

The complaint

Ms L is unhappy that Revolut Ltd (“Revolut”) won't refund the money she lost to job scam.

What happened

In July 2023 Ms L came across remote job opportunity which involved completing tasks for commission. Ms L signed up to the job platform where she would complete her tasks and she could see her commission building up. Ms L was then assigned a set of tasks she was told attracted higher commission but also caused her balance on the job platform to turn negative. Ms L then needed to clear the negative balance by way of a deposit in cryptocurrency in order to unlock further tasks and earn the commission.

As a result of the scam Ms L made the following payments – some to cryptocurrency platforms, some to individuals to purchase cryptocurrency on the peer-to-peer market (P2P).

Transaction #	Date	Amount	Type	Payee
1	08/07/2023	£100.00	push to card	YM
2	09/07/2023	€ 269.70	card	Cryptocurrency M
3	12/07/2023	€ 500.00	card	Cryptocurrency M
4	16/07/2023	€ 200.00	card	Cryptocurrency M
5	17/07/2023	€ 817.44	card	Cryptocurrency M
6	17/07/2023	€ 815.48	card	Cryptocurrency M
7	20/07/2023	€ 1,037.28	card	Cryptocurrency M
8	21/07/2023	£200.00	transfer	Cryptocurrency M
9	21/07/2023	€ 1,000.00	card	Cryptocurrency M
10	21/07/2023	€ 1,000.00	card	Cryptocurrency M
11	07/08/2023	€ 3,000.00	transfer	LZ
12	12/08/2023	€ 2,682.00	push to card	AB
13	12/08/2023	€ 1,000.00	card	Cryptocurrency M
14	18/08/2023	€ 3,000.00	transfer	YU
15	28/08/2023	€ 1,500.00	card	Cryptocurrency M
16	29/08/2023	€ 2,600.00	card	Cryptocurrency O
17	30/08/2023	€ 2,800.00	card	Cryptocurrency O
18	14/09/2023	€ 5,000.00	card	Cryptocurrency M2
19	17/09/2023	€ 642.75	card	Bank W
20	17/09/2023	€ 382.83	card	Bank W
21	18/09/2023	€ 1,574.79	card	Bank W
22	18/09/2023	€ 862.76	card	Bank W
23	19/09/2023	€ 1,000.00	card	Cryptocurrency M
24	22/09/2023	€ 550.00	card	Cryptocurrency M2
25	24/09/2023	€ 1,000.00	push to card	AL
26	26/09/2023	€ 50.00	card	Cryptocurrency M

27	28/10/2023	€ 2,965.83	transfer	XN
----	------------	------------	----------	----

The two greyed out payments were returned to Ms L

The cryptocurrency was placed in wallets in Ms L's own name and from there she transferred the cryptocurrency to what she thought was the job platform but unbeknown to her at the time was actually going to the scammer. Ms L followed the instructions of the scammer until the deposit amounts became too high and she eventually realised she'd been the victim of a scam.

Revolut declined to refund Ms L. It said:

- The payments were authorised and such payments should proceed without undue delay.
- It provided warnings which were sufficient to prevent the scam, but Ms L chose to ignore them.
- There was a lack of due diligence in this case.

Our investigator did not uphold the complaint. He felt that proportionate intervention would not have made a difference.

Ms L's representative did not agree that Revolut only needed to warn about cryptocurrency investment scams as job scams have become more prevalent. It believes for an account that is sending rapidly increasing amounts of money in cryptocurrency, the customer marking the payment purpose as 'something else' does not diminish the need for further investigation. It said Revolut could see the payments were going to cryptocurrency and so should have realised payments made to individuals on the peer-to-peer market were also likely to be cryptocurrency. The cover story Ms L gave her high street bank would not have held up to reasonable scrutiny.

As the complaint has not been resolved informally, it's been passed to me for a 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.

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

In deciding what's fair and reasonable, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

Where the evidence is incomplete, inconclusive or contradictory, I reach my decision on the balance of probabilities – in other words, on what I consider is more likely to have (or would have) happened in light of the available evidence and the wider circumstances.

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.

However, taking into account relevant law, regulatory 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 July 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); 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.

And for transactions after 31 July 2023

- 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;

It isn't in dispute that Ms L has fallen victim to a cruel scam, or that she authorised the payments she made by bank transfers.

Whilst we now know the circumstances which led Ms L to make the payments using her newly opened Revolut account and the process by which her money fell into the hands of the fraudster, I am mindful that Revolut had much less information available to it upon which to discern whether any of the payments presented an increased risk that Ms L might be the victim of a scam.

The transactions were not scam payments themselves but rather genuine transactions for the genuine purchase of cryptocurrency either by cryptocurrency platforms or by third parties on the peer-to-peer market. The scam happened after that by moving the genuine currency onto the scammer's wallet.

However, I am satisfied that by the time Ms L made the payments in July 2023, Revolut ought fairly and reasonably to have recognised that its customers could be at an increased risk of fraud when using its services to purchase cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name.

What did Revolut do to warn Ms L?

