DRN-5037988

The complaint

Mrs F complains that Revolut Ltd won't reimburse her after she fell victim to a scam.

What happened

Mrs F has explained that she received a phone call from an individual purporting to work for a known cryptocurrency platform. The individual told Mrs F that funds had been traded on an account in her name and she therefore was entitled to withdraw these funds – however, she had to first make payments in order to release the funds. Unfortunately, unbeknownst to Mrs F at the time, the individual she was speaking to was in fact a fraudster.

Mrs F said she did initially question elements of the scam – the fraudster called on a number of different mobile numbers, which he said was due to being part of a large company and having a number of different lines. When Mrs F asked how she can be sure the caller was genuine, he emailed her a falsified employee identification card, as well as a letter with the company header, advising Mrs F of the funds in her name.

Mrs F initially made payments towards the scam from a cryptocurrency platform she'd set up some years earlier, but when this platform stopped further funds being sent, she opened a Revolut account on the advice of the fraudster. Mrs F was initially told she needed to pay £1,000 in order to release her funds held on the cryptocurrency platform, but demands from the fraudster kept increasing which he said were due to 'market trends'. In total, Mrs F made the following transactions from her Revolut account:

Date	Payment type	Value
20/06/2023	Bitcoin withdrawal	0.09 Bitcoin + fees (approx. £2,000)
21/06/2023	Push to card payment	€4,201 + fees
21/06/2023	Push to card payment	€1,418 + fees
21/06/2023	Push to card payment	€1,097 + fees

Revolut has said that during the payment process, it provided several warnings to Mrs F. For the cryptocurrency payment, it requested that Mrs F confirm in-app that the payment was being made to a wallet in her name and advised that transfers are irreversible. Then there were several steps Mrs F had to take for the subsequent payments in Euros:

- Mrs F was warned about not making payments to people she didn't know and trust.
- Mrs F was asked the payment purpose, and chose the option *'something else'.*
- In-app messaging advised Mrs F that there was a 'high probability' that the payment was a scam and provided Mrs F with some further advice, largely focused on protecting her from impersonation and safe account scams.
- Lastly, before confirming the payment, Revolut presented Mrs F with another screen that advised '*You're at risk of losing money. This payment is suspicious, only proceed if you're sure it isn't a scam'.*

Mrs F has explained that she gave the fraudster remote access to her computer, having downloaded software on his request, so while she authorised the payments in question, she was guided through the payment process and some parts were completed by the fraudster.

After making the payments and while expecting a later call back, Mrs F began questioning what she had been told and became suspicious. She contacted her banking providers involved and realised she'd fallen victim to a scam. Mrs F logged a scam claim with Revolut.

Revolut considered Mrs F's claim but didn't uphold it. For around a week Revolut advised Mrs F it couldn't consider her claim without a copy of a Police report, despite Mrs F clarifying she had raised the scam with Action Fraud and that the Police (both by phone and in person) had referred her back to Action Fraud a number of times. Mrs F even travelled to a police station in an attempt to progress her claim, despite being in recovery from a broken hip, but was told there was nothing further the Police could do for her. Revolut then agreed to consider Mrs F's claim but didn't uphold it. It said it had sufficient protection in place to warn Mrs F about the payments she was making and was unable to recover her funds.

Mrs F remained unhappy and referred her complaint to our service. An investigator considered the complaint but didn't uphold it. He thought that by the second payment Mrs F had made, Revolut ought to have had concerns that she was at risk of financial harm from fraud, based on there having been a cryptocurrency withdrawal already made, then a notable sized payment to an international account. However, he thought that as the fraudster was largely controlling Mrs F's screens when making the payments, Mrs F wouldn't have been sufficiently impacted by any warnings it provided to stop further payments. He did however award £150 compensation for the difficulty Mrs F had in logging her claim with Revolut at an already stressful time.

Mrs F disagreed with the investigator's view. She thought that as she had only just opened an account, the amount of account activity ought to have appeared as suspicious to Revolut and the account should have been blocked. Revolut agreed to the investigator's compensation suggestion.

