

The complaint

Mrs A complains that Revolut Ltd hasn't refunded unauthorised transactions on her account.

What happened

In February 2024, Mrs A was contacted by an individual about an employment opportunity. Mrs A was told she needed to make some payments as part of this opportunity, but that she'd receive this money back plus commission for her work. Mrs A sent payments over two days and received some funds back. On the third day, Mrs A says she was told the company needed to carry out some software checks on her device. Mrs A allowed them access through a remote sharing app and she says at this point they stole funds from her.

Mrs A reported the disputed transactions to Revolut but it didn't agree to refund them or uphold her subsequent complaint. Mrs A came to our Service, but our Investigator also didn't uphold her complaint. She asked for an Ombudsman to reconsider her case and maintained that she didn't make any of the payments on 22 February 2024.

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.

Were the payments authorised?

The starting position in line with the Payment Services Regulations 2017 ("PSRs") – the relevant legislation here – is that Mrs A is liable for payments she's authorised, and Revolut is liable for unauthorised payments.

For a payment to be authorised, it must be consented to by Mrs A or someone acting on her behalf. This consent must be given in the form and in accordance with the procedure agreed between Mrs A and Revolut. In practice this is set out in the applicable terms and conditions.

It's not in dispute the first three payments were authorised by Mrs A. She accepts making these payments as she believed she needed to use her own money to reset tasks she needed to complete, which would be later returned to her along with commission. So whilst Mrs A was tricked into making these payments under false pretences, they would still be considered authorised in line with the PSRs.

But Mrs A explains that she didn't authorise any payments that took place on 22 February 2024. Revolut has provided our Service with the technical evidence to show these payments were correctly authenticated and processed, but what's in dispute is whether Mrs A carried out these steps, or it was a third-party acting without her authority.

Mrs A says she received a call from the scammer that day and they told her they needed to do software checks to make sure she could continue to receive profits. She downloaded a screen sharing app and gave the scammer access to her phone. And she says from there, the scammer carried out all the payments. She says she couldn't stop the scammer and saw

questions popping up on her screen, but it was the scammer that responded to them.

Revolut has explained that its app can detect when remote software is in use and it has protections that prevent certain screens being seen when this is happening. It's said this blank screen would be shown for all screens relating to payments, including questions about a payment's purpose. It's explained that both parties will be shown a screen that only has the Revolut logo and a statement to explain the screen has been hidden.

As above, when Mrs A told us about what happened she was aware questions had been asked about some of the payments and that these needed to be (and had been) completed for them to go through. She says that the screen wasn't blank and that the protections Revolut has described to us were not in place. But, weighing up the evidence we have, I'm more persuaded it was Mrs A completing the payments now in dispute, which means it was her answering the questions too. I'll explain why.

Mrs A tops up her Revolut account on a number of occasions prior to and during the disputed payments and this is what funds them. She's explained why she did this, to unlock her account with the scammer and receive her commission. But I don't find this persuasive. First, it doesn't logically make sense she'd need money in her Revolut account to *receive* money she was owed from her work, especially as she did have a credit balance in her account at this time. But more importantly, if her testimony is accurate, it's very unclear why she then continued to top-up the account after she's said the scammer began stealing her funds.

Mrs A's testimony is that the scammer took control of her device and so she was watching them making payments without her consent. The first payment out occurs around 10:20am on 22 February 2024. But Mrs A then tops the account up with £1,400 at 12:30, which is subsequently spent in the same way. And top ups and payments continue until nearly 8pm that day. Mrs A hasn't provided a reasonable explanation for why she would keep funding the account the scammer was stealing payments from. It seems more likely she topped up the account to fund the payments as she was making them.

As set out, the payments occur over a number of hours and Mrs A had indicated she started multiple screen-sharing sessions. If Mrs A had funds unexpectedly taken from her around 10:20am, I would've expected her to report this to Revolut immediately and end contact with the scammer. It doesn't make sense that she'd continue letting them access her account for nearly ten more hours and to also top it up, when this was what then enabled them to steal her money. So I'm not persuaded this version of events is what happened and instead I think it was Mrs A carrying out these payments on her own device, due to the job scam she'd fallen victim to – and so they are authorised.

I therefore don't conclude Revolut has done anything wrong by determining these payments were authorised and that Mrs A is liable for them in the first instance.

Should Revolut have done more to protect Mrs A from this scam?

In broad terms, the starting position at 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 Payment Services Regulations (in this case the 2017 regulations) 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 February 2024 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;
- have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;
- 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 – (as in practice Revolut sometimes does including in relation to card payments);
- 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, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

Revolut recognised that Mrs A was at heightened risk of financial harm from fraud when making these payments and did intervene. I'm in agreement with our Investigator that this was a reasonable response to the risk identified for the earlier payments. It's arguable it could've done more than it did towards the end of the scam, but ultimately, I don't think any proportionate intervention by Revolut would have prevented Mrs A's loss. I'll explain why.

As our Investigator set out, a number of Mrs A's payments weren't processed when she initiated them and instead, she was required to complete a series of questions about what she was doing. Mrs A didn't answer these questions honestly. Revolut had an option available to her that related to the type of scam she was involved in – job scams – but she didn't select she was paying the funds as part of a job opportunity. Mrs A gave a number of reasons for the payments with varying detail about what she was doing, such as buying goods from an online retailer and saying she'd checked reviews for the retailer as well as that the price was realistic.

Considering the destinations of the payments and the amounts involved, I think Revolut acted to mitigate the financial risks identified when Mrs A was making the payments here. But Mrs A acted in a way to hide the actual risk. There were a number of failed/declined payments and this is when I think it's arguable Revolut ought to have probed Mrs A further about the payments. But considering I'm not persuaded she's been honest with us about what happened and as she wasn't honest with Revolut at the time, despite multiple opportunities to say why she was making the payments, I'm not persuaded Revolut could've unravelled this scam even if it had done more.

I've then considered whether Revolut could've recovered any of Mrs A's funds after the scam was reported, but I'm not persuaded it could have. I'm satisfied that in this situation chargeback claims wouldn't have resulted in the funds being returned. And there aren't other recovery options for funds, especially for the payments that were made by Push-to-card.

I accept Mrs A has been the victim of a cruel scam and has lost out financially due to this, but I don't think Revolut is responsible for her loss here.

My final decision

For the reasons set out above, I don't uphold Mrs A's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs A to accept or reject my decision before 21 August 2025.

Amy Osborne
Ombudsman