

The complaint

Mrs M has complained that Revolut Bank PLC won't refund transactions she says she didn't make or otherwise authorise.

Mrs M is also unhappy Revolut closed her account.

What happened

Mrs M held an account with Revolut.

Between 8 and 10 August 2022 just shy of £59,000 was paid into Mrs M's account, from a third party I will call Mrs D. The funds were then paid to a cryptocurrency exchange, which I will refer to as N.

At the time the transactions started Mrs M account balance was around £300.

Mrs M says she didn't make any of the transactions. She says she doesn't know Mrs D who deposited money into her account. And she did not send the funds onto N. She says she noticed that her phone was running slowly and believes her phone had been hacked.

On 11 August 2022, Revolut sent Mrs M a message asking her to get in contact with them about the activity on her account.

Mrs M got in touch with Revolut on 12 August. She said she discovered the activity on her account when she noticed emails from Revolut for each transaction in her email spam folder. She told Revolut she hadn't carried out any of the transactions and that her account balance had also been taken by the fraudsters. She explained that she isn't a technical whizz and couldn't explain how her phone had been hacked.

Mrs M has said that when she checked her mobile phone with a work colleague who was more technically savvy, she discovered that a QR code app had been downloaded onto it, which she hadn't done. Mrs M said she used her fingerprint to access her mobile phone and Revolut banking app. She also realised that her biometric fingerprint scan had been removed. She said she deleted the QR app and, noticed that a new payee – N, had been added to her account, which she hadn't done.

Mrs M reported the transactions as fraudulent to Revolut. She told Revolut that she did not authorise the payments and was not scammed into authorising them. She said they were made without her knowledge or permission, and she only found out about them after the fact.

Revolut held Mrs M liable for the payments in dispute, on the basis that they were made from her device and IP address, using her correct security details and one-time passcodes sent to her mobile number.

Revolut reviewed Mrs M's account and took the decision to close it with 62 days' notice. effect. Unhappy with this Mrs M referred her complaint to our service.

Our investigator looked into things but didn't think Revolut needed to do anything more. They were satisfied from the technical evidence that Mrs M's account was accessed by her known device, and they couldn't see how someone else could have accessed this device.

Mrs M disagreed, saying she had not been involved. She maintained that she hadn't carried out the transaction, had reported the matter to the police and she'd lost her own money. As no agreement could be reached the complaint was passed to me to decide. After looking at all the evidence I issued a provisional decision in which I said the following:
After reviewing the evidence, I've reached a different conclusion to the investigator.

Did Mrs M authorise the transactions?

The relevant regulations to authorisation of payments are the Payment Services Regulations 2017 (PSRs). The general principle in the regulations is that if Mrs M didn't authorise the payments, then she won't be liable for them. In this case Mrs M has denied making the transactions from her account to N. But the technical evidence suggests these were initiated from her known device.

In this case Mrs M has denied making the transactions from her account to N. But the technical evidence suggests these were initiated from her known device. However, there has been a suggestion that Mrs M's device could have been infected with malware. From my understanding it is possible for a device to have software that allows it to be accessed remotely, and in some cases bypass other security features to allow transactions to be made.

Revolut claims that it must be Mrs M that made the payments as they were done using her mobile device, which required security credentials. And there is no evidence that any other device was being used.

There's been no indication that Mrs M device was taken from her, or anyone else had access to her device. However, there has been a suggestion that Mrs M's device could have been infected with malware. From my understanding it is possible for a device to have software that allows it to be accessed remotely, and in some cases bypass other security features to allow transactions to be made.

Mrs M has told our service she'd spoken to a work colleague, and they'd removed a QR code from her mobile device. But she hasn't been able to demonstrate what was discussed, or how any malware could have been added to her device.

Revolut have said that their systems did not detect anything to suggest unauthorised or compromised access. That said, I'm persuaded that I should consider this issue of malware seriously. Firstly, the source of a lot of these funds, Mrs D, has brought a complaint to our service, against her bank, which I will refer to as M. Mrs D has said that her phone was infected with Malware in August 2022 after taking her phone in for repair, and more than £54,000 was taken from her account and sent to Mrs M's account.

