

## **The complaint**

Ms Z is unhappy Revolut Ltd won't refund a payment she sent as part of a scam.

## **What happened**

In August 2024 Ms Z says she found an advertisement on social media offering an account with Revolut. She registered her interest by leaving her details via an enquiry form. Afterwards, Ms Z was contacted by different people offering investment opportunities. Including someone from a company I'll call "E", who explained an investment involving cryptocurrency.

Ms Z was provided with documentation showing a company license and sent links to webinars, which persuaded her it was legitimate. She was instructed to purchase cryptocurrency and then send that onto an investment platform, where she saw her profits grow significantly. E's agents pressured Ms Z to invest more and more, with promises of larger returns, and offers to 'loan' her money to make the trades. So between August and October 2024 Ms Z sent close to €90,000 to E (as a mix of Euros and Swiss Francs). The majority of that money was sent from her Swiss bank account, at an institution I'll call "A". But €7,000 of it came from her account with Revolut.

Ms Z had opened the Revolut account in August 2024, and in September 2024 she transferred €7,000 into it from her account at A, which was the first deposit into Revolut. On 16 September 2024 Ms Z attempted to purchase cryptocurrency (at an exchange I'll call "B") with her Revolut card for the full balance. Revolut asked some automated questions and showed a warning, but it says Ms Z cancelled the payment. That caused the merchant to be blocked, so when she attempted the same transaction a few minutes later that also wasn't processed.

The following morning Ms Z tried a smaller amount, under the instructions of the scammer, to another account in an individual's name. Revolut again asked some questions and showed a warning, but says Ms Z chose to decline that payment herself as well. That evening Ms Z attempted to transfer the balance (€7,000) to different account details provided by the fraudsters – with her name entered as the beneficiary.

Before approving the transaction, Revolut asked Ms Z some automated questions in-app. She told Revolut she wasn't being guided or pressured. In response Revolut warned her that if she was being told how to answer its security questions then she was talking to a scammer. Ms Z then answered she was transferring money to her own existing account at a different bank, and that she had full control over it. She was also warned not to give anyone remote access. But the scammers had guided Ms Z on how to answer Revolut's questions, and told her the warnings were just standard messages.

Ms Z made the following payments from her Revolut account as part of the scam:

No.	Date	Time	Type/Payee	Amount	Result
1	16 September 2024	17.57	Card payment to B	€7,000	Declined
2	16 September 2024	18.10	Card payment to B	€7,000	Blocked
3	17 September 2024	08.57	Transfer to individual	€3,999.80	Declined
4	17 September 2024	17.19	Transfer to account in Ms Z's name	€7,000	Successful

Ms Z was persuaded to send further funds after this, but eventually realised that she'd been scammed and reported things to Revolut towards the end of October 2024. It attempted to recover the payments, but was unsuccessful. Ms Z then complained that Revolut ought to have prevented the loss, as it had declined some transactions before the one that went through – indicating it had reasons to suspect there was fraudulent activity on the account. She argued that meant Revolut ought to have blocked the final one too. Revolut's final response said it didn't think it was liable to refund the loss, as it had provided scam warnings and done what it could to try and recover the payment. Ms Z didn't agree with the outcome and so referred the dispute to our service for review.

One of our investigators looked at the complaint and didn't think it should be upheld. In his view, Revolut were right to intervene – but the questions that were asked and the warning provided on the final payment was sufficient. The investigator felt there were more accurate answers Ms Z could have given, and not doing so hid the true risks involved to Revolut. He thought it was reasonable to allow the final payment to leave the account based on what it knew about the circumstances.

Ms Z didn't accept the investigator's opinion, and argued that the scammers controlled her entire interaction with Revolut – telling her which buttons to click and to ignore the warnings, as just the standard process. There was a romance element to the scam, which meant she was particularly under the scammer's spell, and following their guidance. Ms Z also raised that her English isn't advanced, and so she might not have fully understood what was in the warning messages, or what she confirmed in response.

The investigator sympathised with the situation Ms Z found herself in, and why she felt pressured to follow the scammer's instructions. But he didn't think Revolut would have known she was being guided, or that she didn't fully understand what it was telling her. So, the investigator maintained that, in his view, Revolut had acted proportionately in the circumstances, based on the information it had available.

