DRN-4838270

The complaint

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

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 just over £39,000 which Ms L made from her Revolut account in April-May 2022. These were debit card and faster payments which were made in connection with an investment opportunity.

Miss L's Revolut account was opened as part of the scam. She transferred funds into her Revolut account from her account with a high street bank "N". To deposit the funds on to the investment platform, Miss L sent money to a cryptocurrency exchange for conversion into cryptocurrency. Once converted, the cryptocurrency was sent on to cryptocurrency wallets as instructed by the scammer (albeit at the time Miss L thought she was loading it on to her account with the investment platform).

When she was unable to make withdrawals and repeatedly instructed to top up the account with more money, Miss L realised she'd fallen victim to a scam.

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.

But, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to be good industry practice at the time, I consider it fair and reasonable in April 2022 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 including in relation to card payments),

- 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.

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. Miss L authorised the first disputed transaction, a card payment of £500 to a cryptocurrency exchange, on 13 April. I note that in late 2023, the UK financial services regulator published a warning about that cryptocurrency exchange which said that it was operating in the UK without its permission. But no such warning existed at the time of Miss L's transactions. So, I wouldn't have expected Revolut to have flagged the payment based on the merchant's name alone. And I haven't seen any other factors at play here such that, in my view, Revolut should have been concerned and ought to have questioned Miss L.

Revolut has said that the following day it blocked Miss L's account and declined two card transactions, also to the same cryptocurrency exchange, for £1,250. It says it did this because the transactions flagged on its fraud detection systems as possibly unauthorised. The restrictions on her account were removed when Miss L confirmed that it was indeed her who had authorised the payments. Given the risk identified – namely that the transactions may not have been made by the genuine customer – I consider the EMI took proportionate checks to satisfy itself that all was above board.

The next transaction Miss L authorised – a card payment of £2,700 to the cryptocurrency exchange – was over ten days later. Given that she'd previously successfully made a payment to the merchant and not raised any concerns in that period, and subsequently confirmed further attempts to pay were genuine, I don't consider the transaction in question ought to have appeared as unusual or suspicious.

But by the time Miss L authorised the next transaction, a faster payment of £9,000 to the cryptocurrency exchange's account provider, Revolut ought to have recognised that it carried a heightened risk of financial harm from fraud. This is because a pattern of increased activity on cryptocurrency spending had emerged. And there was a significant jump in the amount involved. I consider Revolut should have taken additional steps when it received Miss L's instruction.

The investigator's view was that Revolut should have contacted Miss L and questioned her. I think it's arguable that a proportionate response at that point would have been for Revolut to have provided a written warning specific to the fraud risk identified, namely cryptocurrency scam. In that instance, I would have expected Revolut to have provided a written warning about cryptocurrency investment scams, tackling some of the key features. But regardless of the type of intervention – providing a tailored written warning or making direct contact like the investigator has suggested – I'm not persuaded that any proportionate intervention by Revolut would have prevented Miss L's loss. I'll explain why.

On 12 April – two weeks prior to the £9,000 transaction – Miss L had attempted to send money to the same beneficiary from her account with N, but it was flagged for fraud checks. Miss L was asked to phone the bank to discuss the transaction. I've listened to a recording of the relevant call. When she told the agent that the transaction was in relation to bitcoins,

Miss L was asked if she had done her research into the company she was dealing with. The agent asked if the had checked whether it was approved by the Financial Conduct Authority and protected under the Financial Services Compensation Scheme. As Miss L said she hadn't carried out those checks, it was mutually agreed that the transaction would be paused until she was satisfied, she wanted to go ahead.

The following day, Miss L told N that she wanted the transaction paid. When questioned about it further, it came to light that Miss L had been asked to and had agreed to download a remote access software recently. She explained the request had come from someone she had approached regarding bitcoins. And that they were demonstrating how it all worked. The agent became concerned by Miss L's response and explained that there was no reason for a cryptocurrency provider to access her. They told her that by granting access, the third party could potentially see what Miss L was doing. The agent repeatedly told Miss L that they were quite concerned that someone had access to her device, and she had subsequently made a transaction.

The transaction was declined, and Miss L was warned that this could be a scam and she was possibly falling victim to it. She was encouraged to get her device 'cleaned' and uninstall the remote access software. And to do some research on the company she was dealing with to ensure they were legitimate. Specifically, the agent suggested that Miss L should research cryptocurrency and trading scams.

I've seen the chat correspondence between Miss L and the scammer. I note that she was in constant communication with them when N blocked the transactions. Instead of independently researching whether the scammer's company was regulated, Miss L asked the scammer that question. The following day, when N declined the transaction, Miss L informed the scammer that the bank had told her it was scam. There's an indication in the chat correspondence that Miss L spoke to the scammer over the phone. I don't know what was discussed during that call, but what I can see is that later that day Miss L decided to transfer her money from N to Revolut.

I can't say for certain how Miss L would have responded to Revolut's warning a couple of weeks later. In such circumstances, I need to make my decision on the balance of probabilities. In other words, what I consider to be more likely than not Miss L's response based on the information that is available. What I have is contemporaneous evidence of Miss L ignoring her bank's warnings about the same beneficiary and seeking reassurances from the scammer instead of carrying out independent due diligence after she'd been warned about the common tactics used by scammers.

Given her actions, I'm not persuaded that a specific written warning about cryptocurrency scams by Revolut would have made any difference to her decision-making. Even if I were to make a finding that Revolut ought to have made enquiries – either during the payment flow or through its in-app chat – at the time of the £9,000 transaction, or during the subsequent transactions, I'm not convinced that Miss L would have heeded its warnings.

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. For the debit card payments, the recovery avenue would have been limited to chargeback. But Miss L's payments went to a cryptocurrency exchange. She wouldn't be able to make a successful chargeback claim in the circumstances because the merchant she paid did provide the service requested (i.e., conversion of fiat money into cryptocurrency). For completeness, Revolut couldn't attempt a chargeback against any another party. For the faster payments, I can see Revolut contacted the beneficiary account provider and requested a recall of funds. But it didn't hear back.

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 Miss L. It follows that I don't find it liable for her financial loss.

In summary, I know that Miss L 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 Miss L 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 Miss L to accept or reject my decision before 6 August 2024.

Gagandeep Singh
Ombudsman