DRN-5357690

The complaint

Mr G complains that Revolut Ltd won't refund the money he lost when he fell victim to a scam.

What happened

Mr G says that he saw a news article on a social media site about a local girl whose life had been changed by investing with a company I'll refer to as N in my decision. The article said that a substantial profit could be earned by investing as little as $250. Mr G clicked a link in the article and was taken to N's website, where he left his contact details. Soon after, Mr G was contacted by a representative of N, who I'll call S. S told Mr G that she would be his broker. She explained that they would trade in oil, gas, and gold.

S helped Mr G to set up an account on N's trading platform, where he was able to see live trades. Mr G made an initial investment of $250 from an external account and could see the credit on N's platform. S also helped Mr G to open a cryptocurrency account as he was told he would be sending money through cryptocurrency as it was faster.

Mr G says he was advised that he needed to invest more to keep his account afloat and to do so he should open a Revolut account. He opened an account with Revolut on 4 September 2023, and exchanged £520 to USD and sent cryptocurrency to the scammer on 28 September 2023 so that his account could earn profits again.

Mr G wanted to withdraw his funds. He was put in touch with someone from N's finance team who told him that as some days had passed since he last traded his account was dormant and he needed to trade more. Mr G invested £5,000 and was earning a profit of £500 a day.

Mr G was offered a new investment opportunity in Bitcoin. He was interested but didn't have further funds to invest. N's representative asked Mr G to download a screen sharing application so that he could help him to get a loan. Mr G then transferred £19,000 to his cryptocurrency wallet on 11 November 2023.

For clarity, I have set out in the table below the payments Mr G made.

Transaction	Date	Amount	Notes
1	28/09/23	£520	Exchanged to USD then BTC then withdrawn
2	06/11/23	£5,000	
3	10/11/23	£19,000	
Total		**£24,000 plus BTC withdrawn**	

When he had profits of £50,000 Mr G wanted to withdraw his funds. He was told the finance team had authorised the withdrawal and the funds should appear in his cryptocurrency account. Mr G then received an email that appeared to come from a cryptocurrency provider

which said his wallet address had been flagged for possible money laundering. He was required to make a large payment as proof of wealth. Mr G says he questioned this with a representative of N and was told that if he didn't pay the amount requested, he would be arrested. Mr G realised he was the victim of a scam and reported what had happened to Revolut via its in-app chat on 13 November 2023.

Revolut didn't agree to reimburse Mr G. It said it provided sufficient scam warnings and did everything it could to recover Mr G's funds.

Mr G was unhappy with Revolut's response and brought a complaint to this service. He said that Revolut failed to protect him when he made the payments.

Our investigation so far

The investigator who considered this complaint recommended that it be upheld in part. She said that Revolut should reimburse 50% of payment two and subsequent payments, plus interest. This was because Revolut should have identified that payment two carried an increased risk of financial harm and that it was going to a cryptocurrency provider. Given these factors, the investigator said Revolut should have taken steps to narrow down the likely scam risk and provide a warning tailored to this risk. Had it done so, the scam would likely have been uncovered and Mr G's further loss prevented, particularly as Mr G had doubts at this stage.

But the investigator felt that Mr G should share responsibility for his loss.

Revolut didn't agree with the investigator's findings, so Mr G's complaint was passed to me to decide. In summary, it said:

- The payments Mr G made were "Self-to-Self", so there is no Authorised Push Payment (APP) fraud as defined in DISP rules. The transfers also don't meet the Contingent Reimbursement Model Code (CRM Code) definition of APP fraud or the definition in the PSR mandatory reimbursement scheme. The fraudulent activity didn't occur on Revolut's platform.
- Revolut accounts are not usually used as current accounts but to facilitate payments for a specific purpose. The transactions Mr G made weren't unusual or out of character for an electronic money institution (EMI) account.
- This service's reliance on R (on the application of Portal Financial Services LLP) v FOS is misconceived.
- It is relevant to consider possible other bank intervention or warnings as funds came from Mr G's external bank account.
- It may be relevant for this service to exercise its power to inform Mr G that it may be appropriate to make a complaint against another respondent.

