

The complaint

Ms C is unhappy that Revolut won't refund the money she lost to a scam.

Ms C has used a professional representative to bring this complaint to our service and they have made submissions on her behalf. For consistency, I'll refer to Ms C throughout.

What happened

I issued my provisional decision on this complaint on 8 October 2024. I wanted to give both sides a chance to provide any further evidence and arguments before I issued my final decision. That provisional decision forms part of this final decision and is copied below.

What happened

On 24 July 2023, Ms C received a message from a recruitment company (that I'll call V). They claimed to have received Ms C's job application and said a hiring manager would contact her shortly about a job opportunity. The hiring manager messaged Ms C and explained he worked for an international marketing company (that I'll call H). The job opportunity involved Ms C completing a certain number of 'tasks' per day in the app to increase online traffic for well-known online platforms and brands. After working for five consecutive days, she'd receive a salary of \$800. After working for 15 days she'd get a bonus, and again if she worked for 30 days. She would also only receive a contract after working for 14 days.

Ms C completed some online training, from which she earned a small commission. She then had to top this up to \$100 to start working. The fraudster told Ms C how to open an account with a cryptocurrency exchange (that I'll call C) to receive her wages and make payments to the platform. Ms C made card payments from Revolut to C, in order to purchase cryptocurrency. She then contacted H's customer service team and was given details of where to send the cryptocurrency to in order to complete the tasks on H's platform. At the end of each set, she'd see her balance increase. But she needed to deposit funds again to start a new set.

When Ms C's account went into a negative balance, she had to make payments to clear it. As Ms C continued to complete tasks, the tasks grew more expensive. As she continued to be asked to make further payments to access her funds, she realised she'd been scammed. She reported the scam to Revolut on 15 August 2023. On 11 September 2023, Ms C asked Revolut to raise a chargeback. However, this was declined on 19 September 2023, because it said there were no chargeback rights as the transactions were money transfers.

The case was referred to our service and Revolut maintained its defence. In summary, it said:

- *Revolut acted in line with the rules set out by the card network, which Ms C agreed to abide by when she opted to use the card network services.*
- *In accordance with regulation and its terms and conditions, Revolut should execute payments its customer authorises it to make without undue delay. As the payments were authorised by 3DS secure, Revolut is not liable.*

- The card payments were made to a legitimate merchant who provided the services Ms C paid for. It had no grounds to raise a chargeback for goods/services not delivered. Nor did it have grounds to raise a chargeback on the basis the payments were unauthorised.
- The fraud didn't take place on Revolut's platform. It was the intermediary who received funds from Ms C's main bank (Bank N) and sent the funds to Ms C's account with C, where they were subsequently lost. It is irrational for our service to hold Revolut liable in such cases.
- The Contingent Reimbursement Model (CRM) Code nor the Payment Services Regulation's mandatory reimbursement scheme would require Revolut to refund 'self-to-self' transactions. Such transactions do not meet the DISP rule definition of authorised push payment (APP) fraud as the funds do not go to 'another person'. Nor do they meet the APP fraud definition under the CRM Code or PSR's mandatory reimbursement scheme.
- Revolut sent Ms C an email containing scam advice on 19 May 2023. Ms C neglected this warning and proceeded without questioning the legitimacy of the scammer.
- The payments were made over three days, so Ms C had time to check the legitimacy of the job offer, but she didn't perform due diligence. There were several red flags and inaccuracies regarding the job that she ought to have picked up on. Ms C ought to have known it was too good to be true. This degree of carelessness displaces any liability Revolut might otherwise have had.
- The transactions were not unusual for Ms C. Cryptocurrency investments are becoming more popular amongst laypersons. The account activity suggested Ms C was a legitimate user of a cryptocurrency platform.
- Revolut intervened on the payment for £205.98 and blocked Ms C's card, hence some of her initial attempts were declined. Ms C went to the card settings and unblocked her card and proceeded with further payments.

Our investigator looked into things and upheld Ms C's complaint in part. They thought that Revolut ought to have intervened on payment 6 and a tailored written warning would have prevented Ms C from proceeding. However, they thought Ms C should share liability. So they recommended Revolut refund 50% of Ms C's loss from payment 6, less any refunds or credits. And they recommended it also pay 8% simple interest on this amount, from the date the payments were made until the date of settlement.

