

The complaint

Mrs F 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 the parties and has been previously set out by our investigator.

Briefly, Mrs F fell victim to a cryptocurrency investment scam in the spring of 2023. Between March and May 2023, she was tricked into parting with her funds in connection to what she thought was an investment opportunity. But it turned out to be a scam.

Mrs F purchased cryptocurrency from a cryptocurrency provider using her Revolut card as well as by making electronic payments. The purchased cryptocurrency was then sent to her 'investment' account. At other times, Mrs F also used her Revolut account to exchange fiat currency into cryptocurrency, before sending it on ('cryptocurrency withdrawal').

The following debit transactions are relevant to this complaint –

Transaction	Date	Transaction Type	Amount
1	31 March	Fiat to Crypto exchange	£1,700
	3 April	Crypto withdrawal	0.07200000 BTC
2	6 April	Faster payment	£6,500
3	6 April	Fiat to Crypto exchange	£1,844
	6 April	Crypto withdrawal	0.07000000 BTC
4	6 April	Debit card	£4,388
5	9 May	Debit card	£4,300

Mrs F realised she'd been scammed when she was asked to pay fees – tax – when she requested a withdrawal. She reported this to Revolut, but it refused to refund her loss. A complaint was made and subsequently referred to our service.

In its file submission, Revolut raised concerns about whether our service could consider the cryptocurrency withdrawals Mrs F made in relation to the scam. In their assessment, our investigator explained that although cryptocurrency withdrawals on their own wouldn't fall under our jurisdiction, Mrs F's complaint was broader than the final step of withdrawing the cryptocurrency. To the extent that her concerns involve the cryptocurrency withdrawals from her account, the investigator was satisfied that given the nature of this complaint we could look into those concerns as far as they relate to the exchange of fiat money into cryptocurrency.

In relation to the merits of Mrs F's complaint, the investigator concluded that although Revolut should have provided a warning specific to investment scams involving

cryptocurrency on a few occasions, they weren't persuaded that such a warning would have prevented her losses. The investigator also concluded that Revolut couldn't have done anything else to recover her money once it became aware of the scam.

Mrs F didn't agree with the investigator's conclusions and asked for her complaint to be reviewed by an ombudsman.

Preliminary matters

Revolut hasn't responded to the investigator's findings on matters relating to our jurisdiction. I've therefore assumed that it now accepts the investigator's stance, and I only need to decide the merits of the complaint.

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.

It isn't in dispute that Mrs F authorised the transactions in question. She's therefore presumed liable for the loss in the first instance.

But, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider good industry practice at the time, I consider it fair and reasonable in March 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); and
- 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 limited 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 taken additional steps when Mrs F authorised Transaction 1 (see table above). I accept that Mrs F was exchanging fiat currency into cryptocurrency. But that in and of itself doesn't mean that the transaction ought to have flagged as suspicious. Buying cryptocurrency is a legitimate exercise.

But by the time Mrs F authorised Transaction 2 (the faster payment to purchase cryptocurrency from a cryptocurrency provider), Revolut ought to have recognised that it carried a heightened risk of financial harm from fraud. Revolut knew or should have known that the intended destination of that payment was a cryptocurrency platform, and there was a significant jump in the amount involved. I consider Revolut should have taken additional steps when it received Mrs F's instruction. The information I've seen shows that this is what it did.

Revolut says it paused Transaction 2 and asked Mrs F to confirm the payment purpose by selecting from a list of options. It then provided a scam warning tailored to the option selected over a series of screens which couldn't be skipped. Revolut has provided a screenshot showing the list of options Mrs F could make a selection from. But it hasn't been able to confirm what option was selected.

I've thought carefully about this. I've no reason to believe that Mrs F would have withheld the fact that the transaction was in relation to an investment. I've also seen no indication that she expressed mistrust of Revolut or financial firms in general. So, although I can't be certain, on balance, I think it's more likely than not that Mrs F would have selected the closest or most appropriate option, i.e., *cryptocurrency* or *investment*.

Had Mrs F had so, I would have expected Revolut's warning to have addressed the key features of common cryptocurrency investment scams. For example: an advertisement on social media; an 'account manager', 'broker' or 'trader' acting on their behalf; returns that are too good to be true; and the use of remote access software.

But I'm not persuaded that such a warning would have prevented Mrs F's losses. I'll explain why.

A transfer Mrs F made from her bank account elsewhere to Revolut on 30 March flagged as suspicious and was blocked by that bank. Mrs F phoned the bank the next day to discuss the block. I've seen systems notes from the time. And I've also listened to a recording of the call that took place. Mrs F can be heard telling the agent that she's transferring funds to her Revolut account which she's had for some time and has previously transferred money to. When probed, she confirms she's doing some investments.

The agent picks up on this and, having previously ruled out the possibility that Mrs F had fallen victim to a safe account scam, discusses the prevalence of investment scams. They encourage Mrs F to check the firm with the Financial Conduct Authority and to also check Trustpilot reviews.

The agent also mentions that scams of this nature are often found through advertisements on social media platforms, and that majority of them are a scam. And so, if Mrs F comes across such an opportunity, she should consider it as a red flag and carry out due diligence. Mrs F acknowledges the agent's advice and confirms that she's not being asked to move the money or pressured into doing so or being asked to lie to her bank. And the payment is released.

Having given this a lot of thought, some of what the agent said applied to Mrs F's circumstances. She had come across the firm on a popular social media platform. And a

third party was involved. In the initial complaint referral – submitted via solicitors who are no longer representing her – Mrs F told our service that the scammer advised her they would trade on her behalf to make things easier. As such, I think there were elements in her bank's warning which applied to Mrs F's circumstances. But they don't appear to have resonated with her as the transfer did go ahead. And once the money was paid into her Revolut account, Mrs F proceeded to exchange it into cryptocurrency.

Given the above, I'm not persuaded that a warning by Revolut, covering similar features would have positively impacted Mrs F's decision making. Based on her responses to questions from her main bank, as well as her communication with Revolut over its in-app chat when it restricted her account later on the day of the suggested trigger point, I'm not convinced that the scam would have unravelled. When questioned by Revolut, Mrs F confirmed that she hadn't been contacted or encouraged to invest by someone she didn't know or had only met online recently. She explained that she'd been on courses and was still on one. She reassured the agent that the courses constantly highlighted such risks and warned participants to seek advice through them if necessary.

In the circumstances, I think it's unlikely that Revolut could have prevented Mrs F from going ahead with Transaction 2 had it questioned her about it. I think Mrs F would have answered in the same way as she did two days later when she discussed the restriction on her Revolut account. It seems it was only after the final transaction, when she asked to make a withdrawal and was told she needed to make a further payment, that prompted Mrs F to look into this further and she came to the realisation that she'd been scammed.

I know that Mrs F will be disappointed with this outcome. Not least because the matter has been ongoing for some time. But I can only ask Revolut to reimburse Mrs F if I find that any wrongdoing on its part is the proximate cause for her loss. I've explained above why I don't believe that to be the case.

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 it might be possible to recover the money. Given Mrs F purchased cryptocurrency, which was then sent to an external wallet in the scammer's control (albeit she didn't know this at the time), it's unlikely recovery would have been successful. Revolut was able to recover 58 pence from the cryptocurrency platform, presumably from Mrs F's wallet with it. But in the circumstances of what happened, I don't think Revolut could have done anything else to recover Mrs F's funds.

I fully acknowledge that there's a considerable sum of money involved here. Despite my natural sympathy for the situation in which Mrs F 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 Mrs F to accept or reject my decision before 6 March 2025.

Gagandeep Singh
Ombudsman