DRN-5124984

The complaint

Mrs A complains that Revolut Ltd didn't do enough to protect her from the financial harm caused by an investment scam, or to help her recover the money once she'd reported the scam to it.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

In July 2023, Mrs A saw posts on social media from friends claiming they'd made good returns from cryptocurrency investments through someone I'll refer to as "the scammer". The posts featured screenshots showing the receipt of thousands of pounds into their bank accounts. Mrs A messaged one of the friends and received a response confirming the investment had been a success. Unknown to Mrs A, her friend's social media platforms had been hacked.

She contacted the scammer through a 'tag' on one of the posts and expressed an interest in trading. The scammer's profile seemed genuine, and included a profile picture and other information, and she noted they had the same religious beliefs. The scammer said she was willing to teach her how to invest and that she would earn 10% commission on all her profits.

The scammer told Mrs A to open accounts with Revolut and a trading platform which I'll refer to as "G", which Mrs A noted had positive reviews on the App store. She followed the link to G's website which featured testimonials and a live chat option. She couldn't find much about G online, so she assumed there were no negative results or issues. Finally, she messaged her friend on social media, and the friend confirmed she'd used the same site.

The scammer showed Mrs A how to open an account on the trading platform and between 14 July 2023 and 29 August 2023 she made eleven exchanges to cryptocurrency and twelve cryptocurrency transfers from the Revolut platform to G. But when she decided to make a withdrawal from the trading account, the scammer said she needed to pay fees. She eventually realised she'd been scammed on 10 September 2023 when she saw a post on social media stating the scammed was operating a scam.

Mrs A contacted Revolut but it refused to refund the money she'd lost. It said the cryptocurrency withdrawals were irreversible due to their decentralised nature, and it wasn't liable for any losses which were related to a withdrawal or deposit to or from an external wallet. It said she was given a cryptocurrency withdrawal warning, notifying her that cryptocurrency withdrawals are non-reversible, and she accepted and acknowledged the terms of the withdrawals in the Revolut app. It said she was shown the warning six times (before every transfer that she made to a different cryptocurrency wallet). So, it wasn't at fault for processing the cryptocurrency withdrawals.

Mrs A wasn't satisfied and so she complained to this service with the assistance of a representative. She said she was given pop-up warnings before some of the payments, but the warnings weren't tailored to cryptocurrency scams, and she was simply asked if she was

sure she wanted to make the transactions, which she was because she believed the investment was genuine. Revolut failed to advise her that she could be falling victim to a scam and if she'd understood the risk, she wouldn't have gone through with the payments.

Her representative said Revolut should have intervened because Mrs A made multiple unusually high payments to a new payee in quick succession. They said that even though there was no account history, it should have intervened when she processed the first transaction, and had it done so it would have spotted that the investment had the hallmarks of a scam. It could have then educated her on the scam risk, and she wouldn't have made any further payments.

The representative said the warnings Mrs A received weren't effective and if she'd been asked probing questions, she'd have explained that she was acting under the guidance of a third party and Revolut would have detected the scam and provided an effective warning and encouraged her to carry our further checks.

Revolut further stated that Mrs A created the account on 14 July 2023 declaring 'crypto' as one of the account purposes. It said a warning was displayed each time a cryptocurrency withdrawal was performed to a new external address. The warnings questioned the legitimacy of the beneficiary and explained the dangers of such transactions and the fact that it is non-reversible. It said cryptocurrency withdrawals are an unregulated product and it doesn't consider this service has jurisdiction to investigate any activity relating to Mrs A's cryptocurrency account.

Our investigator explained that the transactions which make up the ultimate loss are transfers of cryptocurrency, which isn't a regulated activity. However, he said the complaint is not solely about the sending of cryptocurrency to an external wallet and the steps leading up to the transfer of cryptocurrency includes both the acceptance of funds into the account and the subsequent request for Revolut to exchange fiat money into cryptocurrency. He explained that these earlier steps amount to payment services, and in the case of the exchanges, at the very least an activity which is ancillary to payment services and therefore our service does have jurisdiction to hear the merits of parts of the complaint.

Our investigator thought Revolut ought to have had concerns by the time Mrs A made the fourth cryptocurrency exchange because by that time £5,000 had either been exchanged or was being requested to be exchanged in under 48 hours. He noted that Mrs A wasn't given a warning before any of the exchanges and that he thought it should have presented a tailored written warning about cryptocurrency investment scams.

However, he didn't think this would have prevented her loss because Mrs A's messages with the scammer show he coached her when she was asked to provide an account purpose. He was satisfied this showed she would have misled Revolut if she was asked about the purpose of the exchanges. And that a written warning wouldn't have been enough to undo the influence that the scammer had over her.

