

The complaint

Mrs A complains that Revolut Ltd ('Revolut') won't refund the money she lost when she fell victim to a scam.

What happened

What Mrs A says

Mrs A says that on the morning of 14 December 2023 she received a call from someone who said they were from the security team at a large online retailer. The caller told her that someone was trying to use her account to buy two mobile phones and asked her to log into her account. Mrs A saw mobile phones in her basket. The caller said they could help to prevent the loss and asked Mrs A to download a screen sharing app. Mrs A was asked about the bank accounts she held.

Initially Mrs A was asked to open the app for her account with another bank and advised to click certain things to transfer money that could be sent back to her. Three transfers were made from this account that Mrs A's bank refunded to her under the Lending Standards Board's Contingent Reimbursement Model Code (CRM Code).

Mrs A was also asked to open a new account with Revolut and was given instructions on how to do so. She was told to transfer funds from a second bank account to the newly created Revolut account. The caller asked Mrs A to click things in the app and told her to ignore the messages that appeared. She was aware that funds were transferred from her other bank to her Revolut account.

Mrs A was then asked to open her savings account. At this point she became suspicious and declined to do so. The caller became nasty and told Mrs A that if she didn't do as directed, she wouldn't get any money back. At this point Mrs A hung up and contacted the two banks she had credited her Revolut account from to report that was the victim of a scam. She also emailed Revolut to report a scam transaction from her Revolut account (of £2,575). Revolut advised her to contact her bank.

Mrs A brought a complaint to this service. Revolut investigated Mrs A's concerns and said it wasn't liable for her loss. This was because it said she authorised the transaction from her Revolut account, and it provided appropriate warnings. Revolut also said that it had done what it could to recover Mrs A's funds.

When Revolut sent its file to this service it added the following points:

- Mrs A's account was opened on 14 December 2023, so it had no data to compare the transaction with. Also, one of the account opening reasons was to transfer funds, so Revolut had no reason to be concerned.
- When Mrs A set up a new payee she received a warning which told her that the name she entered wasn't the name on the account, so she ought to have known funds weren't going to an account in her name.
- Mrs A received a warning that asked her if she knew and trusted the payee. This warning said that scammers can impersonate others and warned that Revolut may not be able to help get the money back.

- Mrs A then received a further warning that said, “*Something doesn’t look right*” and that the transaction had been flagged as a potential scam. As a result, Revolut said it needed to ask some questions. Mrs A was asked for the purpose of the payment when she chose, “*Transfer to my other account*”, and was asked a series of questions including whether she was being assisted in completing the questionnaire, whether she was told to install software, whether she was told her account wasn’t safe and whether she had control of the beneficiary account. These questions weren’t answered correctly. Finally, Mrs A was presented with educational warnings but chose to continue. At this stage, Mrs A signed a risk agreement in which she confirmed that she had been warned that the payment was suspicious and of the risk of losing her money.

Our investigation so far

The investigator who considered this complaint didn’t recommend that it be upheld. She didn’t think Revolut could reasonably have been expected to prevent the loss. This was because there was no previous activity on the account, the transaction value was relatively low, and Revolut appropriately intervened by providing warnings and asking questions about the payment.

The investigator noted that Mrs A said she reported the scam in December 2023, but Revolut didn’t take any action to try to recover Mrs A’s funds until April 2024. Given that scam funds are usually moved out of a beneficiary account rapidly, the investigator said the delay in trying to recover Mrs A’s funds hadn’t made a difference.

Mrs A was unhappy with the investigator’s findings. She said she was the victim of a scam and was entitled to a refund. Mrs A also noted that her bank recognised she was the victim of a scam and refunded her. She doesn’t understand why Revolut didn’t do the same thing.

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 am required to take into account relevant law and regulations, regulators’ rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

Where evidence is unclear or in dispute, I reach my findings on the balance of probabilities – in other words on what I consider most likely to have happened based on the evidence available and the surrounding circumstances.

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.