I intended not to uphold Mr G's complaint so issued a provisional decision on 10 February 2025. In the 'What I've provisionally decided – and why' section of my provisional decision I said:

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.

Revolut raised some issues about jurisdiction in respect of the first cryptocurrency withdrawal Mr G made in September 2023. The investigator responded to the points made

and explained why we can consider this transaction. I don't propose to cover this aspect in detail, except to say I agree with the investigator, as Revolut didn't raise any concerns in response to the view and I don't propose to ask Revolut to reimburse this transaction.

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 at the time the payments were made 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 – (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.*

Should Revolut have recognised that Mr G was at risk of financial harm from fraud?

It isn't in dispute that Mr G has fallen victim to a cruel scam here, nor that he authorised the payments he made by transfers to his cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer).

Whilst I have set out in detail in this decision the circumstances which led Mr G to make the payments using his Revolut account, and the process by which that money ultimately fell into the hands of the fraudster, I am mindful that, at that time, Revolut had much less information available to it upon which to discern whether any of the payments presented an increased risk that Mr G might be the victim of a scam.

But, when these payments were made, firms like Revolut had been aware of the risk of multi-stage scams involving cryptocurrency for some time. Scams involving cryptocurrency have increased over time. The FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018 and figures published by the latter show that losses suffered to cryptocurrency scams have continued to increase since. They reached record levels in 2022. During that time, cryptocurrency was typically allowed to be purchased through many high street banks with few restrictions.

I recognise that, as a result of the actions of other payment service providers, many customers who wish to purchase cryptocurrency for legitimate purposes will be more likely to use the services of an EMI, such as Revolut. And I'm also mindful that a significant majority of cryptocurrency purchases made using a Revolut account will be legitimate and not related to any kind of fraud. However, our service has also seen numerous examples of consumers

being directed by fraudsters to use Revolut accounts in order to facilitate the movement of the victim's money from their high street bank account to a cryptocurrency provider, a fact that Revolut is aware of.

So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Mr G made, 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.

In those circumstances, as a matter of what I consider to have been fair and reasonable and good practice, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments. The introduction of the FCA's Consumer Duty, on 31 July 2023, further supports this view. The Consumer Duty requires Revolut to avoid causing foreseeable harm to its customers by, among other things, having adequate systems in place to detect and prevent scams.

Taking all of the above into account, and in light of the increase in multi-stage fraud, particularly involving cryptocurrency, I don't think that the fact most of the payments in this case were going to an account held in Mr G's own name should have led Revolut to believe there wasn't a risk of fraud.

I've gone onto consider, taking into account what Revolut knew about the payments, at what point, if any, it ought to have identified that Mr G might be at a heightened risk of fraud.

Mr G opened his Revolut account on 4 September 2023, so Revolut didn't have any information about his usual account activity.

I don't think Revolut had any reason to be concerned when Mr G made a cryptocurrency withdrawal in September 2023. It was relatively low in value and was in line with the account opening reasons Mr G gave to Revolut. Many Revolut customers use their accounts to buy cryptocurrency legitimately and Revolut needs to strike a balance between protecting its customers and minimising disruption to legitimate payment journeys.

But I'm satisfied that when Mr G made the £5,000 payment on 6 November 2023 Revolut should have identified that it carried a heightened risk of financial harm and should have taken additional steps before allowing it to debit Mr G's account. The payment was identifiably for cryptocurrency and was for a relatively large amount.

What did Revolut do to warn consumer?

Revolut says that when each new payee was set up it provided Mr G with the following warning:

"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. Remember, fraudsters can impersonate others and we will never ask you to make a payment."

This warning is very general in nature and it's difficult to see how it would resonate with Mr G.

Revolut also held the second payment Mr G made (of £5,000 on 6 November 2023). It provided Mr G with a screen which explained that something didn't look right, and the payment had been flagged as a potential scam. Revolut went on to explain that it needed to ask Mr G some questions which he needed to answer truthfully. Mr G was asked if anyone was prompting or guiding him. After confirming they weren't, Revolut asked Mr G to choose a reason for the payment from a list provided. Although there was an option to choose 'Investment', Mr G chose 'Something else' and was asked a series of questions as follows:

- *Were you told which option to select?*

- *Were you told your account isn't safe?*
- *Have you been asked to install software?*
- *Have you been told to ignore these answers?*

Mr G gave a negative answer to each of these questions. He was then provided with a series of educational screens which covered that it could be a scam, not to give remote access, to be wary of unexpected calls or being told that your account isn't safe, and advice to never ignore Revolut's warning. The payment was then processed.

