DRN-4815715

The complaint

Miss S has complained that Revolut Ltd ("Revolut") failed to protect her from falling victim to an impersonation scam and hasn't refunded the money she lost in the scam.

What happened

The background of this complaint is already known to both parties, so I won't repeat all of it here. But I'll summarise the key points and then focus on explaining the reason for my decision.

Miss S says that on 17 November 2023 she received a text message that appeared to be from a well-known postal service. The message stated that a delivery attempt had been made but no one had been available to receive the parcel. Miss S has explained that as she'd previously missed deliveries she assumed the message was legitimate and clicked a linked contained within the message to arrange a redelivery. After choosing a new delivery time she had to pay a small redelivery fee, which she entered her card details to pay.

Three days later Miss S says she received a call from an individual ("the scammer") who claimed to be from her bank. The scammer told Miss S that fraudulent activity had been detected on her account. During the call the scammer asked if Miss S had recently responded to any text messages, particularly regarding parcel redelivery. When she said she had, he explained that her account had been compromised and that it needed to be secured. He told her that the bank had already blocked some suspicious transactions, which was why she couldn't see any fraudulent activity in her online banking app. But Miss S says the scammer told her that her account was still at risk and advised her to transfer her money to a Revolut account for safekeeping.

Miss S said the scammer was reassuring as he told her she wasn't alone in falling victim to this scam, as it had happened to lots of other people before her. She's described how he was polite and professional, and that he was able to give her details such as the name of her local branch, which made his story even more believable. The scammer then guided Miss S through the process of setting up a Revolut account and linking it to her existing bank account. As part of the setup, she received an authentication code via text, which she entered as prompted. Miss S then transferred £2,125 as three payments from her bank account to her Revolut account, on instruction of the scammer.

Once the payments reached Miss S's Revolut account the scammer told her to create a virtual debit card, and asked her to confirm the virtual card details, including the card number and security code, but reassured her that he would never ask for the expiry date. He said he'd asked for these details so that he could activate the card through the bank's system, and as Miss S was worried about the security of her account, she followed the scammer's instructions.

The scammer then told Miss S that Revolut had placed security restrictions on her new account, requiring additional authentication before she could use it. He said he would trigger a verification notification, which appeared in her Revolut app under the name of a company which I'll refer to here as "S". When she confirmed the notification as instructed, the

scammer said that the verification had failed due to a system issue and that they needed to try again. Shortly after, she received an email from Revolut asking her to verify her payment source by uploading a bank statement. She did this as the request appeared to be part of Revolut's standard security checks.

Miss S has described how the scammer made the scam seem legitimate as throughout the call he urged her not to discuss the situation with anyone, explaining that the fraudster might be monitoring her communications. Miss S has explained how this increased her anxiety and made her reluctant to ask anyone for help.

After a short break the scammer called Miss S again, as he said that the verification process hadn't worked and that they needed to repeat the steps. Miss S was unaware that this was in fact a payment to a cryptocurrency platform and believed it was part of the security process.

Miss S has explained that when she later checked her Revolut transactions, she noticed multiple attempts to make payments to S and the cryptocurrency platform, although most of them had been declined. But two transactions had been successful, one for £1,498.64 and the other for £634.08.

Miss S says that she received an email from Revolut warning her about a potentially fraudulent payment, but as she had poor mobile reception, she didn't see it immediately. She says it was only after a checking her account that she saw the two payments had been successful.

The next day Miss S unlinked her bank account from Revolut and contacted Revolut's customer service via the in-app chat. A Revolut representative confirmed that two transactions had debited her account and explained that the funds were now with the merchant. The representative told her that Revolut couldn't cancel the payments and that Miss S needed to submit a chargeback request. She did so and provided evidence of the fraudulent transactions.

Revolut declined Miss S's chargeback request on the basis that it didn't have chargeback rights, as it deemed that Miss S had authorised the fraudulent transactions using the card network's 3D Secure system, in which she was required to "Confirm" the payment in her Revolut app. The 3D Secure system provides an additional layer of authentication for card payments to help prevent fraud, whereby customers are required to authorise payments using an alternate method, such as in their bank's app or using an SMS security code, to ensure the transaction is being performed by the genuine customer.