Mrs A has asked for her complaint to be reviewed by an Ombudsman. Her representative has argued that Revolut shouldn't have allowed activity on a new account where twenty account opening options were chosen, including "Kids Account". They've argued that it should have frozen the account when Mrs A completed the questionnaire and that this would have prevented her loss.

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've reached the same conclusion as our investigator. And for largely the same reasons. I'm sorry to hear that Mrs A has been the victim of a cruel scam. I know she feels strongly about this complaint, and this will come as a disappointment to her, so I'll explain why.

I've explained why we can't consider the cryptocurrency withdrawals in a separate decision.

There's no dispute that this was a scam, but although Mrs A didn't intend her money to go to scammers, she did authorise the disputed payments. Revolut is expected to process payments and withdrawals that a customer authorises it to make, but where the customer has been the victim of a scam, it may sometimes be fair and reasonable for the bank to reimburse them even though they authorised the payment.

Prevention

Revolut was an emoney/money remittance provider and at the time these events took place it wasn't subject to all of the same rules, regulations and best practice that applied to banks and building societies. But it was subject to the FCA's Principles for Businesses and BCOBS 2 and owed a duty of care to protect its customers against the risk of fraud and scams so far as reasonably possible.

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 September 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;

- have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;

- 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.

Mrs A's representative has argued that Revolut ought to have frozen the account at the point she chose multiple account purposes. I do accept the fact she selected multiple options means Revolut couldn't have argued that the cryptocurrency transactions were in line with the account opening purpose, but I don't think freezing the account at the outset would have been a proportionate response, as this alone wouldn't indicate that she was at risk of fraud.

Mrs A wasn't shown any warnings before she exchanged her funds for cryptocurrency. This was a newly opened account and so there was no account history to compare the transactions with. But this service takes the view that an account holder using Revolut's services to purchase cryptocurrency could just as likely be doing so as a result of a scam as if they were sending external payments to a cryptocurrency provider.

As the first three transactions were low value exchanges to cryptocurrency, I agree with our investigator that Revolut didn't need to intervene. However, by the time Mrs A made the fourth exchange, she'd exchanged a total of £3,000 to cryptocurrency in one day, and the cumulative total for the three days since she opened the account was £5,000, so I think Revolut ought to have intervened.

In the circumstances, I think a proportionate response would have been to provide a tailored written warning which was relevant to cryptocurrency investment scams. However, I've thought carefully about whether a specific warning covering off the key features of cryptocurrency investment scams would have likely prevented any further loss in this case, and, on the balance of probabilities, I don't think it would have.

I would expect a written warning to have covered off some of the key features of cryptocurrency-related investment scams, including the fact victims are usually targeted via social media or email, they will often involve a third party or broker, and fake online trading platforms can appear professional and legitimate.

While Mrs A did find the opportunity online, she reached out to the scammer having seen posts on her friend's social media platforms, which would make it seem more legitimate than if she was cold called, so the warning might not have resonated with her. Further, Mrs A has explained that she believed the investment was genuine because she thought her friends had made profits from their investments, she'd seen testimonials on the website and there were no negative reviews online. Further, the evidence of Mrs A's communications with the scammer shows that she sought and followed his guidance when she opened the Revolut account, including his instructions to select all the account purpose options. This tells me that if she'd been concerned, she would most likely have sought the scammer's advice following a warning from Revolut, rather than seeking advice from an independent source.

Significantly, Mrs A was presented with warnings questioning the legitimacy of the beneficiary each time she transferred cryptocurrency from the Revolut platform to a new external address. While I would expect Revolut to have provided a more effective warning when she made the fourth exchange, the fact she went ahead with the transfers having been presented with relevant warnings is evidence of her determination to make the transactions and her trust in the scammer.

So, I think it's unlikely that a written warning about cryptocurrency investment scams would have stopped her from making the transactions. Therefore, while I think Revolut missed an opportunity to intervene, I don't think this represented a missed opportunity to have prevented Mrs A's loss.

Recovery

I don't think there was a realistic prospect of a successful recovery because Mrs A paid an account in her own name and moved the funds onwards from there.

Compensation

The main cause for the upset was the scammer who persuaded Mrs A to part with her funds. I haven't found any errors or delays to Revolut's investigation, so I don't think she is entitled to any compensation.

I'm sorry to hear Mrs A has lost money and the effect this has had on her. But for the reasons I've explained, I don't think Revolut is to blame for this and so I can't fairly tell it to do anything further to resolve this complaint.

My final decision

For the reasons I've outlined above, 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 A to accept or reject my decision before 6 January 2025.

Carolyn Bonnell
Ombudsman