As Mrs F disagreed with the investigator's view, the complaint has been referred to me for a final decision.

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 Servcies 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 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.

It isn't in dispute that Mrs F has fallen victim to a cruel scam here, nor that she authorised the disputed payments she made from her account, but I've thought about whether Revolut should have reasonably intervened further, prior to processing the payments.

I've had to take into account that Mrs F opened the Revolut account specifically for the scam payments, and Revolut therefore had no prior transaction history to understand what 'typical' spending looked like for Mrs F. Revolut is also, as mentioned, an EMI, and operates differently to typical banks, with different regulatory frameworks. What is considered 'typical spending' on such accounts can also differ, as its customers can use these for different purposes to a bank account.

When opening her account, Mrs F confirmed the purpose of the account was for '*spending abroad'.* While payments two to four were international transfers, I think it's fair to say this isn't what would be considered typical activity for this account purpose. Therefore I think it's reasonable to say that as Mrs F made a payment towards cryptocurrency, followed by three international payments, there was considerable account activity that didn't match the purpose for which Mrs F said she'd opened the account. I therefore think Revolut ought to have intervened on 21 June 2023 to ensure Mrs F wasn't at risk of financial harm from fraud.

Mrs F considers appropriate intervention would've been for her account to be blocked and for her to be questioned on the payments. Unfortunately, I can't agree with this. Revolut has a difficult balancing act to reach between protecting its customers from financial harm, while also not unduly inconveniencing genuine transactions. While I think Revolut was right to question these payments further (as it did by querying the payment purpose and providing a further written warning on this), taking into account the points I've mentioned above, I wouldn't have expected Revolut to intervene further than this, prior to releasing the payments.

I've therefore gone on to consider whether I think the written warnings Revolut provided went far enough in the circumstances of this complaint. Mrs F has explained that the fraudster was largely controlling her computer and going through the payment process quickly and that she therefore didn't notice the warnings Revolut provided. I therefore don't think it would've made much difference here whether Revolut had provided a more tailored warning or not, as it doesn't seem Mrs F was given much opportunity to read them. In any event I've had to also factor in that the scam Mrs F fell victim to is quite niche and not something we typically see. While it could fall under a more general bracket of 'advanced fee scam', I don't think there's much Revolut could've said in a general warning about these scams that would've resonated with Mrs F – as the story she was told simply isn't something seen in many other cases.

Overall, to summarise, while I'm truly sorry to hear Mrs F fell victim to this scam, at a period in her life when she already felt vulnerable from her recent hip injury, I think the steps

Revolut took in highlighting the risks associated with these payments was proportionate in the circumstances. I don't think any intervention short of human interaction would've broken the spell Mrs F was under by the fraudsters and I can't conclude that such intervention was proportionate to the risk the payments she was making posed.

I've gone on to consider whether Revolut could've done anything more to recover Mrs F's money, once it became aware that she'd fallen victim to a scam. Unfortunately, as the first payment went to a cryptocurrency account, there's very little a bank can do to recover these payment types. Similarly, the subsequent payments Mrs F made were all 'push to card' payments, made internationally. Again I think on this basis, any recovery attempts Revolut could've made would have likely been unsuccessful.

Lastly I've thought about the claims process Mrs F experienced when making Revolut aware of the scam. I agree that Revolut made the process more stressful than it needed to be when Mrs F was already at a low point. There was clearly a duplication of messages sent to Mrs F and continuous requests made for something that Mrs F had explained she couldn't provide, despite several attempts. Mrs F also made a number of requests for someone to call her to discuss this further which, given the circumstances, could've really benefitted her. On this basis, while the delay in handling Mrs F's claim didn't impact the overall outcome Revolut reached, I think the £150 recommendation is fair to reflect the additional distress this caused her.

My final decision

My final decision is that I uphold Mrs F's complaint in part, and require Revolut to pay £150 compensation for trouble and upset caused,

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs F to accept or reject my decision before 4 November 2024.

Kirsty Upton
Ombudsman