Miss S made a complaint to Revolut as she said it didn't do enough to protect her from the scam, as it didn't give her any warnings about a suspected scam. She's said that she'd have taken note of any warnings given by Revolut, and consequently, the scam would've been uncovered before it was too late.

Revolut didn't uphold Miss S's complaint and in its response it said the payments had been authorised by Miss S, and as such, it wasn't able to raise chargebacks to dispute the payments with the merchant.

Miss S remained unhappy so she referred the complaint to this service.

Our investigator considered everything and didn't think the complaint should be upheld. He explained he thought that the questions Revolut had asked, and the warnings it gave Miss S, were proportionate to the risk presented by the payments in question.

As Miss S didn't accept the investigator's opinion, the case has been passed to me to make 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.

I'm sorry to disappoint Miss S but having considered everything I'm afraid I'm not upholding her complaint, broadly for the same reasons as our investigator, which I've set out below.

In broad terms, the starting position is that a firm is expected to process payments and withdrawals that its customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And in this case it's not in question whether Miss S authorised these payments from leaving her account. It's accepted by all parties that Miss S gave the instructions to Revolut and Revolut made the payments in line with those instructions, and in line with the terms and conditions of Miss S's account.

But that doesn't always mean that the business should follow every instruction without asking further questions or intervening to ensure requests coming from their customers are firstly genuine, and secondly won't result in harm.

I'd like to start by explaining that although I'm not upholding her complaint, I don't intend to diminish the impact falling victim to this scam has had on Miss S – financially and emotionally. I am in no way blaming Miss S for what happened to her, but in making my decision I have to decide whether Revolut is responsible – that's to say, whether I believe it ought to have uncovered the scam and failed to do so. And I'm afraid I haven't concluded that's the case.

I've firstly kept in mind that at the time the transactions were presented to Revolut, it knew less about them than Miss S did. So the starting point is that I'd expect it to make the payments in line with Miss S's instructions.

But I've also kept in mind the volume of payments that were attempted as part of the scam. I can see that prior to the two payments that successfully debited the account, Revolut declined 14 other payments.

How did Revolut intervene before the payments were made?

I asked Revolut for further information about why the two transactions were approved so soon after the 14 earlier transactions to the same merchant had been declined. And more specifically, I asked whether Miss S had done anything differently that led to the later transactions being approved.

Revolut has explained that its system initially identified the payments as high-risk and declined them as suspicious activity. Following this, Miss S was notified via both a push message to her mobile phone, and an email, letting her know that the payments had been declined due to a potential scam. Revolut says this stage was designed to prompt Miss S to check the risks involved before attempting the transaction again. It also explained that due to the nature of card payments, Revolut couldn't delay processing of the transactions, but instead declined them and asked Miss S to complete a "scam warning flow" before she could proceed with another payment of this type. In practical terms a scam warning flow is a series of informative screens which show scam-related scenarios and warnings relevant to the risks posed by common scams.

Revolut has provided evidence of the warning screens Miss S saw, and having reviewed them I'm satisfied they were clear and unambiguous. After the last declined payment, Miss S was directed (by mobile phone notification and email) to a warning that stated, "Protect your funds by being scam aware - There's a high risk that this payment is a scam." The page explained that Miss S would need to answer questions before she could re-enable payments of this type (that's to say with the same Merchant Category Code, or "MCC").

Miss S then confirmed that she recognised the payment and proceeded to the next step, where she was asked whether anyone was prompting or guiding her. She selected "No, I'm not being guided." A further warning was then displayed, specifically advising that "If someone is telling you to ignore these warnings, they're a scammer." Miss S then chose to continue.

Following this, Revolut then asked Miss S for the purpose of the payment, explaining that the information was used to help protect her account. She selected "Something else" from a list of options which included "To transfer to another account".

Given Miss S response to this question, Revolut's system displayed further warnings, highlighting red flags associated with scams, including "Be wary of unexpected calls. If someone on the phone urges you to do something quickly, hang up. Call the institution directly to verify it's them". Miss S was required to acknowledge this series of warnings before proceeding to the next stage.

Finally, Revolut required Miss S to confirm once more that she wished to proceed by directing her to a "Risk Agreement" screen. This screen warned that there was a risk of losing money and required her to acknowledge: "I understand and accept the risks tied to this payment. I will only proceed if I am confident that it's legitimate." Miss S typed her name to confirm and chose to proceed. I note at this stage she also had the option to stop the process by selecting "No, continue blocking," but she chose to continue.

