DRN-4783572

The complaint

Ms H complains that Revolut Ltd won't refund money she lost to an investment scam.

Ms H is being represented by solicitors in her complaint.

What happened

The detailed background to this complaint is well known to both parties, so I won't repeat it again here. Instead, I'll focus on giving my reasons for my decision.

The complaint concerns ten transactions totalling approximately £20,000 which Ms H made from her Revolut account – mixture of card payments and transfers – in June and July 2023. These were made in connection with an investment opportunity with a firm "B" which Ms H came across on the internet. She subsequently discovered she had been scammed.

Ms H has explained that the scammer instructed her to open the Revolut account as part of the scam. To deposit money into her investment account, Ms H first transferred funds into her Revolut account from her account with a high street bank. This money was then used to purchase cryptocurrency – either directly from a cryptocurrency exchange or through peer-to-peer purchase. Once converted, the cryptocurrency was sent on to cryptocurrency wallets in the control of the scammer (although at the time Ms H believed it was being deposited into her investment account).

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 that in June 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 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.

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.

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 Ms H when she authorised the first four disputed transactions, all card payments which ranged between £800 and £1,200, on 19 and 21 June. I acknowledge that Ms H was sending money to a cryptocurrency exchange. But that in and of itself doesn't mean that the transactions ought to have flagged as suspicious. Buying cryptocurrency is a legitimate exercise.

But by the time Ms H authorised the fifth transaction – a card payment of £1,250 on 21 June – 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. This was the third such transaction in one day, all authorised a minute apart. I consider Revolut should have taken additional steps when it received Ms H's instruction.

I think that a proportionate response to that risk would have been for Revolut to have provided a written warning specific to the scam risk identified. In this instance, the transaction was identifiably cryptocurrency related. So, I would have expected Revolut to have provided a written warning about cryptocurrency investment scams, tackling some of the key features. But, had it done so, I'm not persuaded that Ms H would have stopped in her tracks.

This is because her submissions indicate that she was simply following the instructions of the scammer – she remembers them getting her to approve transactions but doesn't recall anything else. Based on her response, I'm not convinced that she would have taken time to review Revolut's warning about the typical features of investment scams involving cryptocurrency. I think its more likely that she would have instructed Revolut to make the payment when given a choice to continue or cancel the transaction following the provision of the warning.

In making that finding, I'm mindful that during subsequent transactions, when prompted to select the payment purpose, Ms H appears to have selected the first option on the list provided – safe account – on each occasion. I know she submits that she doesn't recall doing that, but from what we know about Revolut's app and restrictions or limitations around remote access it would needed to have come from her. It isn't clear why Ms H selected the reason that she did. But it seems likely to me to be the actions of someone who was either following the instructions of a third party, or simply clicking the first available option to move on to the next screen.

Revolut has said that the next card transaction to the same cryptocurrency exchange was flagged as suspicious and it declined it. Looking at the account activity, a transfer to a third party was attempted following the declined transaction. I don't know for certain, but it looks

like Ms H had authorised a transfer to facilitate the purchase of cryptocurrency from a peer-to-peer seller. But this transaction flagged on Revolut's fraud detection systems and, in addition to telling her that it could potentially be scam related, it asked Ms H to provide a payment purpose. This is when 'safe account' was selected.

Revolut ought to have been concerned when 'safe account' was selected, given it is never a legitimate reason for sending money to another account. I can see that on that occasion, it did direct Ms H to the in-app chat and asked her to provide a selfie to complete verification. Unfortunately, despite several attempts, Ms H didn't comply with Revolut's requirements. And the transaction in question didn't go through.

The next time a transfer was attempted, and 'safe account' was selected, Revolut simply provided a written warning covering the common features of safe account scams. I don't consider displaying a scam warning on the screen and giving Ms H 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, was a proportionate response to the risk identified given what I've said about customers selecting 'safe account' as the payment purpose. Revolut ought to have contacted Ms H to discuss the payment further, even if it meant directing her to an in-app chat again to satisfy itself that she hadn't fallen victim to a safe account scam. So, I consider it missed an opportunity.

But that's not the end of the matter. Causation is a critical determinative factor in every scam case. It isn't enough that a payment service provider like Revolut missed an opportunity to intervene; its acts or omissions must be the immediate and effective cause of losses that were reasonably foreseeable at the time of the breach. I can't know for certain what would have happened if Revolut had questioned Ms H further about the payment purpose selected. In such situations, I reach my conclusions not based on mere possibilities but rather on what I find most probable to have happened in the circumstances. In other words, I make my decision based on the balance of probabilities – so what I consider most likely to have happened considering the evidence and wider circumstances of the case.

Had there been a direct intervention and questions asked about the payment purpose selected, on balance, I think it's more likely than not that Revolut would have been advised Ms H had made a mistake and selected the safe account option in error. This is not a finding I've made lightly. A transfer from Ms H's account with the high street bank into her Revolut account was flagged for fraud checks a few weeks later. Ms H was required to phone the bank to discuss the transaction. I've listened to a recording of the relevant call. Ms H didn't answer the agents' questions truthfully. Before she was even asked what the payment was for, Ms H volunteered a response and said she wanted to transfer funds to Revolut to pay for a family holiday. When questioned further, she also confirmed that: she'd had the Revolut account for around a year; no one had asked her to open it; and no one had instructed her to make the payment.

So, what I have is evidence of Ms H misleading another business when questioned over the phone. I acknowledge that the questions and warnings weren't specific to cryptocurrency investment scams. But Ms H's answers suggest she was willing to mislead her bank. As I've mentioned before, based on her answers it seems likely that Ms H was being coached on how to answer questions from her bank. Therefore, I'm not convinced that she would have responded honestly like her representatives have suggested had Revolut made further enquiries along the lines I've described above – either at that time or during subsequent interventions.

I've considered that the 'cover story' provided to the high street bank might not have worked with Revolut. But I think the important detail to mention here is that it's not the specifics of the dishonesty itself, but the willingness. I accept it's possible that Ms H's answers to the

bank's questions are unlikely to have worked with Revolut. But it's equally possible that Ms H could have provided a different cover story. Having given this a lot of thought, and based on my findings above, I'm not persuaded that the true purpose of the payment would have come to light.

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 Ms H.

Recovery wise, these transactions were made to legitimately purchase cryptocurrency. Given the purchased cryptocurrency was then moved on to the scammer's wallets, recovery would likely have failed. For completeness, Revolut couldn't have attempted recovery from the third-party wallet owner (i.e., the scammer). It could have only contacted the seller of the cryptocurrency, i.e., the cryptocurrency exchange or the peer-to-peer seller.

In summary, I know that Ms H 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 she 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 Ms H to accept or reject my decision before 5 September 2024.

Gagandeep Singh
Ombudsman