After some further explanation was provided as to why Revolut didn't need to intervene until payment 6, Ms C accepted this outcome. Revolut did not. As no agreement could be reached, this case was passed to me to be decided.

What I've provisionally 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.

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 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;
- from 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;
- 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, when deciding whether to intervene.

In light of the above, I've considered whether Revolut can fairly and reasonably be held liable for Ms C's loss. Whilst I think Revolut ought to have recognised that Ms C was at a heightened risk of financial harm from fraud when making the £986.91, I don't think Revolut could have reasonably prevented her loss. I know this will be disappointing for Ms C, so I'll explain why.

Firstly, I'm in agreement with our Investigator that Revolut ought to have intervened further when Ms C made the payment for £986.91 from her Revolut account. I say this because, by 31 July 2023, the value of the disputed payments began to significantly increase, with the payment for £986.91 being the third payment in a short space of time, with over £3,000 debiting the account. I'd also expect Revolut to recognise, in July 2023, the risks of multi-stage scams involving cryptocurrency. Given the industry awareness of this since mid-2018, and such scams increasing over time, with losses suffered reaching record levels in 2022, I'd expect Revolut to recognise, at the time the payments were made, that cryptocurrency related transactions carry an elevated risk of the likelihood of being related to a fraud or scam.

Taking all of the above into account, I think Revolut ought to have made further enquiries with Ms C about the payment for £986.91, with the starting point that Ms C was making a payment related to cryptocurrency. And it could have made such enquiries, for example, by asking a series of automated questions designed to narrow down the type of cryptocurrency scam Ms C was at risk of and provided a scam warning tailored to that risk.

But even if it had done so, I'm not persuaded that would have prevented Ms C's loss. I'll explain why.

I can see in the messages between Ms C and the fraudster that on 30 July 2023 at 14:52, Ms C tells the scammer that she had difficulties with her card and suspected the bank had blocked it for security reasons. So, she used another card instead. It's not clear which card Ms C had difficulties using. I can see she made a number of card payments to different cryptocurrency exchanges from Bank N between 28 July 2023 to 31 July 2023, before continuing to make payments from Revolut instead. I can also see her Revolut card was declined a number of times on 30 July 2023, around 15:40, but she resumed successful payments at 18:04. She explained to the fraudster that her card was blocked 'Because of

[sic] scam, as soon as they see crypto...They lock the account'. The fraudster reassured her it's because companies don't like 'employees' investing in cryptocurrencies. This tells me that Ms C was desensitised to warnings about cryptocurrency scams.

This is further supported by the evidence I've obtained from Bank N. I've seen evidence that when Ms C made a payment on 31 July 2023, from Bank N to Revolut to fund the scam, she used the payment reference 'Holidays'. Ms C says the scammer told her to use this as the reference. She explained she was under stress at the time because she was worried if she didn't pay, she'd lose all her money. Bank N intervened and made enquiries with Ms C about this payment, through a series of automated questions. When asked about the purpose of the payment, Ms C selected the option relevant to 'investments'. Although I am aware that there was no option for an 'employment opportunity' to choose from. However, I've seen the warning it presented to Ms C and a lot of it was relevant to her circumstances, despite it being focused on investments. It warned her against opportunities found on social media platforms, and the promise of high returns with little or no risk. It warned against fraudsters setting up fake cryptocurrency investments to steal people's money, and whilst it might look professional it's a scam. It warned against fraudsters creating a sense of urgency to get you to act quickly. And it warned against paying up front fees, which is what Ms C was being asked to do to gain employment. Ms C says she was under a lot of stress and fear and 'just wanted it all to finish' so she proceeded after seeing this warning. I accept this warning wasn't completely specific to Ms C's circumstances, but I am persuaded there was enough contained within the warning that ought to have resonated with Ms C.

I can also see on 1 August 2023 at 19:01 she said, 'Everyone was telling me to stop because this was a scam...And I tried once more....And I end up without nothing'. This tells me Ms C was aware of the possibility that she was being scammed, as she was warned by third parties, yet in her own words, she 'tried once more'.

