phone. Revolut’s records indicate that no other devices were present that day.

Miss D says she was told to download a remote access software which she says gave the scammers access and says she did not authorise any of the payments.

From the information I’ve seen, Miss D was using an iPhone at the time. Revolut’s system logs show that the app was accessed from an iPhone using the iOS operating system. This means Miss D’s phone wasn’t ‘jailbroken’ as it was using the manufacturer’s operating system.

The iPhone operators have also confirmed that remote access software Miss D says she downloaded is limited in terms of its functionality on devices using the iOS operating system – they have explained that whilst the software would have allowed a third party to see the information displayed on Miss D’s screen, it wouldn’t have allowed them to take control of her device.

Although Revolut hasn’t indicated that it detected remote access in this case, Revolut has previously confirmed to us that where remote access is detected on the consumer’s device, many of the screens within the Revolut app will be blacked out. So, in this scenario it isn’t generally possible to complete any meaningful functions via remote access in Revolut’s app.

All the payments were e-commerce ones. For a payment to be successful, the merchants had to know the customer's full card details which would then need to be entered into their websites. So, Miss D must either have done this herself or provided her full card details to the fraudsters on seven separate occasions (as seven cards were created and used to make the disputed transactions) to enable them to initiate the payments.

Revolut told us that the merchants instructed the payments to be authenticated via 3DS. This is an extra layer of authentication required. The 3DS requests show the name of the merchant and the transaction amount, before being approved. The first four payments were authenticated using the registered phone on the account, which was accessed with either PIN/access code or facial recognition biometrics, in the Revolut app. As there is no explanation as to how someone else could have accessed her physical device, I think it is more likely Miss D authenticated these herself. The rest of the payments made were automatically accepted without them needing to be confirmed in the app. Revolut explained that Miss D would have received a push notification in her Revolut application that required her to log in to the account to approve each payment.

So, I’m satisfied on balance that the transactions were properly authenticated.

Thinking about consent, in the context of the PSRs this isn’t the same as ‘informed’ consent. If Miss D used the agreed form and procedure for making a payment order (which she did), then she’s given consent. Given that Miss D would have needed to complete the agreed steps on the Revolut app on her phone, under the PSRs she’d be considered to have consented to the transactions. Even if she provided the scammers with

the details to carry out the activity – she still would be deemed to have consented to them (albeit she may have been tricked into doing so).

Given what I've noted above, as well as Miss D's recollection, I don't think it's plausible that someone other than Miss D could have authorised the transactions.

As I'm satisfied that the transactions were authenticated correctly and that Miss D consented to them, they're considered authorised. I accept, from her testimony, it's likely that she was tricked into doing so, but that's not a consideration under the PSRs when thinking about whether the payments were authorised. And that means that the starting position is that Miss D is liable for the payments.

In broad terms, the starting position at law is that a bank or EMI (Electronic Money Institution) such as Revolut is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And I have taken that into account when deciding what's fair and reasonable in this case.

The Lending Standards Board's voluntary Contingent Reimbursement Model (CRM) Code was in place at the time the payments were made. But Revolut wasn't signed up to the CRM Code, so it doesn't apply to Miss D's case

However, where the customer made the payments as a consequence of the actions of a fraudster, it may sometimes be fair and reasonable for a bank or an EMI such as Revolut to reimburse the customer even though they authorised the payment. An example of this would be if a payment instruction is sufficiently unusual or uncharacteristic for the usual use of the account.

In this case, Miss D didn't have an account with Revolut before the scam. She set it up as instructed and so there was no transaction history to compare the payments with.

There's also a balance to be struck between identifying payments that could potentially be fraudulent and minimising disruption to legitimate payments. Whilst banks and EMI's such a Revolut, have obligations to be alert to fraud and scams and to act in their customers' best interests, they can't reasonably be involved in transactions like the ones Miss D made.

Given this, and the relatively low value of the individual amounts involved and the fact that they were made to genuine merchants, I don't consider Revolut acted unfairly or unreasonably in allowing the payments to be made.

I've finally considered whether Revolut could have done more to recover Miss D's funds after it became aware of the scam. The transactions had already been made by the time Miss D reported the scam. They went to genuine merchants. The only potential avenue for recovering funds would have been via the chargeback scheme.

Whilst there is no right to a chargeback, a chargeback generally is only raised if there is a reasonable chance of it succeeding. But in this instance the merchants provided the services they were instructed to do - albeit Miss D was tricked into paying these merchants by the scammers. This means these payments are not recoverable by Revolut through the chargeback scheme.

In summary, I recognise that this will come as a considerable disappointment to Miss D. But in the circumstances, I'm not persuaded that Revolut can fairly or reasonably be held liable for her loss.

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 Miss D to accept or reject my decision before 12 June 2025.

Kathryn Milne
Ombudsman