What kind of warning should Revolut have provided?

I've thought carefully about what a proportionate warning in light of the risk presented would be in these circumstances. In doing so, 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.

The FCA's Consumer Duty, which was in force at the time these payments 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.

I'm mindful that firms like Revolut have had warnings in place for some time. It, along with other firms, has developed those warnings to recognise both the importance of identifying the specific scam risk in a payment journey and of ensuring that consumers interact with the warning.

In light of the above, I think that when these payments 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 for APP.

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 a firm should, by November 2023, on identifying a heightened scam risk, 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 it to provide more tailored warnings.

In this case, Revolut knew that payment two was being made to a cryptocurrency provider and its systems ought to have factored that information into the warning it gave. Revolut should also 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 a victim's money across a range of different scam types, including 'romance', impersonation and investment scams.

I am satisfied that, by November 2023 Revolut ought, fairly and reasonably, to have attempted to narrow down the potential risk further. I'm satisfied that when Mr G made payment two, 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 he was making – have provided a scam warning tailored to the likely cryptocurrency related scam Mr G was at risk from.

I recognise that Mr G told Revolut he was buying goods and services. But Mr G was paying a cryptocurrency provider, so I think that irrespective of the payment reason chosen Revolut ought fairly and reasonably to have recognised the risk posed by such a payment and taken steps to identify the actual scam risk.

In this case Mr G was falling victim to an investment scam. As such, I'd have expected Revolut to have asked a series of simple questions 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 Mr G gave.

The warning Revolut ought fairly and reasonably to have provided should have highlighted, in clear and understandable terms, the key features of common cryptocurrency investment scams, for example referring to: an advertisement on social media, promoted by a celebrity or public figure; an 'account manager', 'broker' or 'trader' acting on their behalf; the use of remote access software and a small initial deposit which quickly increases in value.

If Revolut had provided a warning of the type described, would that have prevented the losses Mr G suffered from payment two?

After carefully considering the evidence, I'm not persuaded that a warning of the type I've described would have prevented Mr G's loss.

This service has obtained evidence from Mr G's bank, including recordings of two telephone calls (on 4 October 2023 and 10 November 2023) when Mr G transferred funds from his bank account to his Revolut account.

When Mr G spoke to his bank on 4 October 2023, he wished to transfer a £10,000 loan he had received from an external provider, which was credited to his bank account, to Revolut. He said the payment was for an investment, that he was dealing with a broker, the company had a website and he had access to a platform. He was asked if anyone had asked him to install remote software and said they hadn't. Mr G was also asked if he had been able to withdraw funds. He confirmed that he hadn't.

The adviser Mr G spoke to explained that he wasn't concerned about Mr G's funds crediting his Revolut account, but about what happened to them after that. He explained that the bank had seen a lot of investments involving brokers where customers don't get what they wanted and referred Mr G to the bank's online investment scam advice. Mr G was also told that lots of people start with small amounts and it's when they make larger payments that they have problems, and to make sure he could withdraw funds.

The £10,000 that was transferred from Mr G's bank account to Revolut was returned and Mr G says that he paid off the loan company.

On 10 November 2023 Mr G called his bank about a transfer of £17,000 to his Revolut account. Mr G said he had got a loan through his bank for home improvements including work on the roof and buying things for the house. He explained he was moving funds to Revolut because of the benefits it offered.

During this call, the adviser from Mr G's bank explained that the bank was seeing lots of investment scams through social media where people were coerced into opening another account for the purposes of the investment. The adviser went on to say that scammers will ask victims to download remote access software. Mr G was specifically asked if anyone had asked him to send the money for any other reason than the one given (home improvements) or asked him to lie to his bank. Mr G replied, "Nope, all good".

The adviser Mr G spoke to expressed concern about remote access detected on his phone that hadn't been seen before. Mr G explained that the remote access applications related to his work and, when asked, said nobody had asked him to download them.

