DRN-5302362

The complaint

Ms P complains that Revolut Ltd won't refund money she lost when she fell victim to an employment scam.

Ms P is being represented by solicitors in her complaint.

What happened

In June 2023, Ms P was contacted on a popular instant messaging service by an individual purporting to be from a recruitment company. She was offered a job opportunity with a company "X" which required her to "push" apps forward on the website X was using in order to assist in getting the apps into the top 10 apps on the App store. It was explained to her that her job would involve completing "tasks" to earn commission.

The representative from X explained to Ms P that she would sometimes have to make an advance payment to complete "special tasks". Once the set of tasks was completed, the advance payment could be withdrawn alongside the commission. They also advised Ms P that she would receive cryptocurrency for completion of the training. Ms P states she was provided with reasons why X made use of cryptocurrency rather than traditional marketing methods, but our service hasn't been told what those reasons were. Ms P also states she was assured that her position was a safe job with no financial risk, and she wouldn't need to invest her own funds as she could utilise the cryptocurrency she received in training to make the initial investments.

In order to make the advance payment, Ms P was instructed to convert her money into cryptocurrency. She transferred funds into her existing Revolut account before using her Revolut card to purchase cryptocurrency from a cryptocurrency provider. The cryptocurrency was then sent to wallet addresses provided by her supervisor. Ms P believed she was making deposits into her account with X, given its account balance went up by the same amount.

Ms P expressed concerns to X when she kept being assigned special tasks which took her account into deficit and required top-ups from her own money. She was told not to worry as completing special tasks meant the returns would be higher. At one point, she was informed she needed to top-up her account to £19,000. After her withdrawal request was denied, Ms P recognised that the position wasn't a genuine employment opportunity and she had fallen victim to a scam.

Ms P made the following scam-related transactions, all card payments, from her Revolut account –

Payment	Date	Amount
Payment 1	13 June	£83.00
Payment 2	16 June	£60.00
Payment 3	16 June	£79.00
Payment 4	17 June	£710.50
Payment 5	17 June	£1,566.79

Payment 6	17 June	£3,318.21
Payment 7	17 June	£5,000.00
Payment 8	17 June	£137.58

Revolut declined to refund any of the disputed payments, saying Ms P had authorised them and there were no chargeback rights.
The complaint was referred to our service and it was considered by two investigators. Both concluded that there was nothing unusual about Payments 1-5 such that they ought to have concerned Revolut. But given the increased cryptocurrency related activity, it should have provided a written warning tailored to the most common types of cryptocurrency scams at the time, i.e., investment scams when Ms P authorised Payment 6. However, this wouldn't have uncovered the scam as Ms P had fallen victim to an employment scam.

By Payment 7, the investigators considered the intervention should have gone beyond a written warning and Revolut should have carried out a direct human intervention. Had it done so, there's nothing to suggest Ms P wouldn't have been honest about what she was doing, and the hallmarks of employment scams would have immediately become apparent to Revolut and further losses prevented. The investigators held Revolut liable for Ms P's losses from Payments 7 and 8, but they thought Ms P should share equal responsibly for what happened. So, they recommended Revolut to refund 50% of the last two payments, along with interest.

The second investigator noted that Ms P had some cryptocurrency left in her wallet with the cryptocurrency provider which was accessible to her. So, it was reasonable that the residual cryptocurrency balance was taken into account when calculating the Ms P's loss from Payments 7 and 8.

Revolut accepted the recommendation, but Ms P didn't. In summary, she says Revolut should have intervened at Payment 4 given it was highly unusual for the account. Ms P also states a human intervention should have taken place at Payment 5 (if not earlier). She also disagrees she should be held responsible for what happened, given she checked X's website and it appeared to be legitimate.

As the matter couldn't be resolved informally, the complaint's been passed to me to decide.

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 Ms P has fallen victim to a cruel scam here, nor that she authorised the card payments she made to cryptocurrency platforms (from where that cryptocurrency was subsequently transferred to the scammer).

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;

- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multistage 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.

Should Revolut have recognised that Ms P was at risk of financial harm from fraud?

I don't think Revolut should reasonably have suspected that Payments 1-3 might be part of a scam. It seems Ms P is also in agreement given she didn't dispute it when the investigator made the same finding. I accept Payment 4 is higher in value than previous payments made from the account in the 12 months preceding the scam payments. But I don't think it's *that* unusual such that it ought to have given Revolut cause for concern. I agree with Ms P that Payment 5 was unusually higher than her normal spending activity. But it isn't unusual for customers to make a one-off large payment every now and then. So, I don't think the payment warranted an intervention.

Even if I were to agree that Revolut should have taken identified that Payment 5 carried a heightened risk of financial harm from fraud, I also need to think carefully about what a proportionate warning in light of the risk presented would be in these circumstances. A written warning about the most prevalent type of cryptocurrency scams, i.e., investment scams, tackling some of the key features would have been a proportionate way for Revolut to minimise the risk of possible financial harm to Ms P by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

But I'm not persuaded that such a warning would have prevented Ms P's loss. This is because she wasn't sending payments in connection with an investment. She understood she was using the cryptocurrency platform to deposit funds into her account to spend with her 'employer'. So, it wouldn't have resonated with Ms P.

By the time Ms P authorised Payment 6, I think that the circumstances should have led Revolut to consider that she was at heightened risk of financial harm from fraud. In line with good industry practice and regulatory requirements, I'm satisfied that it is fair and reasonable to conclude that Revolut should have warned its customer before this payment went ahead. I've taken into account that many payments that look very similar to this one will be entirely genuine. I've given due consideration to Revolut's duty to make payments promptly, as well as what I consider to have been good industry practice at the time this payment was made.