Following this intervention payments to the merchant in question, as well as other merchants using the same MCC, were unblocked, and Miss S was free to make payments using her debit card.

Did Revolut do enough to warn Miss S?

Having carefully considered the way Revolut intervened before allowing Miss S to make the payments seen in this scam, I'm satisfied that the extent of its interventions was proportionate in the circumstances. Revolut initially protected Miss S from substantial financial harm by declining the 14 transactions prior to the two that were authorised. Following this, Revolut's automated warnings based on the questions it had asked allowed it to provide sufficiently tailored scam information and warning messages before further transactions of the same type could take place.

Although I do understand Miss S was put under pressure to act quickly by the scammer, it's evident the warnings were designed to encourage her to pause and think, and the information they contained was sufficient to help her identify whether she was being scammed. It was only after its intervention – in which Miss S indicated she wasn't at risk of harm – that the payments were allowed to be made.

Revolut went some way to providing tailored warnings by asking Miss S for the reasons for the payments, but as it wasn't able to establish a specific reason, it gave Miss S a range of general scam warnings, including scenarios commonly seen in scams. And at least one of

those scenarios – in relation to receiving a phone call out of the blue and being pressured to act quickly – was relevant to what was happening in this scam.

I've noted that Miss S says she thought that authorising the payments to S using the 3D Secure pop-up in the Revolut app was the system the scammer was using used to unblock the account. I've reviewed what the 3D Secure popup would've looked like and whilst I accept Miss S was under pressure to act quickly, I don't agree it gives the impression that it is for the purpose of unblocking a card. In fact, it shows the merchant's name and the amount of the transaction being presented for payment, which I don't think would be the case if it were only unblocking a card.

Miss S also says Revolut shouldn't have removed her account restrictions after her account was opened due to the declined transactions happening around the same time.

Having thought carefully about this I'm not persuaded that the account restrictions were related to the scam, but instead appear to be related to Miss S's source of funds for her newly opened Revolut account. Miss S went through a separate process to verify the source of funds and have those restrictions removed. So they don't have a bearing on how Revolut dealt with the scam transactions taking place.

I've thought carefully about Miss S's point that Revolut's in-app question about whether she was being guided to make the payments wasn't clear enough, as she was having an anxiety attack. I've looked at an example of what the warning screens looked like and whilst I appreciate Miss S might not have found the question clear or particularly prominent, in my view it was a clear question. It was the only question on the screen and written in a large font covering approximately one third of the screen, and it was followed up with some further information on why the question was being asked. Even though the page including this question doesn't specifically refer to a scam, it's reasonable to assume the question needed to be answered honestly. But Miss S answered "No, I'm not being guided" to the question and Revolut was entitled to accept her answer and proceed to authorise the payments on that basis.

Having considered everything, I've concluded that Revolut's interventions before these payments were made was proportionate. It did ask Miss S additional questions about the two payments, and she firstly confirmed they were genuine by authorising them, and secondly confirmed she wasn't being guided to make them or on how to answer Revolut's questions. It also then gave her sufficiently clear and tailored warnings.

With all of the above in mind I haven't found that Revolut failed in its duty to protect Miss S from financial harm as I'm satisfied it took proportionate steps to intervene, albeit unsuccessfully on this occasion.

Recovery of the funds

As the payments were made using Miss S's debit card, the chargeback process is relevant.

Revolut considered raising chargebacks on the grounds of fraud, but it concluded it didn't have chargeback rights as it was satisfied that Miss S had authorised the payments, albeit that she later found out they were related to a scam.

Whilst I understand it'll be disappointing for Miss S to hear, I'm satisfied that Revolut acted fairly here. Chargebacks don't cover authorised payment scams, and for that reason, they're not a mechanism for a consumer to recover the funds they've lost as part of a scam.

I'm very sorry that Miss S has fallen victim to this scam and I do understand that my decision will be disappointing. But for the reasons I've set out above, I don't hold Revolut responsible for that.

My final decision

I don't uphold Miss S's complaint against Revolut Ltd.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss S to accept or reject my decision before 15 April 2025.

Sam Wade
Ombudsman