DRN-5793964

The complaint

Mrs P complains that Revolut Ltd won't refund money she lost when she was a victim of a scam

What happened

In 2025 Mrs P was contacted on WhatsApp from a person, that we now know to be a scammer, regarding a remote-working job opportunity. The scammer claimed to have obtained Mrs P's details from a recruitment firm. I understand Mrs P thought this contact was legitimate as she had provided her CV to various online recruitment firms. Mrs P was told the role involved product optimisation, which required completing daily tasks on an online platform to receive commission. In addition to this, Mrs P would receive a salary based on the number of consecutive days worked.

As part of the scam there were 'merge missions' (tasks) that paid more commission. But these types of tasks required Mrs P to fund her account as they put it into a negative balance. To do this, Mrs P purchased crypto – totalling nearly £15,000 across 21 transactions between 1 February and 22 April 2025 - using her Revolut account before forwarding it to the scam.

When Mrs P tried to withdraw her funds, she was told by the scammer that she needed to pay a further £9,000 to repair her credit score. She also tried to call several numbers in the WhatsApp group chat she'd been added to, but none worked. At this point, Mrs P realised she'd been scammed.

Mrs P notified Revolut and raised a complaint. Revolut rejected it. Unhappy with this, Mrs P brought her complaint to the Financial Ombudsman. Our Investigator didn't think Revolut had to do anything further. In short, he said:

- Although crypto withdrawals aren't a regulated activity, and thereby not part of the Financial Ombudsman's jurisdiction, Mrs P's complaint is broader than the sending of crypto alone. Instead, it's about Revolut's failure to protect her from the scam. And here, the deposits of fiat currency into Mrs P's Revolut account are a regulated activity and the exchange of it into crypto is an ancillary payment service. So, these activities – but not the crypto withdrawals – can be considered by our service.
- He didn't think there was enough reason for Revolut to suspect Mrs P might be at risk of financial harm from fraud up to, and including, the 15th crypto exchange transaction. This is because those transactions wouldn't have looked suspicious to Revolut based on their value. So, he wouldn't reasonably have expected the transactions to have triggered Revolut's fraud detection system.
- Revolut should've carried out additional checks before processing the 16th crypto exchange transaction due to its higher value – which was a significant increase compared to the prior activity. But even if Revolut had done this, he didn't think they would've uncovered the scam or prevented the transaction being made. This is because Mrs P was being guided by the scammer on how to respond to any intervention by Revolut.

- And when Revolut did question Mrs P about several of the crypto withdrawals, and provided scam warnings, she didn't provide accurate information – as, for example, she confirmed it was for investment purposes. Consequently, even if Revolut had questioned Mrs P about the 16th crypto exchange transaction, he considered she would've answered similarly – thereby impacting Revolut's ability to provide warnings relevant to job scams.
- Even if Revolut had questioned Mrs P further about the subsequent crypto exchange transactions, it's likely she would've followed the scammer's instructions to ensure they were processed.
- There wasn't any prospect of recovering the funds here.

Mrs P disagreed with our Investigator. In short, she said:

- Revolut has a duty of care to identify and protect vulnerable customers. And she was experiencing a reduced income and heightened stress at the time, which put her in a vulnerable position.
- Although Revolut did intervene at times, this was reliant on self-reported honesty. And she was in constant contact with the scammer who was instructing her on how to respond to Revolut's questions. This meant Revolut's interventions were ineffective safeguards.
- Her account activity ought to have triggered more rigorous checks – as it went from initial small transactions to higher value transactions. And stronger interventions, such as direct telephone contact, could've broken the scammer's influence.
- The warnings she received from Revolut were generic and primarily framed around investment scams. And so, they didn't resonate with her actual situation.
- Revolut had the ability, and the responsibility, to detect she was at serious risk of harm before the funds were irretrievably lost.
- She received returns of about £200 during the scam which reinforced her belief it was a genuine job. And she was misled by the scammer as they used the name of a legitimate recruitment firm to reassure her it was a legitimate job. And the financial and emotional pressure she was under impaired her judgement at that time.