I appreciate Ms P feels strongly that a direct intervention ought to have happened at this time. But I consider a proportionate response to the risk the transaction presented would have been for Revolut to have provided a written warning about the most prevalent type of cryptocurrency scams, i.e., investment scams, tackling some of the key features. As I've mentioned above, I'm not persuaded that such a warning would have prevented her loss.

Ms P says she doesn't believe the warning would have met the criteria set out by the Lending Standards Board's Contingent Reimbursement Model Code ("the CRM Code"). But the Code only applies to firms that are signatory to the Code or those that have committed to follow it and is specifically designed for victims of authorised push payment (APP) scams. Revolut hasn't signed up to the CRM Code or committed to follow it. Moreover, Ms P's payments were made using a card – these are 'pull' payments not 'push' payments, so they fall outside the scope of APP scams.

By the time Ms P authorised Payment 7, she had already sent over £5,000 in cryptocurrency related activity in one day. With Payment 7, that amount doubled to just over £10,000. In the circumstances – increasing pattern of cryptocurrency-related spending with a combined daily value of £10,000 – I think a proportionate response to the risk stemming from Payment 7 would be for Revolut to have attempted to establish the circumstances surrounding the payment before allowing it to debit Ms P's account. I think it should have done this by, for example, directing Ms P to its in-app chat to discuss the payment further.

If Revolut had attempted to establish the circumstances surrounding Payment 7, would the scam have come to light, and would that have prevented the losses Ms P suffered from that point onwards?

Revolut's already accepted that an intervention of the kind described would have uncovered the scam. But for completeness, I've found nothing within Ms P's written correspondence with the scammer that suggests she was asked, or agreed, to mislead Revolut or disregard any warnings provided. So, If questioned, I'm satisfied that Ms P would have explained she was purchasing cryptocurrency to make advance payments to complete the job tasks she had been assigned. And based on her response, I think Revolut would have been able to identify that Ms P was falling victim to an employment scam. This type of scam had been on the rise when Ms P's payments were made.

Overall, I consider that attempts to establish the circumstances surrounding Payment 7 followed by a scam warning specific to the risk identified would have given Ms P cause for concern. And I think she's likely to have decided not to go ahead with the payment, and subsequent payments, as a result of that intervention.

Should Ms P bear any responsibility for her losses?

I've thought about whether Ms P should bear any responsibility for her loss. In doing so, I've considered what the law says about contributory negligence, as well as what I consider to be fair and reasonable in all of the circumstances of this complaint.

I recognise that there were relatively sophisticated aspects to this scam, not least a platform, which was used to access and manage the user's apparent earnings and tasks. I can imagine this would have given some validation to the scheme.

But, at its heart, the scam appears to have been fairly implausible. While I haven't seen and heard everything that Ms P saw and was told, the scammer's explanation for how the scheme worked is quite baffling and I think Ms P ought reasonably to have questioned whether the activity she was tasked with carrying out (which doesn't appear to be particularly time-consuming or difficult) could really be capable of generating the returns or "income" promised. And it appears that Ms P did, give she seemed to have had concerns about repeatedly receiving special tasks by the point I consider Revolut should have taken further steps.

So, given the overall implausibility of the scam and Ms P's own apparent recognition of the risk of being continuously granted special tasks, I think she ought to have realised that the

employment opportunity wasn't genuine before going ahead with Payment X. In the circumstances, I consider she should also bear some responsibility for her losses.

I've concluded, on balance, that it would be fair to reduce Revolut's liability because of Ms P's role in what happened. Weighing the fault that I've found on both sides, I think a fair deduction is 50%.

Could Revolut have done anything to recover Ms P's money?

These were card payments to a cryptocurrency provider. I don't consider that a chargeback would have had any prospect of success given there's no dispute that the exchange provided cryptocurrency to Ms P, which she subsequently sent to the scammer.

So, I don't think Revolut should have done anything more to try and recover Ms P's money.

Putting things right

Ms P has confirmed that a residual balance remained in her cryptocurrency wallet after she realised she'd been scammed. So, in working out Ms P's losses from Payments 7 and 8 Revolut Ltd can, if it chooses to, deduct the GBP equivalent of the residual balance given it wasn't lost to the scam. But this isn't straightforward, because although Ms P has provided a screenshot which shows she had 0.49617904 Binance Coin (BNB) left in her cryptocurrency wallet, the screenshot is undated.

Due to the sums involved, I don't consider it reasonable to delay matters further to try and determine when this screenshot was taken to work out the GBP equivalent. In the circumstances, I'm going to assume that the BNB residual balance seen on the screenshot is what would have been in Ms P's wallet after she transferred the last scam related cryptocurrency to the scammer on 17 June 2023.

If Revolut Ltd chooses to make a deduction for the residual balance, to work out Ms P's loss, it'll need to calculate the GBP equivalent of the residual BNB based on the conversion rate on 17 June 2023 and deduct it from the total of Payments 7 and 8. It then needs to refund Ms P 50% of the loss, adding simple interest[1] at 8% per year on the refunded amount calculated from the date of loss to date of settlement.

My final decision

For the reasons given, my final decision is that I uphold this complaint. Revolut Ltd needs to put things right for Ms P as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms P to accept or reject my decision before 25 April 2025.

Gagandeep Singh
Ombudsman

[1] If Revolut Ltd considers that it's required by HM Revenue & Customs to deduct income tax from the interest award, it should tell Ms P how much it's taken off. It should also provide a tax deduction certificate if Ms P asks for one, so that the tax can be reclaimed from HM Revenue & Customs if appropriate.