DRN-4532284

The complaint

Mrs B complains that Revolut Ltd won't refund money she lost when she fell victim to an investment scam.

Mrs B is being represented by a claims management company in her complaint.

What happened

The detailed background to this complaint is well known to both parties and has been previously set out by the investigator in their assessment. So, I won't repeat it again here, Instead, I'll focus on giving my reasons for my decision.

The complaint concerns several transactions totalling over £50,000 which Mrs B made from her Revolut account in March and April 2023. She's explained they were made in connection with two investment opportunities, both of which turned out to be a scam.

The Revolut account was opened as part of the scam and Mrs B followed the scammer's instructions in transferring money into her Revolut account, before sending it to cryptocurrency exchanges for conversion into cryptocurrency. Once converted, the cryptocurrency was sent on to cryptocurrency wallets as instructed by the scammer. On one occasion, Mrs B exchanged fiat money into cryptocurrency via Revolut before sending it on.

I'm aware that Mrs B sent scam-related payments from at least two other payment service providers. This decision solely relates to payments made from Mrs B's Revolut account and her complaint about its acts and omissions. Her complaint about the other payment service providers has been considered under separate cases by our service, but where relevant, I've taken into consideration evidence held on those cases.

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 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.

There's no dispute that Mrs B made the transactions using her security credentials, and so they are authorised. But, in accordance with the law, regulations and good industry practice, a payment service provider including an EMI should be on the look-out for and protect its customers against the risk of fraud and scams so far as is reasonably possible. If it fails to act on information which ought reasonably to alert it to potential fraud or financial crime, it might be fair and reasonable to hold it liable for losses incurred by its customer as a result.

EMIs are set up with the purpose of sending and receiving money and the type of payments they're generally used for tends to be somewhat different to banks and building societies.

Often, the payments will be for larger sums. Where there's no previous account history, as was the case here, what should reasonably strike Revolut as concerning for a first payment isn't down solely to the transaction amount involved.

The investigator didn't think our service could consider the cryptocurrency withdrawal Mrs B made directly from Revolut on 23 March – they said the cryptocurrency services were provided separately from the provision of Mrs B's main e-money account and they didn't think the provision of cryptocurrency services is sufficiently closely linked such that it should be deemed ancillary to it. But considering the circumstances of this case, I'm not sure I agree with what the investigator has said. The complaint isn't just about the final step in the payment journey of transferring cryptocurrency to an external wallet, but rather also the prior steps of the scam. These include the acceptance of funds into Mrs B's Revolut account and then a request for Revolut to exchange fiat money into cryptocurrency.

Those steps amount to payment services, or at the very least an activity which is ancillary to payment services – in much the same way that banks or payment service providers exchanging GBP into a foreign currency is an ancillary activity (as foreign exchange isn't covered in its own right).

But even if that single cryptocurrency withdrawal transaction is considered, and that would make it the first disputed transaction from the account, I haven't seen any factors at play here such that, in my view, Revolut should have been concerned and ought to have taken additional steps when Mrs B authorised it. The amount withdrawn was 0.084 BTC, which at the time would have been equivalent to around £1,800. Amount aside, the transaction wouldn't have appeared unusual to Revolut given it had been advised that the account had been opened for making cryptocurrency transactions.

I understand that the next transaction, an electronic transfer of £500, flagged on Revolut's system and it asked Mrs B to select the purpose of the payment from a list of options and displayed a warning based on the purpose selected. Mrs B selected 'safe account', and after displaying a warning covering the typical hallmarks of safe account scams, Revolut presented her with the option to (1) read its scam guidance, (2) get advice from one of its agents, (3) cancel the payment, or (4) go ahead with it. Mrs B decided to go ahead with the payment.

I don't think 'safe account' could ever be a legitimate reason for sending money to another account. While Revolut displayed warnings which covered the most common features of such scams, I think it ought to have contacted Mrs B to discuss the payment further, even if it meant directing her to an in-app chat. But I don't think that would have made a difference here.

I say this because five days later Revolut did direct Mrs B to the in-app chat after she selected 'safe account' once again for a much larger transaction of £10,000. Her answers during the payment flow and the subsequent chat correspondence indicate that she'd likely made a mistake in choosing the payment purpose. For instance, Mrs B confirmed she'd not been contacted by someone telling her she'd been a victim of fraud and then rushed into making the payment.

Given that both transactions had triggered on Revolut's systems prior to it being told the 'safe account' payment purpose, I would have expected it to continue with its enquiries on discovering that Mrs B likely selected that payment purpose in error. But I'm not persuaded that Mrs B would have been forthcoming about the true purpose of the transactions. As the investigator highlighted, she didn't respond to Revolut's questions truthfully. For instance, she was asked if she'd been asked to install remote access software on her computer or phone – Mrs B said no. Mrs B also told Revolut that no one else had been involved in the

transaction. None of these facts were true. We know the scammer had instructed her to grant remote access.

There's also contemporaneous evidence of Mrs B misleading two other payment service providers on multiple occasions over the phone when questioned about transactions linked to the same scam which were made from accounts held with them. Call recordings have been shared with Mrs B's representative. I understand questions have been raised about the quality of those interventions. I don't think it's appropriate to address those concerns in this complaint which is about Revolut's actions. What I would say is that the important detail to mention here is that there's evidence of willingness to mislead. Despite what her representative states, the evidence strongly suggests that Mrs B was being coached by the scammer at the time.

Had Revolut continued making enquiries when it intervened through the in-app chat, on balance, I'm not convinced that Mrs B would have responded honestly like her representatives have suggested. Even if Revolut had managed to establish that Mrs B's payments were investment related, based on how she responded to interventions by other payment service providers – it was explained to her that scammers often spend days and weeks building trust and tell victims to move money to different accounts to potentially invest in cryptocurrency – I'm not persuaded that she would have heeded its warnings. The limited chat correspondence between Mrs B and the scammer that I've seen shows that trust had been gained.

For completeness, I don't consider any of the disputed transactions in fiat money were identifiably cryptocurrency related. I've checked and the beneficiary account providers offer accounts to cryptocurrency and non-cryptocurrency firms. So, under the circumstances, I'm not convinced that better intervention by Revolut along the lines I've described above would have positively impacted Mrs B's decision-making. And much for the same reasons, I don't think further intervention at a later point would have made a difference either – although it's arguable whether the later transactions would have appeared unusual, given the earlier ones would have established a pattern of regular spending.

I've also thought about whether Revolut could have done more to recover the funds once it became aware of the situation, as in some circumstances the money can be recovered. Given Mrs B had legitimately bought cryptocurrency before sending it on to wallets in control of the scammer, it's unlikely recovery from the cryptocurrency exchange would have been successful.

What this means is that in the circumstances of this case, I don't consider Revolut acted unfairly in executing the payment instructions it received from Mrs B. It follows that I don't find it liable for her financial loss.

In summary, I know that Mrs B will be disappointed with this outcome. Not least because the matter has been ongoing for some time. I fully acknowledge that there's a considerable amount of money involved here. Despite my natural sympathy for the situation in which Mrs B finds herself, for the reasons given, it wouldn't be fair of me to hold Revolut responsible for her loss.

My final decision

For the reasons given, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs B to accept or reject my decision before 21 August 2024.

Gagandeep Singh
Ombudsman