As no agreement could be reached, the complaint was passed to me for a final decision on the matter. Ms Z raised the following points for me to consider:

- Ms Z thought that if Revolut had a more flexible risk assessment system, it could have identified the suspicious behaviour in time and prevented the transfer. She argued the danger of standard questions is that fraudsters can easily adapt to them, which is why many banks introduce additional levels of verification to prevent fraud. She didn't think issuing standard warnings and automated questions was not enough when dealing with sophisticated fraud operations. She thought, in her circumstances, effective fraud prevention should have involved deeper intervention as clear risk factors were present.

- Before the successful transfer, several attempts were rejected. Ms Z thought that should have been a clear signal to Revolut that the transaction might be fraudulent. She believed that if the system recognised all the transactions as suspicious, it shouldn't have let the final one through.
- Ms Z thought Revolut's system hadn't assessed the situation comprehensively. If it had, it would have noticed the inconsistency between her responses and the suspicious nature of the transactions.
- She complained that Revolut does not offer live communication with customers in emergency situations, and thought that left people vulnerable.
- Ms Z raised that Revolut could have at least delayed the transaction and requested confirmation via a phone call or two-factor authentication.
- After the fraud occurred, Ms Z immediately tried to report the issue to Revolut, but the process was extremely inconvenient. All communication had to be done through the online system, which she doesn't think is suitable for urgent situations.
- As of 7 October 2024, new rules came into effect in the UK, requiring banks and financial organizations to refund victims of fraud in certain scenarios. Although these transactions occurred prior to the implementation of those rules, Ms Z believed that the introduction of such measures in the UK highlighted that protection against fraud and the prevention of similar incidents was an issue. She thought many banks, including Revolut, had not provided adequate protection for their customers, leading to an increase in such claims.
- Ms Z says the fraudsters specifically instructed her to transfer funds from her account at A, in Switzerland, to her newly opened Revolut account. She thinks the scammers were clearly aware that once the money was in Revolut, it would be much easier to transfer it onwards. Ms Z suggested that fraudsters specifically target Revolut because they know its security measures can be bypassed.
- The investigator had mentioned that even direct human intervention might not have helped in Ms Z's case – but she disagreed. She argued that studies and real-world scam cases showed that fraudsters deliberately isolate their victims and keep them under psychological pressure. Had Revolut spoken to her she thinks it would have disrupted the fraudsters manipulation, and the agent would have noticed inconsistencies in her answers. It also would have given her a moment to step back and reflect – which might have broken the fraudster's control over her.

I want to thank Ms Z for effort she went to in providing detailed replies, and the considered arguments she has presented in support of her case.

### **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.

Having done so, I'm not upholding Ms Z's complaint. I appreciate that will come as a great disappointment to Ms Z, who I know feels strongly that Revolut should have done more. I was also saddened to hear about how much the incident had affected her, and what a challenging situation the theft has left her in. She truly has my sympathies. There's no dispute that Ms Z fell victim to a cruel, sophisticated and very persuasive scam. But what I must decide is whether Revolut should reasonably have uncovered what was happening,

and prevented the loss. On balance, and having considered things very carefully, I don't find that Revolut likely could have in this case. I've explained my rationale below.

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.

In broad terms, the starting position at law is that Electronic Money Institutions ("EMI's") such as Revolut are expected to process payments and withdrawals that a customer authorises them 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 March 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 their 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 do);
- 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 has a difficult balance to strike in how it configures its systems. It needs to detect unusual activity, or activity that might otherwise indicate a higher than usual risk of fraud, whilst not unduly hindering legitimate transactions. There are many millions of payments made each day, and it would not be possible or reasonable to expect firms to check each one. In situations where firms do (or ought to) carry out checks, I would expect that intervention to be proportionate to the circumstances of the payment.

As Ms Z has pointed out, the disputed transaction in question was made before the Payment Services Regulator rules came into effect, and Revolut wasn't signed up to the voluntary scheme that predated those rules (The Contingent Reimbursement Model). That means I would have to be satisfied that a mistake was made by processing the final payment in order to award that loss. Revolut did intervene to ask some automated questions and provide warnings on all these payments (both the ones attempted and successful). So the question for me to decide is whether, in the circumstances, Revolut ought to have done more – and if so, consider whether that would have produced a different outcome.

