

The complaint

Miss T 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 February 2023, Ms T came across an advert for an investment company on social media. She completed an online contact form and was contacted by someone I'll refer to as "the scammer" who claimed to work for Company C and told her he'd been her financial advisor. Miss T opened an account on the trading platform and made an initial deposit of £250. The scammer told her to first purchase cryptocurrency through cryptocurrency exchange companies and then load it onto an online wallet. She sent funds to Revolut from Bank S and Bank L, and between 16 February 2023 and 18 October 2023, she made 48 card payments to four different cryptocurrency exchanges totalling £131,687.75. During the scam period she took out a loan for £10,000 to fund the payments.

Miss T realised she'd been scammed when the scammer kept encouraging her to make larger payments. She complained to Revolut but it refused to refund the money she'd lost and so she complained to this service with the assistance of a representative.

Her representative argued that the payments were large and unusual and Revolut should have questioned her about the circumstances, warned her about the potential risks, and advised her to exercise due diligence. And had it done so she'd have taken the necessary steps to address the risk.

Responding to the complaint, Revolut said there was no valid chargeback because once the funds were deposited to the beneficiary accounts and the service was considered to have been provided. And Miss T was sending funds to cryptocurrency accounts in her own name, so the transactions from Revolut weren't fraudulent.

It said the account was opened on 9 August 2022 with the purpose of the account declared as 'crypto' and 'transfers', so the payments were in line with the selected account purposes. It said Miss T had opened the account in connection with a scam she'd fallen victim to in 2022, and that it had been mostly dormant since then.

It said at the time of the payments, it was an Electronic Money Institute (EMI) and typically this type of account is opened and used to facilitate payments of a specific purpose and often not used as a main account, so the payments weren't out of character or unexpected with the typical way in which an EMI account is used. It also said there was no transactional activity it could have used to determine what can be deemed as unusual activity and so it didn't show any warnings.

It cited the Supreme Court's judgment in *Philipp v Barclays Bank UK plc* [2023] UKSC 25 where Court held that in the context of APP fraud, where the validity of the instruction is not in doubt, 'no inquiries are needed to clarify or verify what the bank must do. The bank's duty is to execute the instruction and any refusal or failure to do so will *prima facie* be a breach of duty by the bank'.

It said that for this service to effectively apply the reimbursement rules to self-to-self transactions executed by Revolut is an error of law. Alternatively, we have irrationally failed to consider the fact that these transactions are self-to-self and therefore obviously distinguishable from transactions subject to the regulatory regime concerning APP fraud. And it is irrational (and illogical) to hold Revolut liable for customer losses in circumstances where Revolut is merely an intermediate link, and there are typically other authorised banks and other financial institutions in the payment chain that have comparatively greater data on the customer.

It also said Miss T was negligent because she'd fallen victim to a scam six months before, so she should have known about the hallmarks of such scams and done more diligence. It said if she'd checked online and she'd have seen C doesn't offer cryptocurrency exchange services, and there were negative reviews on Trust Pilot.

Our investigator thought the complaint should be upheld. He didn't think Revolut needed to intervene in the first two payments because they were low-value. But he noted the third payment brought the cumulative total for the day to £4,400 to a high-risk cryptocurrency merchant, so Revolut should have given Miss T written warning that was tailored to cryptocurrency investment scams. Had it done, as there was nothing to suggest she wouldn't have heeded a warning from Revolut, he thought she'd realised there were 'red flags' present and done additional checks which would have uncovered the scam.

He thought Revolut should refund the money she'd lost from the third payment onwards, but he recommended that the settlement should be reduced by 50% for contributory negligence. He said he hadn't seen any evidence that Miss T had tried to verify that the investment was legitimate having found it on social media before investing large amounts of money on the advice of someone she'd never met. He noted that she'd been scammed before and so she ought to have known about the risks and had she done some basic research she'd have seen warnings about cryptocurrency investment scams, which might have made her think twice about the investment.

