

The complaint

Ms B is unhappy that Revolut Ltd won't refund the money she lost to a scam.

What happened

In March 2024 Ms B came across an investment opportunity involving cryptocurrency, offered through a company I'll call "T". She says she checked the company and it seemed to be legitimate and regulated. Ms B initially invested £200 from her bank account and saw her profits rapidly increase daily on the platform. She was then told for security purposes she needed to set up a wallet, at a cryptocurrency exchange I'll call O, in order to withdraw the profits. The scammer sent an email impersonating O, and told Ms B that she needed to transfer £5,000 to complete verification, and raise her trading account to a higher level. So she borrowed the money needed, and sent it from her existing Revolut account – which she'd had for a couple of years, but used infrequently.

Ms B was given the beneficiary details for the transfer by the scammer, which was an account at a bank I'll call "L". But that transaction actually purchased cryptocurrency from a seller through O's peer-to-peer (P2P) platform – which appeared on her statement as a transfer to an individual. Prior to allowing the transfer to complete, Revolut asked a series of automated questions in app. The answers to those included confirmation she wasn't being assisted, that she was paying back a family member or friend for something they purchased on her behalf, and that the bank details were provided face to face. Revolut subsequently showed Ms B a series of warning screens, tailored towards the potential risks identified from the automated answers given. She opted to continue with the transfer.

Once the purchase was complete the cryptocurrency was withdrawn to the scammer's wallet address. Ms B was told those funds would be returned to her after 24 hours, once verification was complete – but that didn't happen, and the trader strung her along with various excuses for the delay. After a few days Ms B found that she'd been blocked by the scammer on the messaging service they had been communicating on, and the platform had disappeared. She found T's contact details online, but it said it didn't have an account for her – and she'd likely been dealing with a clone. It was at that point Ms B realised she'd been scammed, and so she reported things to Revolut and Action Fraud.

Revolut investigated the fraud claim and said it hadn't been able to recover the lost funds, and declined to reimburse the payment as several preventive warnings had been shown. Ms B complained about the outcome, and highlighted prior decisions from our service, on cases she thought were similar, where we had said the banks had to pay back the stolen funds as the fraud security measures in place hadn't been adequate. Revolut's final response reiterated that it had provided warnings prior to the transfer and had done what it could to recover the money. As Revolut felt it had taken reasonable steps to protect Ms B, it didn't think it was liable to cover the loss in the circumstances.

Ms B wasn't happy with the response and so referred the complaint to our service for review. She told us she was struggling with the monthly loan repayments, and was also frustrated that she hadn't been able to speak with anyone over the phone at Revolut. She also felt Revolut ought to have been liaising with the payee's bank to retrieve the funds, and that L

had facilitated scammers. One of our investigators considered the complaint and didn't think it should be upheld. In his view, Revolut had provided proportionate warnings tailored to the purpose Ms B had selected during the transfer process. The investigator also thought Revolut had done what it could to recover the loss, but no funds remained in the beneficiary account when it contacted L.

Ms B didn't accept the investigator's opinion, and said the scammers knew when the loaned funds were paid into her account, and seemed to be able to masquerade as her when talking to banks and O. She thought the scammers had accessed her account and answered Revolut's questions prior to the transfer. Ms B clarified she had made the transfer, but questioned what proof Revolut had that it wasn't talking to the scammer when carrying out any checks and balances. She was adamant she would never have provided those answers to Revolut, though did remember some tick boxes and generic warnings being shown at one point. Ms B also referred to more decisions we'd made on different cases, where we directed Revolut to pay back some or all of the lost money due to failings in its fraud controls.

The investigator considered the further points raised, but maintained his position on the complaint. The decisions referenced involved different circumstances, with far larger amounts sent, and the payments identifiably going to cryptocurrency (whereas Ms B had paid an individual). He added that Revolut had controls in place to block out online banking screens when remote access or screensharing software was detected, so he didn't think it was likely the scammer's had been able to access the account. The investigator also pointed to Ms B's earlier testimony where she had said she'd processed the transaction herself.

As no agreement could be reached, Ms B requested that an ombudsman reviewed the complaint – so the matter was passed to me to decide.

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 the complaint. I appreciate that will come as a great disappointment to Ms B, who has sadly lost a lot of money to a cruel and sophisticated scam. I have a great deal of sympathy for what she's been put through at the hands of the fraudsters, and the continuing impact this had following the scam by having to maintain the loan repayments. But, on balance, I can't fairly say Revolut should be held responsible for the loss. I've explained why below.

In broad terms, the starting position in law is that a payment services provider is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the terms and conditions of the account and the Payment Services Regulations (PSR's). Ms B 'authorised' the transaction in question (she made it), albeit under the false belief it was for a legitimate investment opportunity. So Revolut was under an obligation to process the payment – but that isn't the end of the story, as far as Revolut's responsibility in the matter goes.

While that's the starting position, I've also taken into account the regulator's rules and guidance; relevant codes of practice, along with what I consider to have been good industry practice at the time. That means I consider Revolut should fairly and reasonably have been on the lookout for the possibility of fraud at the time, and intervened if there were clear indications its customer might be at risk.

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. Revolut gave automated warnings but didn't make further enquiries, via its chat function, with Ms B about this payment before processing it. So the question for me to decide is whether the disputed transaction ought to have looked concerning enough to have prompted more involved fraud checks.