Revolut correctly identified Ms Z was at risk of being scammed when making the €7,000 payment. It showed her screens saying something doesn't look right and that it could be a scam. It also asked her questions to narrow in on the potential risks involved, highlighted the importance of being honest, and gave scam warnings. I think that was fair in the

circumstances. I accept that the transactions made on the account up until that point indicated some risk (and so it was worthy of a check). But there weren't sufficient concerning factors present to warrant speaking to a human.

The account activity would have suggested to Revolut that Ms Z was thinking of buying cryptocurrency, saw the warnings presented, and then changed her mind (she cancelled it). It saw she attempted the same transaction ten minutes later, but the merchant code had been blocked. There were no further attempts to make any payments that evening, or to send money to cryptocurrency after that. Then Revolut would have seen that Ms Z attempted to send a smaller amount to a friend/family member the next day – but she was shown warnings, and again she decided not to go ahead with it. Finally, after a long delay, Ms Z seemingly sent the balance back to herself – to an overseas account in her name.

Here's what Revolut knew about the risks involved by the last payment:

- Ms Z had opened an account almost four weeks prior to the first transaction, and had told Revolut her intended purpose was cryptocurrency and transfers (among other things). So the (attempted) card payments to a cryptocurrency provider and transfers were in line with what Revolut were expecting, based on the account opening reasons given (albeit large amounts). Lots of people open accounts at Revolut for legitimate cryptocurrency purposes – so just the fact Ms Z was attempting to buy cryptocurrency was not necessarily indicative of a scam. But given the amount involved, an automated check from Revolut was reasonable.
- There wasn't any prior account activity for Revolut to compare these transactions to, in order to determine if they were out of character for Ms Z. But it did know they were larger payments, either going to cryptocurrency or internationally – which carry elevated risks compared to domestic payments or other purchases.
- The time gap between opening and making the first payments would also have suggested she wasn't under immediate pressure to send money when she applied for the account. It's more common in scam situations for transactions to be attempted soon after opening – so the delay there would have reasonably reassured Revolut.
- There were also time gaps between the transactions once Ms Z started spending – money was deposited in the account in the morning on 16 September 2024, and the cryptocurrency purchase wasn't attempted until the evening. The first transfer was then attempted the following day, with the payment that went through sent eight hours later. Those timings wouldn't have strongly suggested to Revolut that Ms Z was under pressure to move money quickly – as is common in scams.
- I accept it was somewhat strange for Ms Z to cancel two transactions in two days, but Revolut could reasonably assume its warnings had resonated and she wanted to carry out some further checks herself before continuing. It hadn't declined the payments due to fraud concerns, as her answers had provided reassurance she likely wasn't being scammed. No further attempts were made to cryptocurrency either, so the chances of her being involved in a cryptocurrency investment scam also decreased.
- The answers Ms Z had provided in app weren't particularly inconsistent – and most would have seemed plausible based on what Revolut knew about the transactions. She said the card payment to a cryptocurrency provider was sending money to her own account, which wasn't wrong (though there might have been better answers she could have given). The account at B would have been in her own name, as the card used for purchases at B has to match the name on the account (as is the case for

most exchanges, and Revolut would have been aware of that). The first transfer was to an individual's account abroad, for a lower amount, and Ms Z said that was to pay a friend/family member, and that she hadn't sent money there before – all plausible answers as far as Revolut were concerned. The final payment was supposedly going to an account in Ms Z's name, under her control, and again I've not seen anything that would reasonably cause Revolut to question that. The beneficiaries (and the amount on one of them) were all different too, so you'd expect different purposes/answers.

- The final payment was going to a different account to the one that paid the funds in originally – but that deposit had also originated from an account abroad, and people often have more than one account. So I don't think Revolut would have been concerned by that. It was draining the full balance, but that had only been there less than two days, and was going to an account under Ms Z's control (according to her answers).
- Revolut delayed sending the last payment by three hours, and told Ms Z it would, to give her time to pause, reflect and check she was happy. It could also be cancelled within that window if Ms Z decided she didn't want to go ahead, after researching or speaking to someone. That was done to allow an opportunity for the spell to be broken, in the outside chance she was being scammed.