From the evidence I've seen, a new payee – Mrs M was created on 7 August 2022 on Mrs D's phone at 03:14. A SMS text message, providing a new payee passcode, was sent to the registered mobile number at 03:14. Mrs D, or whoever had access to her phone, would have needed to input this passcode, select an effective warning and acknowledge they had read and understood the implications about potential fraud, in order to be able to complete the payee set up process, prior to making payment. The case was initially not upheld by M, as it was not possible to see how Mrs D's details had been compromised.

However, on 30 November 2022, M called Mrs D to tell her it had re-opened her case as new information had come to light that identified that her device could have been subject to a potential malware virus. This was based on the fact that the majority of the payments to Mrs M's Revolut account were made at around three am.

Mrs D confirmed that she was using her bank account as a savings account for her business so she could pay back her bounce back loan. She confirmed her old phone was broken as on 10 August 2022 it wouldn't come on, yet it had been working the night before. She put her SIM card in another phone. She took her old phone to the repairers. They said it could be the screen, but they couldn't fix the phone.

Later that evening she noticed the funds had been taken from her account. Mrs D also confirmed no-one else had access to the phone at the time. She didn't download anything that appeared suspicious at the time. She had no performance or battery issues at the time. M told Mrs D that there was a possibility that she had malware on her phone, meaning she had some kind of virus, which had allowed someone to gain access to her device and make the payments from somewhere else. M asked if Mrs D could take her phone to the manufacturer or anywhere where they could run a diagnostic report to see if there was any malware installed on the device.

Mrs D told M that when she spoke to another bank, she was told not to touch the device in case she corrupted anything that may be needed by the Police or M. So M, confirmed it would let her know where she could get the phone looked at, but that M would need the report to be able to see if M could refund her loss and reinstate her account following the closure.

On 1 December 2022, M called Mrs D and suggested she get in contact with Samsung. She could go online and book herself in for a repair or she could contact a support centre in London. Mrs D confirmed she would do this.

On 6 December 2022, Mrs D provided evidence from Samsung that had guided her to detect that there was malware on her device. It was disguised as an add-on to QR scanner.

On 9 December 2022, M emailed Mrs D to confirm it would be providing a full reimbursement of £54,905. This was credited to her account the same day. The account closure was also revoked, and Mrs D's online security credentials were reset in her local branch store.

M has accepted that their systems detected potential malware, albeit several days after the transactions to Revolut. This isn't necessarily conclusive. But it was enough for them to give Mrs D the benefit of the doubt and refund all the transactions. So, there seems to be links to malware in this case, and the links seem more than fanciful. I've also considered the wider circumstances of this complaint.

Looking over Mrs M's account history with Revolut, there doesn't seem to be any history of using or investing in cryptocurrency. It seems unlikely that she would suddenly decide in the early hours of the morning to invest any available funds in cryptocurrency. She's not mentioned speaking to someone about investing in cryptocurrency or falling victim to a scam.

Considering that funds were subsequently paid into her account, it would also need me to accept that Mrs M was likely running a sophisticated cryptocurrency scam across multiple accounts, including those she used for day-to-day spending. I've seen nothing to suggest this was the case, or that she has willingly allowed her account to be used to launder the funds from a scam. She's not claimed to Revolut that she knew about the funds being paid

into her account. Mrs M has been consistent that she doesn't know what happened on her account, and she seems genuinely confused about what has happened. Most significant though, is that after allowing a friend to examine her phone she found a QR app had been downloaded – which is what happened to Mrs D.

In the full circumstances of the complaint, I'm inclined to say that Mrs M's story is largely credible. On balance I'm persuaded that it's more likely than not she didn't authorise the payments from her Revolut account, and that they came about through access to her device by an unknown third party.