Our Investigator considered what Mrs P said, but his position remained the same. He explained Revolut weren't aware of Mrs P's circumstances at the time and so, as they wouldn't have known she was vulnerable, they didn't know to put enhanced protective measures on her account. He also said that, unfortunately, Mrs P was under the scammer's spell and believed what they told her. But because of this, it meant Revolut wouldn't have been able to uncover the scam had they intervened further and asked more questions about the transactions – as the scammers would've guided Mrs P on what to say to circumvent their checks.

Mrs P remained in disagreement with our Investigator and asked for her complaint to be referred to an Ombudsman. In short, she further added:

- Although unaware of her personal circumstances, Revolut has a duty to identify and support customers in vulnerable situations – even if those vulnerabilities aren't explicitly disclosed. Her account activity was unusual, high risk and inconsistent with prior account usage. It also had clear scam indicators – such as unusual recipients, new payees and atypical payment amounts. This should've prompted further scrutiny and protective interventions. Relying solely on her responses, at a time when she was under extreme psychological control from fraudsters, was not a reasonable safeguard.
- A well-designed scam intervention should go beyond scripted questions. Instead, they should use tailored scenario specific warnings to break a scammer's influence.

And in her case, a stronger intervention, such as putting a hold on the transaction(s) and an escalation to a human fraud investigator, could've prevented her losses.

- Under the FCA's Consumer Duty and the Contingent Reimbursement Model (CRM) code, Revolut had an obligation to prevent foreseeable harm. In her case, there were multiple opportunities to identify the risk and intervene more effectively.
- Her other bank – which I'll refer to as 'H' – refunded her in a separate scam where their systems were used. Revolut's refusal to do the same demonstrates an inconsistent and unfair approach within the banking sector.
- The consequences of the scam have been devastating, with her owing money to others and struggling to repay them. It has pushed her into serious financial hardship and caused significant emotional distress.
- Revolut failed in their duty of care, and a fair and just outcome would be for Revolut to refund her – recognising the inadequacy of their fraud prevention measures and the impact it's had on her life.

The matter has now 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.

I'm sorry Mrs P has been the victim of a scam, and I don't underestimate the impact this has had - both financially but also on her mental health and wellbeing. But while I accept Mrs P has lost a lot of money due to the deception of scammers, I must consider whether Revolut is responsible for the loss she has suffered. I haven't made my decision lightly. But while I know this won't be the outcome Mrs P is hoping for, for similar reasons as our Investigator, I don't think they are. So, I don't think Revolut has acted unfairly by not refunding Mrs P. I'll explain why.

Before I do, I want to reassure Mrs P that I've considered everything she has submitted in support of her complaint. And so, while I've summarised this complaint in far less detail than what has been provided, I want to stress that no discourtesy is intended by this. If there is a submission I've not addressed, it isn't because I have ignored the point. It's simply because my findings focus on what I consider to be the central issue in this complaint – that being whether Revolut are responsible for any loss Mrs P suffered because of the scam.

Mrs P has referenced the CRM code. This voluntary code, which Revolut wasn't signed up to, was replaced by the Authorised Push Payment (APP) Fraud Reimbursement Scheme that came into effect in October 2024. Nevertheless, this scheme doesn't cover the transactions Mrs P is disputing here – as it only covers payments made by Faster Payment or CHAPS sent to an account that isn't in the person's own control. And in this case, Mrs P was exchanging fiat currency to crypto with her Revolut account before forwarding it to the scam as crypto withdrawals (and so, not a Faster Payment or CHAPS). I've therefore considered whether it would otherwise be fair and reasonable to hold Revolut responsible for Mrs P's loss.

In broad terms, the starting position in law is that an electronic money institution (EMI) is expected to process payments that their customer authorises them to make. It isn't disputed that Mrs P knowingly made the payments on her account and so, I'm satisfied she authorised them. Therefore, under the Payment Services Regulations 2017 and the terms of her account, Revolut are expected to process Mrs P's payments, and she is 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 to have been good industry practice at the time, I consider it fair and reasonable 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 their customers were at risk of fraud. 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 their products, including the contractual terms, enabled them 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 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.