This was a larger payment, and looking at the previous sporadic account usage it was out of character compared to the smaller transactions typically seen. So I think Revolut were rightly concerned Ms B might be at risk of financial harm when she put it through. It wasn't identifiably going to cryptocurrency though (it looked like a transfer to an individual), so Revolut wasn't aware of that risk. An obvious scam pattern hadn't formed yet either (e.g. escalating amounts in quick succession) with this being the only disputed transaction. People can also make one off larger payments without them necessarily being fraud related. So, while I think checks of some kind were warranted, I don't consider Revolut ought to have been concerned enough to need to speak with Ms B. An automated intervention, followed by a tailored warning based on the answers given, was proportionate to the risks that were apparent.

Revolut asked about the purpose of the payment, and some other questions about the circumstances to check for common risk factors and narrow in on the type of warning that would most likely capture the potential scam risk. That automated process didn't highlight any further concerning factors or inconsistencies that meant Revolut ought to have spoken to Ms B. The payment was going to an individual, so the context given of paying back a friend or family member for something they'd bought would have seemed plausible. The other answers selected (like the bank details being provided face to face) would also have provided reassurance to Revolut that it didn't need to take further action. Scammers frequently guide victims on how to answer security questions, so Revolut needed to be alive to that possibility – but I haven't seen anything it should have picked up on in that regard. It also displayed a clear warning that if Ms B was being coached through the process then she was dealing with a scammer. So I find Revolut acted fairly when it intervened, carried out automated fraud checks, and gave warnings prior to allowing the payment.

Ms B has said she made the transfer but doesn't remember selecting those answers during the process, and strongly states she would never have answered in that way. She does remember there being some boxes, and seeing warning screens she thought were generic – but speculates that the scammers must have had access to her account and answered those questions on her behalf. I find that option unlikely. The system evidence suggests face ID was used to open the app, and the same device (the one registered to the account from the start) was used to complete all the steps involved in the payment – including clicking the options presented to the fraud related questions. Revolut is also able to detect when a screenshare is in progress, and in response blanks out the screens for the customer and anyone remotely viewing. Ms B doesn't recall the screens being blocked out for any part of the process though. If the scammer had access to Ms B's account then I'm not sure why they would have needed Ms B to make the payment either, if the money was already there for the taking.

I agree it's weird the scammers seemed to know when the loaned funds had been paid into the account, and I can't explain how they knew that – whether it was a lucky guess or they had access to Ms B's emails for instance. I also don't think Ms B had full control over the wallet with O, which is how the scammers were able to withdraw the cryptocurrency once the £5,000 had been exchanged and paid to it. But, as I've not seen any evidence of third party access to the Revolut account during the transfer, I find it more likely that Ms B answered

the automated questions in app as part of the payment screens. Even if she didn't, I'm satisfied she authorised the transfer, and I don't think Revolut ought to have detected that the questions weren't answered by its customer – so it was entitled to rely on that information when assessing the fraud risk involved.

Ms B has referred to various decisions we've issued previously, where we upheld the complaints, and said those show she should be entitled to a refund from Revolut. She's argued the circumstances in those are similar to hers, and the decisions show that Revolut's fraud prevention controls weren't robust enough at the time. I've looked through those decisions, and all of them involve amounts far larger than the loss here (many times more in some cases), and usually multiple payments forming an obvious scam pattern, which are identifiably going to cryptocurrency. So the risks that ought to have been evident to the firms in those cases were far greater than what Revolut had in Ms B's scenario – and I don't think they are comparable. In any event, Revolut did correctly identify she might be at risk of being scammed, and intervened to provide warnings – those just didn't resonate, due to the answers provided during the automated checks.

I've thought about whether Revolut could have done more to recover the loss when the matter was reported, and I've decided it couldn't have. It did reach out to the receiving bank, and no funds remained at that point to recover – but I'm not persuaded the individual Ms B paid was part of the scam anyway. I find the evidence suggests he was likely a legitimate P2P cryptocurrency seller – and the screenshots provided of her wallet show cryptocurrency was provided in exchange for the funds (it was just withdrawn by the scammers). Ms B didn't have full control over the account with O, and I know she later found the scammers were chatting to the cryptocurrency seller, telling him to hurry up with the exchange, as if they were her. But I don't think that necessarily points to him being involved, and I think it's less likely they would have been communicating through the official O channels if he was. The P2P seller also seemed willing to help once Ms B realised the cryptocurrency wasn't in the wallet, and offered to show her where he sent the cryptocurrency. So I don't think recovery would have been possible anyway, even if funds remained, as I think the individual would have likely been able to show his bank that the cryptocurrency Ms B paid for was provided.

Ms B has expressed frustration with Revolut's contact options. She said she found it difficult to locate the chat function, and the multiple different agents picking up the conversation made things slow and cumbersome. I can totally see why being able to speak to Revolut over the phone would have been easier for Ms B, particularly if she's less tech-savvy. But I've reviewed the communication here, and find it was fine in the circumstances. Revolut managed to get all the information it needed in order to assess the fraud claim in as timely a manner as it could, and there weren't long gaps in the agents coming back to Ms B. It also gave her an answer to the dispute within a reasonable timeframe, and recovery wasn't possible in this case anyway. So I don't think any of the communication concerns Ms B has raised had a discernible impact that would warrant compensation.

Having considered everything, and whilst I recognise the horrible situation Ms B found herself in, having lost this money to scammers, I don't think Revolut ought reasonably to have done more to prevent what happened. So I'm not directing it to refund the stolen funds.

My final decision

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

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms B to accept or reject my decision before 27 August 2025.

Ryan Miles
Ombudsman