Mrs M hasn't claimed ownership of any of the funds transferred in from Mrs D, so it wouldn't be reasonable to award her any of these funds. So, from what I can see the loss she's suffered is her Revolut account balances, which was sent to the crypto exchange. As such, I think it's reasonable for Revolut to refund this directly to her. And add simple interest at 8% for loss of use of these funds.

Account closure

Revolut also took the decision to close Mrs M's account shortly after these disputed transactions. Revolut have a broad commercial discretion on who they provide accounts to. The terms of the account allow Revolut to withdraw banking facilities for any reason so long as they provide at least two months' notice. Revolut have done that here. So, I can't say they have treated Mr M unfairly when they decided to close her account. Mrs M didn't use the account for day-to-day spending and held a low balance at the time. So, I think the impact of Revolut's actions here would not be significant.

In summary I remain satisfied that it's more likely than not Mrs M's device was compromised in some way, which led to an unknown third party making unauthorised transactions. I've seen nothing to suggest Mrs M has failed in her obligation to keep her personalised security credentials secure – either intentionally or with gross negligence. I also think Revolut could have investigated more thoroughly – such as asking more questions. And contacting the sending bank – if they had done so, I think it's more likely than not they would have uncovered the wider picture of what happened here and came to the conclusion that Mrs M had more likely than not been the victim of a sophisticated fraud.

Under the relevant regulations I'm satisfied it's reasonable for Revolut to refund the Mrs M's account balance that was taken, and to add the 8% simple interest per annum to this amount to reflect the time without these funds.

Account closure and customer service

I have considered this point further based on what Mrs M has said about the stress that was caused. But I'm also mindful here that the primary cause of any distress is the unknown fraudster.

My provisional decision was that I upheld Mrs M's complaint and intended to direct Revolut Ltd to put things right by, refunding Mrs M's account balances along with 8% simple interest for loss of use of the funds.

Revolut didn't respond to my provisional decision. Mrs M agreed and made some further comments for me to consider. In summary she said:

- She has been a victim of fraud and is worried Revolut may have added her name to a fraud report which will impact her credit history.
- She wants a breakdown of her account statements and account balances.

- Will Revolut now offer to reopen her account.

Now both sides have had an opportunity to comment I can go ahead and issue my final 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.

It's disappointing that Revolut didn't respond to my provisional decision. Mrs M did so I will address her comments.

Mrs M is worried that Revolut have added a marker which will impact her credit file. I can understand Mrs M's concern here, especially as it appears Mrs M has been the victim of a sophisticated fraud. I've not seen any evidence that Revolut has loaded any markers against Mrs M. So, if Mrs M is experiencing any problems obtaining credit or opening other accounts, I can't say that this is more likely than not anything to do with this matter and that it is as a result of anything Revolut has done.

Mrs M has also asked if Revolut would be willing to reopen her account in light of my provisional decision. It's generally for banks and financial businesses to decide whether or not they want to provide, or to continue to provide, account facilities to any particular customer. Just as consumers usually have a choice of who they bank with. So, I won't be asking Revolut to reopen Mrs M's account. However, she is free to apply for an account with Revolut, which will be subject to Revolut's usual account opening checks and processes.

In summary, I see no reason to depart from my provisional findings. I remain of the view that this complaint should be upheld for the reasons set out in my provisional decision, which are repeated above and form part of this decision.

My final decision

For the reasons I've explained my final decision is that I uphold this complaint. To put things right Revolut Ltd should do the following:

- Refund Mrs M's account balances (prior to Mrs M receiving any funds from Mrs D) - that were taken when the disputed transactions to N were carried out.
- Pay Mrs M 8% simple interest for loss of use of Mrs M's account balances from 7 August 2022 up until the date of settlement*.
- Provide Mrs M with copies of her account statements.

*If Revolut Ltd considers that it's required by HM Revenue & Customs to deduct tax from that interest, it should tell Mrs M how much it's taken off. It should also give Mrs M a tax deduction certificate if she asks for one, so she can reclaim the tax from HM Revenue & Customs if appropriate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs M to accept or reject my decision before 16 January 2025.

Sharon Kerrison
Ombudsman