I appreciate Ms Z doesn't think Revolut should have been reassured by her automated responses, as fraudsters can circumnavigate them. But these were dynamic warnings, which changed according to the answers given – and I don't agree that they can't be effective. In fact, they seem to have largely worked here given the first three transactions didn't go out. This type of intervention is employed by most banks and payment service providers, and backed by the regulators as well as codes of best practice for being effective (where it's proportionate to the risks). It also wouldn't be reasonable to expect a firm to call its customer on every transaction that potentially poses a risk – only those that really warrant it.

The warnings given to Ms Z were clear and very stark – Revolut effectively said that if someone is guiding you on these answers, or you've been asked to use screensharing software, then you are dealing with a scammer. Those messages, among others, should have resonated with Ms Z. I accept that the scammers were very convincing, and it's clear she was completely under their spell. That's not necessarily through any fault of her own I should say – the levels of manipulation and social engineering in this case were high. I also acknowledge there was a romance element to the scam, which would have made the fraudster's influence even harder to break. So I can understand to an extent why Ms Z didn't think the questions were that important, and the slight language barrier wouldn't have helped. But I don't accept she wouldn't have been aware on some level that she was misleading Revolut. It's people's adverse reaction to doing that which often makes them realise what's happening, and means this can be an effective intervention.

It's true that firms should be alive to the fact that customers can be coached to lie, or provided with cover stories during a scam. So Revolut needed to be on the lookout for inconsistencies in what it was told, and risk factors building. But in this case, I don't think there were enough concerning factors or inconsistencies to warrant a more in depth intervention on the last payment. Particularly, as I've set out in the bullet points above, there were lots of factors that Revolut could find reassurance in. I also don't think an obvious scam pattern had formed either (for instance, payments made in quick succession for escalating amounts). Ms Z was the one who had decided not to proceed with the earlier payments, rather than Revolut (though that seems to have been under the instruction of the scammer). So I don't find that Revolut made a mistake by not discussing the payment further with Ms Z.

I know Ms Z feels that if she'd have spoken to someone at Revolut it could have made all the difference, and I accept what she's said about the research into this. Revolut does offer live communication with its customers, via its chat function – and it also can call people in particularly risky situations. But I'm not convinced speaking to someone would have meant the payment wasn't sent. Ms Z was being guided, and that would likely have continued during any conversation using the chat function, and Revolut would have been reassured all was fine. She was also under pressure to get funds over to the scammer. So, even if Ms Z spoke to someone on the phone, given how under the scammer's spell she was, I think she'd have likely maintained the story that the payment was going to an account in her own name, under her control. I don't think there was enough going on that would have caused Revolut to really question that answer, or ask for proof – and the prior transactions could be explained away as her deciding not to go ahead after thinking about it.

Ms Z says speaking to someone would have given her time to pause and think. But the scam had been going on for weeks, with lots of opportunity to stop and reflect at various points, and that hadn't worked to break the spell. So I'm not persuaded chatting to Revolut would have changed that, or avoided the loss. Ms Z has raised some generalised concerns about Revolut's fraud prevention measures, but I haven't found they failed her here. I just don't think, unfortunately, this scam was one it could reasonably have been expected to uncover.

I've thought about whether Revolut could have done more to recover the payment, and I don't think it could have. The time that had elapsed between the transfer being sent and the fraud being flagged to Revolut meant any chance of recovery was unlikely – given scammers usually move funds on quickly. I appreciate Ms Z found the process of reporting the scam frustrating – but I can see that Revolut was responsive in the chat, and the larger gaps between messages came from Ms Z. I don't think a quicker process for logging things would have made a difference to whether any of her money could be recovered. I also haven't seen enough inconvenience was caused at any point to warrant compensation.

Having considered everything, and whilst I recognise that Ms Z has sadly had this money stolen, I don't think Revolut could reasonably have been expected to prevent the loss. So, I'm not directing it to refund the payment she sent.

### **My final decision**

My final decision is that I don't uphold Ms Z's complaint about Revolut Ltd.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms Z to accept or reject my decision before 24 July 2025.

Ryan Miles  
**Ombudsman**