Revolut explained that it provided warnings for all the new beneficiaries set up.

“Do you know and trust this payee? If you're unsure, don't pay them, as we may not be able to help you get your money back.”

It also provided warnings on 8 July 2023 and 7 August 2023 in response to the payment purpose Ms L gave: "Something else".

What kind of warning should Revolut have provided to Ms L?

Payments 1-9

This was a newly opened account – so there was no prior history to compare the transactions to. But I think Revolut should have identified some of the payments were going to cryptocurrency providers (M, O and M2 are well-known cryptocurrency providers) but I don't agree it would have been obvious the other payments in the table above were going to cryptocurrency. The initial payments were low in value and spread out. So I don't think Revolut should reasonably have suspected that they might be part of a scam.

On balance, taking into account that Revolut needs to take an appropriate line between protecting against fraud and not unduly hindering legitimate transactions, and also considering the value of the first nine payments, I don't think Revolut ought to have been sufficiently concerned about the first nine payments that it would be fair and reasonable to expect it to have provided warnings to Ms L at this point.

Payment 10

But I do think Revolut ought to have recognised Ms L was at risk of financial harm from fraud when she purchased cryptocurrency using her Revolut account on 21 July 2023 (transaction 10). In line with the good industry practice that I've set out above, I think a proportionate response to that risk (at the time the transaction was made in July 2023) would have been for Revolut to have provided a tailored written warning relevant to cryptocurrency investment scams.

I appreciate Ms L's representatives feel a job scam warning should have been provided but at the time in question, I consider what I have set out above would have been proportionate to the potential risk identified.

Payments 18

I think by payment 18 in August 2023, Ms L had made a series of higher value payments to cryptocurrency and payment 18 was for € 5,000.00 (over £4,000). Revolut should have been mindful that cryptocurrency scams have become increasingly varied over the past few years. Fraudsters have increasingly turned to cryptocurrency as their preferred way of receiving victim's money across a range of different scam types, including 'romance', impersonation and investment scams.

By the time of payment 18, Revolut ought to have attempted to narrow down the potential risk further. I'm satisfied that when Ms L made payment 18, Revolut should – for example by asking a series of automated questions designed to narrow down the type of cryptocurrency related scam risk associated with the payment she was making – have provided a scam warning tailored to the likely cryptocurrency related scam Ms L was at risk from.

As such, I'd have expected Revolut to have asked a series of simple questions in order to establish that this was the risk the payment presented. Once that risk had been established, it should have provided a warning which was tailored to that risk and the answers Ms L gave. I accept that any such system relies on the accuracy of any information provided by the customer and cannot reasonably cover off every circumstance.

If Revolut had provided warnings of the type described, would that have prevented the losses Ms L suffered?

Payment 10

If Revolut had provided a written warning tailored to cryptocurrency investment scams for payment 10 - I'm not persuaded it would have resonated with Ms L or prevented her loss. Ms L wasn't sending payments in connection with an investment opportunity. So, I'm not convinced that a written warning relating to cryptocurrency investment scams would have resonated with Ms L and the circumstances she found herself in. I think it's likely that Ms L would have seen a warning about investment scams involving cryptocurrency and disregarded it, as she wasn't making an investment, and proceed with the payment.

Payment 18

I am aware Ms L gave her high street a cover story when questioned over the telephone about the purpose of her payments from her account with it into her account with Revolut. I acknowledge that it wouldn't have been possible for Ms L to have plausibly told Revolut that she was moving funds in respect of needing money in euros to make a music video abroad as she told her bank. Revolut would have known that this wasn't true, as it could readily identify that the funds were being transferred to a cryptocurrency wallet. But this doesn't mean that Ms L would have been honest about the reason for the payment.

I have reviewed the messages Ms L had with the scammer. The evidence suggests Ms L allowing the scammer to guide her through the payments and sharing screen shots with him.

I'm therefore persuaded that if more questions had been asked of Ms L, she would have reverted to the scammer on how to answer them. That's evident given Ms L didn't always answer Revolut's questions accurately because of the coaching she was receiving from the scammer.

At one stage she was warned that a cryptocurrency wallet she was trying to send money to, was recognised as a scam. Instead of independently checking things out further – Ms L turned to the scammer for advice and took his explanation at face value. So, I think on balance she would have done the same with any written warnings from Revolut.

I appreciate that further intervention beyond written warnings might have made it harder for Ms L to follow the scammer's advice. But I don't think Revolut needed to go further than what I've set out above.

I'm also not persuaded there were any prospects of Revolut successfully recovering the funds, given the money was used to purchase cryptocurrency from legitimate providers.

Ms L has fallen victim to what can only be described as a cruel and callous scam. I'm sorry she has lost so much money, and I can understand why she would like to be compensated for all her losses. But I can only ask Revolut to reimburse Ms L if I find that any wrongdoing on its part caused her loss and I'm not persuaded that this was the case. For the above reasons, I don't think Revolut has acted unfairly by not refunding the payments.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms L to accept or reject my decision before 21 May 2025.

Kathryn Milne
Ombudsman