Taking all of the above into account, I'm not persuaded that an online warning from Revolut would have prevented Ms C from making further payments. Firstly Ms C's testimony suggests the fraudster coached her through the payment from Bank N, so I can't be certain that Ms C wouldn't have been coached through any warnings from Revolut. But also, Ms C let me know she was under pressure to make the payment for fear she'd lose all her money, so she bypassed a warning that contained information relevant to the circumstances she found herself in. So I don't think that an online written warning from Revolut more likely than not would have persuaded her against proceeding, given the pressure she was under and fear she'd lose the money she'd invested already if she stopped. I'm also not persuaded, under these circumstances and considering the payments in dispute, that it would be reasonable to expect Revolut to have intervened further at a later point.

I have a lot of sympathy for Ms C and I'm sorry she lost this money in such a cruel way. I also know that fraudsters can be incredibly persuasive and I've no doubt she was under a lot of stress and pressure at the time. However, I have to remember that it's not Revolut who has stolen this money from Ms C – it's a fraudster. Whilst I agree that Revolut failed to deliver a proportionate intervention in these circumstances, I'm not convinced that this error had a material impact on the losses Ms C suffered. The weight of evidence compels me to believe that Ms C more likely than not would have bypassed such an intervention, given her strong motivation for proceeding. So for these reasons, I don't find Revolut is liable for her loss.

Recovery of funds

Ms C made the payments to C – a legitimate cryptocurrency exchange platform. And C provided the services Ms C paid for, that being the provision and/or transfer of

cryptocurrency. So I don't think there was any reasonable prospect of Revolut being able to recover Ms C's funds via a chargeback claim.

My provisional decision

My provisional decision is that I do not intend to uphold this complaint about Revolut Ltd.

Revolut confirmed it had nothing to add in response to my decision. However Ms C said that she didn't make any payments from Bank N to the scammers as they didn't release any amounts. She said she used Revolut because it didn't have strong security blocks on her account. Had Revolut blocked the account like Bank N did from the start, she would not have had a way to continue with the transactions.

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, my decision remains the same. I know that this scam has had a significant impact on Ms C and I'm sorry that she lost this money through the cruel actions of a fraudster. However, I've explained that while I think Revolut should have provided a warning of the type I've described, I need to consider whether its failure to do so, on the balance of probabilities, caused some of Ms C's loss. But for the reasons I've already explained, the evidence I've seen persuades me that an intervention of this nature would not have deterred Ms C from proceeding.

It's clear that Ms C had built up a rapport with the fraudster, and she was keeping them up to date with any obstacles she faced in terms of warnings or restrictions from the firms she was transacting with. This meant the fraudster was able to convince Ms C that 'companies don't like employees investing in cryptocurrencies'. And, by Ms C's own admission, the fraudster coached her through an intervention from Bank N, which was similar to the one I think Revolut ought to have provided. So I'm not persuaded that Revolut's failure to give a proportionate intervention on the payments Ms C was making, had a material impact on the loss Ms C suffered.

I appreciate Ms C's comments that she feels Revolut ought to have taken further steps to restrict her account, as she thinks Bank N did the same. However, I'm not persuaded this would have been a proportionate response to the risk identified on Ms C's Revolut account. For the reasons I've explained in my provisional decision, I think Revolut ought to have made further enquiries with Ms C about the payment for £986.91, with the starting point that Ms C was making a payment related to cryptocurrency. And it could have made such enquiries, for example, by asking a series of automated questions designed to narrow down the type of cryptocurrency scam Ms C was at risk of and provided a scam warning tailored to that risk. However, as I've set out, I'm not persuaded that Ms C would have been receptive to the type of intervention I've described. Nor am I persuaded that there was enough going on here for Revolut to have restricted Ms C's account, or to refuse to process the transactions she had asked it to make.

And whilst I've not seen any evidence that Bank N restricted Ms C's account, if Ms C was prevented from making payments to the scammer from her Bank N account, I still need to consider that she moved her funds from Bank N to Revolut in order to fund the disputed payments from her Revolut account instead. So even if Bank N did restrict Ms C's account, this did not prevent her losses either.

Taking these things into account, and for the reasons set out in my provisional decision, my

final decision is unchanged from the provisional findings I've set out above.

My final decision

For the reasons I've explained above, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms C to accept or reject my decision before 26 November 2024.

Meghan Gilligan
Ombudsman