DRN-5094428

The complaint

Mrs D complains that Revolut Ltd didn't do enough to protect her from the financial harm caused by an advance fee 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.

Mrs D responded to advert on Google and was contacted by someone I'll refer to as "the scammer" who claimed to be a recruiter. The scammer told her about an opportunity to work from home on a platform I'll refer to as "D". He explained the role would require her to increase the sales of products online in return for a commission on each task.

The scammer explained that she would have to pay for tasks using cryptocurrency and told her to open accounts with Revolut and a cryptocurrency exchange company, instructing her to first purchase cryptocurrency and then load it onto an online wallet Before she went ahead, she did some background checks and didn't see anything concerning.

Mrs D transferred funds to the Revolut from Bank S and between 23 December 2023 and 25 December 2023, she made six card payments to the cryptocurrency exchange totalling £4,258. She could see her commission growing as she completed the tasks, but she realised she'd been scammed when she completed her allocation and was asked to make payment to bring the account back to a positive balance.

She contacted Revolut but it refused to refund any of the money Mrs D had lost. It said the chargeback claims were rejected because Mrs D had paid a genuine merchant and the service was provided.

It said it stopped two attempted payments on 24 December 2023 and engaged Mrs D in a live chat where it warned her that the transactions seemed riskier than usual and that there was a high chance that she was being scammed. She was asked if she was being guided or pressured into making the payments, which she denied, and whether she'd opened and had access to the cryptocurrency account.

Revolut said Mrs D was warned that scammers use sophisticated tactics to deceive their victims, and that if she was suspicious, she shouldn't make the payments. It said it questioned her regarding the payments and gave warnings about the risks the risks, which she acknowledged before proceeding with the payments.

Mrs D wasn't satisfied and so she complained to this service with the assistance of a representative. She said Revolut failed to provide adequate warnings or intervene effectively, and had it done so her loss would have been prevented. Her representative explained that Mrs D wasn't coached to lie, but the scammer told her the intervention was normal because Revolut would want to keep her money.

Our investigator didn't think the complaint should be upheld. She noted that Revolut intervened on 24 December 2023 when Mrs D attempted to pay £480 to the cryptocurrency exchange. She was warned that if she was being scammed, the fraudster may ask her to hide the real reason for the payment. She was also asked if she was being guided – to which she responded negatively - before being warned: *'if someone is telling you to ignore these warnings, they're a scammer. Only continue if you're sure that you are not being prompted into making a payment'.* Mrs D confirmed she'd read the warning and was then asked to provide a payment purpose.

She further explained that Mrs D said she was making the payment 'as part of an investment' and was asked questions relevant to that purpose. She was then shown a series of educational stories to warn her about the risks, including warnings about being wary of scams and social media promotions, giving people remote access, conducting research, and to not be rushed into making payments.

She was then required to engage in a conversation with a live agent when she was warned about scammers using fake investment websites and platforms and asked whether she had access to the cryptocurrency account, how she decided which platform to use and where she learnt about it, how long she'd been investing, and whether she'd installed any remote access software. She also warned: 'Make sure any research you do is your own – fraudsters create convincing-looking posts on social media share articles about investing. If someone says you need to send money as a tax or fee to access your funds, you are being scammed'.

Our investigator commented that a more accurate response to the question about the payment purpose would have been to 'complete a task on a job hiring process' and that the WhatsApp messages between Mrs D and the scammer showed she was being guided. She said that Revolut was only able to act on the information available to it and if Mrs D had been honest about the payment purpose, Revolut could have asked more relevant questions.

She also explained that even if she felt Revolut should have intervened in any of the later payments, she didn't think it would have made a difference because Mrs D would have given misleading responses, and it wouldn't have been able to detect the scam or provide effective warnings. Overall, she was satisfied that Revolut's warning was proportionate, and she didn't think it was at fault for processing the payments.

Finally, she explained that Mrs D would have received a service from the cryptocurrency exchange, so there wasn't a reasonable prospect of a successful chargeback. And she didn't think Mrs D was entitled to any compensation.