At which point, I'm aware that Revolut has argued that this complaint isn't within our jurisdiction – as crypto withdrawals aren't a regulated activity, nor can the exchange of fiat currency to crypto be considered as an ancillary service to payment services in situations whereby the ultimate asset the customer receives is an unregulated crypto asset. I've given careful thought to Revolut's points on this. Having done so, I don't agree. I accept crypto withdrawals aren't a regulated activity which means I cannot consider them in isolation. But I agree with our Investigator that the exchange of fiat money to crypto, which although not a regulated activity, is one which our service would consider ancillary to payment services. This is in the same way we consider exchanging GBP into foreign currency an ancillary activity. And I'm not persuaded that the ultimate asset being an unregulated crypto asset changes that. Therefore, given the nature of Mrs P's complaint, I'm satisfied that I can consider whether Revolut did what they should have, in relation to her funds and account, when she used Revolut to exchange her fiat money to crypto. And if not, whether this caused Mrs P to suffer her loss.

So, the starting point here is whether the instructions given by Mrs P to Revolut (either individually or collectively) were unusual enough to have expected additional checks to be carried out before the transactions were processed.

When considering this, I've kept in mind that EMIs process high volumes of transactions each day. And that there is a balance for Revolut to find between allowing customers to be able to use their account and questioning transactions to confirm they're legitimate – as it wouldn't be practical for EMIs to carry out additional checks before processing every transaction.

Mrs P's account was opened in November 2024, several months prior to the disputed transactions. And during this time, Mrs P's account was typically used for low value day-to-day transactions – and not crypto purposes. But while the crypto activity that started in February 2025 might have been new for Mrs P's account, I must take into consideration that many Revolut customers use their services for legitimate crypto purposes. So, I don't think this alone would've given Revolut enough reason to suspect Mrs P could be at significant risk of financial harm from fraud. Nor do I think the value of the first 15 crypto exchange transactions (ranging between £20 and £1,500), or the payment pattern surrounding them, was so unusual or suspicious whereby I would've reasonably expected Revolut to have been concerned – thereby prompting additional checks to be carried out before processing them.

This however, in my view, changed at the point of the 16th crypto exchange transaction. This is because, while this type of activity may have been somewhat normalised on Mrs P's account by this point, the value (£3,475) was significantly greater than the prior crypto activity. And knowing the risks associated with crypto, I think Revolut ought to have had enough reason to suspect Mrs P was potentially falling victim to a scam at this point. I therefore would've expected Revolut to have carried out additional checks before processing this payment.

I've therefore considered what type of intervention would've been proportionate to the risk the transaction presented. And what would've likely happened if Revolut had done this. When doing so, I've taken into account that Revolut did carry out some additional checks before processing 11 of the crypto withdrawal transactions (both prior to and after the 16th crypto exchange transaction).

As I've said, the majority of crypto transactions Revolut process will be for legitimate purposes and not associated with any kind of fraud. I've also 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.

The FCA's Consumer Duty, which was in force at the time these transactions were made, requires firms to act to deliver good outcomes for consumers including acting to avoid foreseeable harm. In practice this includes maintaining adequate systems to detect and prevent scams and to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers.

In light of the above, I think that by March 2025, when this transaction took place, Revolut should have had systems in place to identify, as far as possible, the actual scam that might be taking place and to provide tailored, effective warnings relevant to that scam. I accept that any such system relies on the accuracy of any information provided by the customer and cannot reasonably cover off every circumstance. But I consider that by March 2025, on identifying a heightened scam risk, a firm such as Revolut should have taken reasonable steps to attempt to identify the specific scam risk – for example by seeking further information about the nature of the payment to enable them to provide more tailored warnings.

In this case, Revolut knew that the transaction was to purchase crypto and their systems ought to have factored that information into the warning they gave. Revolut should also have been mindful that crypto scams have become increasingly varied over the past few years. Fraudsters have increasingly turned to crypto as their preferred way of receiving victim's money across a range of different scam types, including investment, impersonation and job scams.