Finally, he said there would have been no chance of a successful recovery because Miss T reported the scam over three weeks after the final payment. And there were no chargeback rights because Miss T paid a legitimate cryptocurrency exchange and would have received a service. He also said she wasn't entitled to any compensation.

Miss T has indicated that she's happy with the outcome, but Revolut has asked for the complaint to be reviewed by an Ombudsman.

It has argued that the payments were sent to an account in Miss T's name, and she lost control of the funds further in the chain, so the fraudulent activity didn't occur from the Revolut platform. It also said it is relevant to consider other bank interventions as the funds that originated with Revolut came from Miss T's own external bank 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.

Having done so, I've reached the same conclusion as our investigator. And for largely the same reasons.

I'm satisfied Miss T '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, she is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Miss T 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 February 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;
- 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 genuine cryptocurrency exchange companies. 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 ought to have intervened to warn Miss T when she tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect Revolut to intervene with a view to protecting Miss T from financial harm due to fraud.

The payments didn't flag as suspicious on Revolut's systems and she wasn't shown any warnings. I've considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how Miss T normally ran her account and I think they were. The first two payments were relatively low value and Miss T was sending funds to a legitimate cryptocurrency merchant, so Revolut didn't need to intervene. But by the time she made the third payment, the cumulative total of the three payments she'd made that day had risen to £4,400, so Revolut ought to have intervened.

In February 2023, we would expect it to have shown Miss T a written warning that was tailored to cryptocurrency investment scams. 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 balance, I think it would have. There were some key hallmarks of cryptocurrency investment scams present in the circumstances of Miss T's payments, such as finding the investment on social media and being assisted by an account manager.

Bank L has confirmed it didn't intervene in any of the payments Miss T made from that account and we know Bank S intervened on 23 August 2023, with Miss T stating that she hadn't been asked to send the money or provide misleading information. I've thought about whether this means it's less likely that Miss T would have acted on a tailored warning from Revolut in February 2023, and I don't think it does. Firstly, the intervention I would expect from Revolut wouldn't require Miss T to give it any information and, secondly, the intervention from Bank S happened much later in the scam at a point when she'd invested more money and had more to lose as a result of a payment being blocked.

I haven't seen any evidence that Miss T was asked, or agreed, to disregard any warning provided by Revolut and I haven't seen any evidence to suggest she was so taken in by the scammer that she wouldn't have listened to advice from Revolut. Therefore, on balance, had Revolut provided Miss T with an impactful warning at the beginning of the scam that gave details about cryptocurrency investment scams and how she could protect herself from the risk of fraud, I believe it would have resonated with her and that she'd have paused and looked more closely into the scammer before proceeding. Had she done so, she would likely have come across the negative reviews and other information about cryptocurrency investments as referenced by Revolut and decided not to make any further payments.

As I'm satisfied that Revolut missed an opportunity to prevent the scam and that this represented a missed opportunity to have prevented her loss, I agree with our investigator that it should refund the money she lost from the third payment onwards.

Contributory negligence

I accept there's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence and in the circumstances, I think Miss T could have done more to protect herself. She accepts that she'd previously been scammed and in those circumstances, I would expect her to have been more mindful of the potential risks and done some basic due diligence which would likely have raised some doubts about C and, ultimately, prevented her loss. So, I agree the settlement should be reduced by 50% for contributory negligence.

Recovery

I don't think there was a realistic prospect of a successful recovery because Miss T paid accounts in her own name and moved the funds onwards from there.

Miss T's own testimony supports that she used cryptocurrency exchanges to facilitate the payments. It's only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchanges would have been able to evidence they'd done what was asked of them. That is, in exchange for Miss T'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 Miss T 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.

My final decision

My final decision is that Revolut Ltd should:

- refund the money Miss T lost from the third payment onwards.
- this settlement should be reduced by 50% to reflect contributory negligence.
- pay 8% simple interest*, per year, from the respective dates of loss to the date of settlement.

*If Revolut Ltd deducts tax in relation to the interest element of this award it should provide Miss T with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss T to accept or reject my decision before 28 April 2025.

Carolyn Bonnell
Ombudsman