Mrs D has asked for her complaint to be reviewed by an Ombudsman. Her representative has explained that she was under pressure to complete the transactions urgently and didn't select 'complete a task on a job hiring process' because she'd already been 'hired'. They don't accept she'd have done the same thing if Revolut had intervened again and have argued that the educational stories were irrelevant, and strong effective warnings about potential scams could have stopped the scam by providing the necessary information to recognise the fraudulent nature of the transactions.

They've also argued that Mrs D wasn't being guided on how to circumvent the block, she simply told the scammer the payment had been blocked.

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 D 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'm satisfied Mrs D 'authorised' the payments for the purposes of the of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although she didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of her bank account, Mrs D is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mrs D 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

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 have been good industry practice at the time, I consider it fair and reasonable in December 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;

• 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.

I've thought about whether Revolut could have done more to prevent the scam from occurring altogether. Buying cryptocurrency is a legitimate activity and from the evidence I've seen, the payments were made to a genuine cryptocurrency exchange company. However, Revolut ought to fairly and reasonably be alert to fraud and scams and these payments were part of a wider scam, so I need to consider whether it did enough when Mrs D tried to make the payments.

It wouldn't have needed to intervene when Mrs D made the first payment on 23 December 2023 because even though she was paying a high-risk cryptocurrency exchange, the payment was very low value and so it wouldn't have needed to intervene.

The next two payment attempts (£480 to the same cryptocurrency exchange) on 24 December 2023) were blocked and as described above, Mrs D was asked to provide a payment purpose and provided warnings based on the stated purpose. Unfortunately, she didn't select the most appropriate option, and this meant that she was shown warnings which weren't relevant to her circumstances and therefore didn't resonate with her.

She was also asked questions which I'm satisfied were sufficiently probing, but her responses suggested she was investing in cryptocurrency rather than using it to pay for tasks which she expected to be paid a commission for completing, and that she was confident and researched the investment herself. So I don't think it's unreasonable that Revolut didn't detect the scam.

I've considered whether the intervention was proportionate to the risk presented by the payments, and I'm satisfied that it was. Unfortunately, Mrs D's responses prevented Revolut from detecting the scam or from giving relevant warnings, and in the circumstances, I don't think there was anything else it could reasonably have done to prevent her loss.

I've also considered whether Revolut ought to have intervened again, and I think it's debateable whether it needed to. In any event, based on the outcome of the interventions that did occur, I have no reason to think that Mrs D wouldn't have responded in the same way and so I don't think the outcome would have been any different, especially as there's evidence that she was in contact with the scammer. Mrs D's representative has argued that its not fair to assume that she'd have done the same thing if it had responded again, but I consider her behaviour when it did intervene is evidence of how she would have responded if it had done so again, and I agree with our investigator that a further intervention is unlikely to have prevented her loss.

Recovery

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

Chargeback

I've thought about whether Revolut could have done more to recover the payments when Mrs D reported the scam to it. Chargeback is a voluntary scheme run by Visa whereby it will ultimately arbitrate on a dispute between the merchant and customer if it cannot be resolved between them after two 'presentments'. Such arbitration is subject to the rules of the scheme — so there are limited grounds on which a chargeback can succeed. Our role in such cases is not to second-guess Visa's arbitration decision or scheme rules, but to determine whether the regulated card issuer (i.e. Revolut) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder (Mrs D).

Mrs D's own testimony supports that she used a cryptocurrency exchange to facilitate the payments. Its only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchange would have been able to evidence they'd done what was asked of them. That is, in exchange for Mrs D's payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I'm satisfied that Revolut's decision not to raise a chargeback request against either of the cryptocurrency exchange companies was fair.

Compensation

The main cause for the upset was the scammer who persuaded Mrs D 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.

Overall, I'm satisfied Revolut took the correct steps prior to the funds being released – as well as the steps it took after being notified of the potential fraud. I'm sorry to hear Mrs D 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 D to accept or reject my decision before 24 July 2025.

Carolyn Bonnell
Ombudsman