Taking that into account, I am satisfied that, by March 2025, Revolut ought to have attempted to narrow down the potential risk further. I'm satisfied that when Mrs P made the payment, Revolut should – for example by asking a series of automated questions designed to narrow down the type of crypto related scam risk associated with the payment she was making – have provided a scam warning tailored to the likely crypto related scam Mrs P was at risk from. At which point, I should explain that while Mrs P has suggested otherwise, I'm not persuaded that the crypto activity on her account alone warranted intervention beyond automated questioning, such as a direct telephone conversation - as I don't think that would've been proportionate to the risk the transaction presented at that time.

In this case, Mrs P was falling victim to a 'job scam' – she believed she was making payments to receive an income. But even if Revolut had asked a series of simple questions to try and establish the risk the transaction presented, thereby allowing them to provide a warning tailored to it and the answers Mrs P gave, I'm not persuaded Revolut would've been able to identify Mrs P was making the transaction as part of a job scam.

This is because, when Revolut did carry additional checks before processing 11 of the crypto withdrawals, Mrs P didn't provide accurate responses. Nor did warnings that were relevant to her situation resonate with her. For example, Mrs P confirmed:

- She was making the transactions for investment purposes, and so not as part of a job. And as part of Revolut's questioning, she confirmed she'd come across the investment opportunity via a friend or family member.
- She understood that she had to answer Revolut's questions honestly, as she might not get her money back if she didn't. And if she was being scammed, fraudsters might ask her to hide the real reason for the payment.
- She was completing the transaction by herself. And so, she wasn't being pressurised to make the transaction or being told what to say – as, if she was, Revolut warned it may be a scam.

Revolut also provided warnings, albeit tailored to investment scams, that included:

- **Unsolicited contact**

  If someone contacts you out of the blue with an investment opportunity, especially if you've never interacted with them before, it's likely to be fake

- **Multiple money movements**

  Scammers ask for payment through untraceable means like gift cards, wire transfers, or cryptocurrency, making it hard to recover funds

- **'Too good to be true'**

  Offers that seem too good to be true often are. Trust your judgement

While Revolut's questioning and warnings happened at the point of the crypto withdrawals, I think Mrs P would've likely answered similarly if questioned about the 16th crypto exchange transaction. Consequently, I think Revolut wouldn't have become aware of the true purpose of the transaction or the circumstances surrounding it. And I likewise consider Mrs P would've ignored any warnings, similar to those listed above, that while tailored to investment scams were somewhat relevant to her situation.

I appreciate Mrs P was being coached by the scammer on how to respond to Revolut's questions. I sympathise with Mrs P as I understand, due to her personal circumstances, that she was in a vulnerable state at the time – which is why she placed trust in the what the scammer was telling her. But while Revolut should be on the lookout for vulnerabilities with their customers, and how this could increase their risk of falling victim to a scam, I don't think Revolut would've had enough reason to suspect that in these circumstances. This is because I don’t think the crypto activity was unusual or suspicious enough, nor do I think the responses Mrs P would’ve provided to questioning about the crypto exchange transaction would’ve alerted them to this fact either (as I don’t think it would’ve put them on notice she wasn’t answering them honestly). Sadly, I think the scammer’s influence on Mrs P would’ve led to Revolut considering Mrs P was making the transaction(s) for legitimate purposes. So, while I appreciate Mrs P is an innocent victim here, I don’t think I can fairly hold Revolut responsible for the inaccurate responses she provided. Nor do I think Revolut’s failure to question Mrs P about the 16th crypto exchange transaction led to the scam not being uncovered.

It follows that I don’t think Revolut could reasonably have prevented Mrs P’s loss.

Recovery of funds

Crypto withdrawals aren’t a regulated activity and so, it isn’t something I can consider. That said, the irreversible nature of crypto transactions meant there was no method of recovery here.

I appreciate Mrs P will be disappointed by this outcome. I realise the scam has had a huge impact on her. But it would only be fair for me to direct Revolut to refund her loss if I thought they were responsible. And so, while I’m pleased Mrs P did receive a refund from H in respect of a separate scam, I can only look at the actions of Revolut here. And for the above reasons, I don’t think Revolut is responsible for Mrs P’s loss. I therefore think Revolut have acted fairly and so I’m not going to tell them to do anything further.

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 Mrs P to accept or reject my decision before 9 February 2026.

Daniel O'Dell
Ombudsman