

## **The complaint**

Mr M complains that Revolut Ltd didn't protect him when he fell victim to a Safe account scam.

## **What happened**

Mr M received a call from someone purporting to be his bank. They explained there'd been unusual activity on his account and asked him to confirm if a payment to a gym was him, which Mr M confirmed it wasn't. They listed other transactions Mr M hadn't made and so persuaded him to move his funds out of his bank account to his existing Revolut account to keep them safe, as they said his bank account was compromised.

The scam went on for over a week, with Mr M receiving daily calls from the scammer to arrange for funds up to his daily bank account limit to be moved over to Revolut. He said they asked him for different parts of his security details each day, so would've acquired his full PIN and password for his bank account. But Mr M says he never shared any Revolut details with the caller. However the scammer was actually spending all the funds Mr M moved to Revolut, using a virtual card set up on their device.

Mr M has explained the scammer also told him to delete the Revolut app so that the hacker couldn't compromise these funds too. Mr M says this prevented him from realising the scammer was somehow moving money out of his Revolut account. However Mr M has also told us that he did reinstall the app at one stage, and this caused his phone to shut down. He later explained he did see transactions leaving his Revolut account when he reinstalled the app, but the scammer assured him these were to trick the hacker into thinking the account was empty.

Mr M reported all the transactions out of the Revolut account as unauthorised and done by the scammer without his consent. Revolut didn't uphold his complaint as it said that Mr M had shared a code with the scammer to enable them to set up the virtual card. And that there were no recovery options for the card payments once they'd been made. Mr M brought his complaint to our service.

Our Investigator didn't uphold Mr M's complaint. She said the evidence we held indicated he must've shared the code with the scammer to allow them to make the payments. She concluded that Revolut ought to have intervened during the scam, but said she couldn't safely say this would've unravelled it. Mr M disagreed and maintained he hadn't shared any of his Revolut information with the scammer. And maintained the scam would've unravelled if he'd been contacted. So the complaint has been passed to me for 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.

The starting position in line with the Payment Services Regulations 2017 ("PSRs"), the relevant legislation here, is that Mr M is liable for payments he's authorised, and Revolut is

liable for unauthorised payments.

For a payment to be regarded as authorised, the PSRs explain what steps must be completed. They set out that the payer (Mr M) must have given their consent to the execution of the payment, or a series of payments. And this consent must be given before, or if agreed between parties, after the payment; in the form, and in accordance with the procedure, agreed between the payer and the firm; and can be given via the payee or a payment initiation service provider.

In this case, Mr M says the payments were unauthorised and made by a third-party without his knowledge. As above, the PSRs set out that consent is given by three things – the key one here being that consent must be given in line with what has been agreed between Mr M and Revolut. So that is what I need to consider.

Revolut's terms don't specifically set out the steps for authorising a payment, but instead set out that all card payments made, bar certain situations, would be considered authorised. Revolut has shared the practical steps required to add a virtual card – and evidenced these would need to be completed for one to be used.

Revolut has shown that Mr M's virtual card was added to a new device on 18 November 2022. To add the card, the scammer needed to know Mr M's card details and follow steps on their own device to add this new card. This then generated a text message to be sent to Mr M's registered device containing an OTP (one-time-passcode). This code needed to be entered onto the new device to finalise adding and activate the card.

Revolut has shown it sent this kind of text message to Mr M's registered mobile device – and at this time Mr M has now confirmed it was received by him. And we know the card was successfully set up on the scammers device and then used for all the disputed payments.

So the evidence indicates that someone using Mr M's trusted mobile device received the OTP and shared it with a third-party, allowing them to add the virtual card to their device. Mr M has confirmed he had his phone in his possession and didn't download any third-party software or press any unknown links. I recognise that Mr M didn't complete all the steps himself in this case and that a lot of the procedure was completed by the scammer. But without Mr M's involvement, the scammer couldn't have set up the card.

Mr M, via his representative, originally told us he didn't receive a text message from Revolut on 18 November 2022. However after our investigator issued her assessment, Mr M provided us with a copy of the text message, alongside others he'd also received from Revolut relating to the time of the scam. But he maintains he didn't share the code. Mr M's testimony/recollections have therefore changed over time, and this makes it more difficult to place weight on what he is saying, especially enough weight to consider his testimony more likely than the contemporaneous evidence Revolut has provided.

Based on the evidence I hold, it seems Mr M must've shared the code which allowed the third-party to set up this card on their device. The text message is clear about what the code is for. And Mr M hasn't provided any alternative explanation for why he shared this. So, I can't safely conclude Mr M didn't authorise these payments, meaning they must be treated as authorised.

As I've considered Mr M authorised the payments, I've then considered whether Revolut missed an opportunity to prevent these funds leaving his account. Or to recover or reimburse him for them at a later date.

In broad terms, the starting position in law is that an Electronic Money Institution (“EMI”) such as Revolut is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the PSRs and the terms and conditions of the customer’s account.

But, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in 2022 that Revolut should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;
- have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers) and the different risks these can present to consumers, when deciding whether to intervene.

I’m in agreement with our Investigator that Revolut ought to have had concerns Mr M might be at risk of financial harm when the scammer made the 4<sup>th</sup> payment on 19 November 2022, as this meant the spending on the account that day went over £6,000, so a high amount and out of character for the account compared to previous usage. So I think Revolut shouldn’t have processed the payment for £3,077 until it had spoken to Mr M and checked what was going on.

Mr M says speaking to Revolut would’ve unravelled the scam, as two individuals from the same fraud company contacting him would’ve flagged to him as a concern. But the challenge with this case is that Mr M’s recollections and the evidence we have don’t match.

I recognise that the spending pattern and value of the transactions made were out of character for Mr M’s account. But because I don’t have the full context of this scam or know why Mr M shared the code which allowed the scammer to set up the virtual card, I can’t be sure what he’d have said to Revolut if it had spoken to him. The scammer was able to persuade Mr M to share the code and allow them to have a virtual card. And his testimony is that they persuaded him a loan he received paperwork for wasn’t something to be concerned about and that he should move these funds. So it seems possible, even likely, they’d also have persuaded him they were genuine and the agent at Revolut wasn’t to be trusted.

Overall, I have considered what Mr M has told us would’ve happened, but this is provided with the benefit of hindsight and we’re aware he hasn’t shared all the circumstances of the scam. With this in mind, I can’t safely say that had Revolut stopped some of the payments and spoken to Mr M, it would’ve prevented the loss. As I don’t know exactly what was going on with the scam or why Mr M shared the code, I can’t fairly conclude that a conversation with Revolut during the scam would’ve unravelled it.

I have then considered whether Mr M’s funds could’ve been recovered by a chargeback claim, but I’m in agreement with Revolut that his circumstances wouldn’t meet the criteria to successfully claim. And as the disputed transactions are all card payments to genuine merchants, there are no other ways Revolut could’ve recovered his funds.

I have considered the information Mr M has shared about his health and how that impacts

him. I acknowledge he has been through a difficult time and this impacts him adversely in stressful situations. But there aren't considerations for vulnerability in the PSRs, so this information doesn't change my outcome.

Whilst it's not clear exactly how the events unfolded, I do think Mr M has lost out financially as a result of a scam, and I recognise how difficult this is for him. But I can't fairly conclude that Revolut has done anything wrong here. I agree that in line with the PSRs, the payments would be considered authorised. And I can't safely say that Revolut could've prevented his loss, considering what Mr M has told us and maintains happened.

### **My final decision**

For the reasons set out above, I don't uphold Mr M's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 11 February 2025.

Amy Osborne  
**Ombudsman**