I’ve carefully considered the evidence to determine whether I consider it to be more likely than not that Mrs A authorised the £2,575 transaction from her account. Overall, like the investigator, I’m persuaded that she did and will explain why.

I recognise that Mrs A is the victim of a scam and didn’t intend that her funds end up with a scammer. But I’m persuaded that she knew a transaction was being made from her Revolut account (although she likely believed funds were going to an account in her name).

When the investigator discussed this complaint with Mrs A, she referred to the specific questions Revolut asked when the transfer was made. Mrs A remembered the questions and

said the scammer told her to follow their instructions and what to click on. The questions asked by Revolut in the app included the following (with answers in italics):

- Is anyone telling you how to answer these questions? Is someone telling you which options to choose or telling you this is urgent? *No, I am not being assisted through this questionnaire*
- Why are you making this transfer? *Transfer to my other account*
- What kind of account? *Checking or savings account in another branch*
- Have you been asked to install software? *No, I was not asked to install any software*
- Were you told your account isn't safe? *No, I was not told my account isn't safe*
- Is the transfer to an account you control? *Yes, it's my existing account*

The questions posed by Revolut made it clear that a transfer was being made, so I'm satisfied the transaction was authorised, albeit that Mrs A didn't intend her funds to end up in the hands of scammers. Other evidence from Revolut, including the fact a passcode was entered from Mrs A's registered device when the payment was made, also point towards the transaction being authorised. And I note that Mrs A authorised payments from her bank as she was reimbursed under the CRM Code, which only covers authorised payments.

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 December 2023 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 – (as in practice Revolut sometimes does).

In this case, I'm mindful Mrs A didn't have an existing relationship with Revolut as the account was opened on the day of the transaction. This means that Revolut didn't have an understanding of Mrs A's normal spending patterns. The reason given for opening the account was to make transfers, and this is what happened.

But when Mrs A set up a new payee it was clear to Revolut that the account name provided by Mrs A (her name) wasn't correct. The value of the transaction was relatively low and so not concerning to Revolut, but I think it likely that this confirmation of payee no match result led Revolut to ask some questions about the transaction (as well as providing a standard new payee warning). I have set out above the questions Revolut asked to satisfy itself Mrs A wasn't at risk of financial harm.

The answers provided in response to the questions asked by Revolut were consistent with a genuine payment made to an account Mrs A had control of. Revolut went on to provide some educational messages that covered impersonation scams, being wary of unexpected calls, not giving anyone remote access, being told an account isn't safe and a warning that scammers will advise a customer to ignore the warnings provided.

Given the questions asked and warnings provided, together with the relatively low value of the transaction, I'm persuaded Revolut's response was proportionate, and it didn't need to take further steps.

Mrs A has referred to the fact that during the same scam she transferred funds from her bank which have been refunded to her. I have seen her bank's response, which says the refunds were made under the CRM Code. Whilst Mrs A's bank is a signatory to the CRM Code, Revolut is not. So, I can't consider Mrs A's complaint about Revolut under the provisions of it.

I turn now to whether Revolut did enough to recover Mrs A's funds. Revolut told this service that it attempted to recall Mrs A's funds within 24 hours of her reporting the scam in early April 2024. But Mrs A says she reported the scam to Revolut in December 2023, so I asked Revolut for evidence. Revolut found that Mrs A reported the scam to it by email on 14 December 2023, the day the scam took place. It didn't investigate what had happened at this stage, but referred Mrs A to the bank that held the account Mrs A used to credit her Revolut account. This service has obtained evidence from the bank that received Mrs A's funds to see if Revolut's delay prejudiced its chances of recovering Mrs A's funds. This evidence shows that Mrs A's funds were used up rapidly, and before Mrs A contacted Revolut. So, in the particular circumstances of this complaint, Revolut's delay didn't have an impact on Mrs A's chances of recovering her funds.

Overall, whilst I'm sorry to hear about Mrs A's loss, I can't reasonably ask Revolut to reimburse her.

My final decision

For the reasons stated, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs A to accept or reject my decision before 30 September 2024.

Jay Hadfield
Ombudsman