The point at which I consider Revolut should have provided a written warning tailored to cryptocurrency investment scams was shortly before the call on 10 November, on 6 November. At this stage Mr G misled Revolut about the reason for the payment and didn't accurately answer all its questions.

After carefully considering the evidence, I'm not satisfied that a written warning tailored to cryptocurrency investment scams on 6 November 2023 would have resonated with Mr G and prevented his loss. His bank had already expressed concern and referred Mr G to investment scam advice which he hadn't heeded. Very shortly afterwards, when Mr G was

given all the information I think Revolut should have provided in a written warning, (an investment on social media, a broker acting on his behalf, the use of remote access software, and returns) he still went ahead and made a £19,000 payment on the same day as the call. In the circumstances, I can't fairly conclude that further intervention by Revolut would have made a difference in this case and prevented Mr G from making payment two.

It's arguable that Revolut should have done more when Mr G made payment three and asked Mr G questions in the chat. But, given the available evidence, I'm still not persuaded Mr G's loss would have been prevented. While his funds were clearly going to a provider of cryptocurrency, so Mr G couldn't say he was paying for home improvements, I don't think he would have answered Revolut's questions accurately. On the same day, he misled his bank and I think Mr G would have been coached to do the same thing. He may have revealed that he was investing, but not that someone was helping him.

I realise how disappointing my provisional decision will be and the substantial impact of this cruel scam. But, overall, I can't fairly ask Revolut to reimburse Mr G.

Revolut didn't respond to my provisional decision. Mr G, through his representative, let me know that he didn't agree and asked me to consider the following points:

- My provisional decision acknowledges that Revolut should have provided more specific and tailored warnings about cryptocurrency investment scams. Had it done so, Mr G would have had a better understanding of the risks involved and may have reconsidered.
- He was vulnerable as a result of lack of financial expertise, which should be taken into account when assessing his responses to warnings and interventions.
- Revolut has a duty to protect its customers from foreseeable harm.
- Revolut was in a unique position to provide targeted warnings at the time of the transaction which could have had greater impact than more general advice from the bank.
- Revolut's failures significantly contributed to the outcome so it should share responsibility for his loss.

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 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.

I have carefully considered Mr G's response but am not persuaded to reach a different outcome. For the reasons I set out in my provisional decision (and reproduced above) I can't fairly ask Revolut to reimburse any of Mr G's loss.

Mr G has referred to Revolut's duties at the time he made the payments. I covered this aspect in detail in my provisional decision and acknowledged that Revolut should have done more to protect Mr G. So I don't see any merit in discussing this area any further.

I can't uphold Mr G's complaint solely on the basis that Revolut's intervention didn't go far enough. I need to go on to consider causation – whether suitable intervention would have made a difference to Mr G's decision making or Revolut could have reasonably prevented the loss. In deciding this, I need to consider the evidence that was available at the time the payments were made.

Mr G said in response to my provisional decision that had Revolut provided more specific warnings he "*may have reconsidered proceeding with the transactions*". But I'm required to reach a decision based on what is more likely than not to have happened, rather than what may have happened.

Mr G's bank went further than providing a tailored on-screen warning and spoke to him about transfers to his Revolut account. In the first call, shortly before the transfer of £5,000 on 6 November 2023, Mr G was honest about what he was doing. He was given scam advice and referred to online investment scam advice. After this, Mr G was clearly persuaded to mislead his bank to ensure the transfer to Revolut was processed. Even though Mr G said the transfer was for home improvements, his bank provided him with advice about investment scams through social media, being coerced into opening another account for the purpose of the investment, and remote access software. These factors were present, but the verbal warnings provided to Mr G didn't resonate or break the spell. And I don't agree with Mr G that the warnings provided by his bank were general in nature.

I recognise Mr G wasn't a financial expert and that he was under the spell of cruel scammers. But in this case the available evidence doesn't lead me to conclude that different intervention by Revolut would have made a difference or prevented Mr G's loss.

Overall, whilst I'm very sorry to hear about this scam and the impact it has had on Mr G, I can't fairly ask Revolut to reimburse him.

My final decision

For the reasons stated, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr G to accept or reject my decision before 26 March 2025.

Jay Hadfield
Ombudsman