

## **The complaint**

Miss C complains that Revolut Ltd won't refund payments she didn't make from her account.

## **What happened**

Miss C says she realised that payments had been made from her account she didn't recognise and reported this to Revolut. All the payments were made on 11 August 2021 to a food delivery merchant. And came to over £1,000.

Revolut said it wouldn't be refunding this money. It said that it had found no evidence of fraud on Miss C's account. It said that the payments were made using the app. And there was no evidence of unauthorised activity. The payments didn't meet the criteria for a chargeback.

Our investigator recommended that the money be refunded to Miss C with simple interest of eight percent and £75 compensation. Revolut said that the payments were made with a 'virtual' card present only on the app. She didn't think it had been able to show that Miss C created this from her device. And this had been created in April 2021 and she didn't think it likely Miss C would have waited to use this. Revolut hadn't been able to show which device was used for the payments. She didn't think Miss C had authorised the payments and as these were 'distance contracts' Revolut was liable to refund them.

Revolut didn't agree and wanted the complaint to be reviewed. It provided information about the virtual card and how the payments were made. It said that it couldn't attribute them other than to Miss C or someone she'd allowed to use her account. It noted what the merchant had said to Miss C about the way the payments were made and that any issue would have originated from her Revolut account.

## *My provisional decision*

I issued a provisional decision on 24 November 2022. I set out below what I said.

I explained that I needed to take into account the Payment Services Regulations 2017 in considering this complaint. These state that a payment can only be authorised if it was consented to. So, it's not enough for it to be authenticated with Miss C's details. And if they weren't authorised Miss C wouldn't generally be responsible for them as in this case these were distance contracts.

So, I would be thinking about the following areas in looking at this complaint:

- What is the most likely explanation of what happened to the card details used for these payments?
- Did Miss C either authorise the payments on the account, or allow someone else to use the virtual card as Revolut says?
- Did Revolut act reasonably?

I said I wouldn't be able to say *exactly* what happened and I would be thinking about what is *most likely*.

I'd looked at the information about the virtual card on the account. This was set up on 29 April 2021. I could see that only one phone device had ever been used to access Miss C's account. Revolut says there's been no change to the password or other details to the account. I noted the time before the card was used and I thought it unlikely that if a fraudster had somehow created the virtual card it wouldn't have been used until August 2021. So, I found this was most likely created by Miss C.

I'd seen a record from Revolut showing that the virtual card details were used for the payments. And this has been confirmed by the merchant who also explains that the payments were verified using '3 D Secure'. Revolut says that this would have happened through the app. I was satisfied that the payments were authenticated with Miss C's details.

The issue is whether she consented to them. Miss C has said to this service that she had a passcode on the Revolut app and that she'd not written this down or shared it with anyone. She also said she had a passcode on her phone.

There was no use of the virtual card before the day of the disputed payments. There was no access to the app with any other device. So, the only way the card details could have been found out is through the app. And as I've said the merchant confirmed that a higher level of security was used to verify the payments.

That letter from the merchant does say that details were changed on Miss C's account with it. And so, I understand that this had been done on a merchant account Miss C had used for genuine orders before. The merchant said that as these disputed payments were made using 3 D Secure it wouldn't be refunding them and directed Miss C to Revolut as her bank account provider.

I appreciated the pattern of payments is unusual with so much ordered within a short space of time and from 10 payments. Almost all the money on Miss C's account was taken and she says she didn't notice this until an account fee took the account overdrawn in December 2021.

I didn't see any likely way in which an unknown third party discovered the card details. And Miss C has said to this service that "*I am vigilant and take good care.*" That leaves the possibilities of Miss C making the payments or her allowing someone known to her access to her details to enable this to happen – through what would be 'apparent authority'. And in that case even if she'd only say expected one order to be made she'd have consented then to what happened after that. A key point is that the person making the orders would have needed access to her phone at that time and she's not given any information say about that being somehow hacked or it being out of her possession. And even that wouldn't explain how the passcode on the app was discovered.

There was no indication about any concern from Revolut about these payments at the time. And as I'd said they were verified, and this meant that it didn't have a basis to attempt a chargeback. They wouldn't have been eligible under the relevant scheme rules and a chargeback would have been bound to fail.

I knew Miss C would be very disappointed with my provisional decision not to uphold her

complaint especially as I'd taken a different position to our investigator in my assessment.

### **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.

Revolut didn't make any further comments.

Miss C was given an extension from 22 December 2022 until 5 January 2023 to respond given the holiday period. Miss C indicated she'd like longer to advocate her case. But there were no exceptional reasons to extend this further and it was unclear what she'd be able to provide in addition.

She had a telephone call with our investigator which I've listened to, and she sent some further comments. Miss C said she was very disappointed and didn't know what else to do. She said that the payments by their nature were clearly fraudulent, and this was a huge amount of money. Miss C considered that there must have been a data breach as she was vigilant and was sure that she had kept her details safe and didn't believe that she was the point of entry for a hacker. And this virtual card which she accepted she'd created had never been used before. She wasn't suggesting someone had taken her phone and she said there must be other cases where there's been a system breach. She emphasised that she hadn't made any fraud claim at any financial business before. And she referred again to what the food delivery merchant had said in its letter and that this was fraud.

I accept that the main point suggesting fraud is the nature of the payments and that they came within a short period. As I referred to in my provisional decision the letter from the food merchant isn't in my view clear evidence of payment fraud though. What it says is that the payments were made and authorised using strong customer authentication (3 D Secure). And it says it did this because it had detected changes to her account. So, it won't refund them and says the bank involved with the payments should. It says that its systems weren't compromised. And access to Miss C's account with the merchant to make any changes was due to a password 'likely' being leaked from another platform.

But this doesn't deal with how the payments were made. I'm going to summarise some key points about that:

- Miss C does accept she set up the virtual card and this had never been used before these disputed payments.
- The payments were made using this virtual card.
- There was no new device registered to the account for these payments.
- The payments were authenticated using strong customer authentication.
- Miss C says no one had access to her phone or passcodes and that she kept these secure.
- The only way the payments could have been made was through the app. I can expand on that now and say that even if say her card details had been somehow leaked or compromised and about which there is no evidence and so likelihood – then that wouldn't necessarily help explain how strong customer authentication was made through the app on a recognised device.

I need as I said in my provisional decision to consider the most likely explanation taking into account the evidence. And to decide whether it's reasonable for Revolut to hold Miss C responsible for these payments. Having balanced all the factors and Miss C's testimony I'm afraid I remain of the view that the most likely explanation is that these payments were authorised. And so, I don't have a reasonable basis to require Revolut to do anything more.

If Miss C doesn't accept my decision she remains free to pursue this in court subject to any relevant time limits.

### **My final decision**

My decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss C to accept or reject my decision before 17 February 2023.

Michael Crewe  
**Ombudsman**