DRN-5054689

The complaint

Mr G is unhappy that Revolut Ltd didn't refund payments he made as part of a scam.

Mr G is professionally represented in the complaint, but for simplicity I've only referred to the actions of Mr G throughout.

What happened

In early 2023 Mr G received a call from someone he didn't know, who turned out to be a scammer. They began to talk via an instant messaging service and got to know each other. Eventually the conversation turned to passive income and an investment opportunity the scammer was earning from, involving cryptocurrency. It was positioned as an 'internal project' with a real European bank, I'll call "R" – where you deposited funds like a traditional savings account, but R paid would pay 1.3% compound interest per day.

Having seen a demonstration of the platform, and finding the scammer to be genuine and friendly, Mr G decided to invest. He was instructed by the scammer to purchase cryptocurrency, which he initially did by making payments from his main account, at a bank I'll call "H", to an exchange I'll call "C". Mr G started with smaller amounts but as they began to increase H blocked them. So instead he switched to sending the funds from H to his Revolut account, which he hadn't used since opening it the year before, and began making payments to different cryptocurrency exchanges.

Mr G tried twice to make a payment for £12,500 to one cryptocurrency exchange from his Revolut account, but those attempts were blocked. Revolut directed Mr G to the in-app chat function to answer some questions, but before it could ask about the transfers he told Revolut to cancel them, which it did. Mr G then tried to purchase a smaller amount of cryptocurrency (£5,000) using his card, at a different exchange I'll call "B". Revolut asked him for the purpose of the payment, and he selected 'transfer to a safe account'. Revolut subsequently allowed the transaction to go through after showing a warning related to 'safe account' scams. Mr G then sent the cryptocurrency onto the fake project platform from his wallet with B.

The trading platform showed Mr G was making large profits on his investment, and so was encouraged to send increasing amounts. He made a total of 13 card payments totalling more than £52,000 over the next six weeks as part of the scam. The disputed transactions are set out below – and the dates and times shown are when Mr G put through the payment, going by the system data (rather than when it completed).

Payment	Date	Time	Type/payee	Amount
1	23 May 2023	17.26	Card payment to B	£5,000
2	24 May 2023	11.11	Card payment to B	£5,000
3	24 May 2023	11.23	Card payment to B	£2,500

4	24 May 2023	11.52	Card payment to B	£100
5	31 May 2023	16.10	Card payment to B	£4,220
6	2 June 2023	12.24	Card payment to B	£5,000
7	2 June 2023	12.26	Card payment to B	£3,400
8	6 June 2023	23.11	Card payment to B	£4,200
9	18 June 2023	18.23	Card payment to B	£4,075
10	30 June 2023	18.32	Card payment to B	£4,125
11	5 July 2023	15.17	Card payment to B	£5,000
12	5 July 2023	15.36	Card payment to B	£5,000
13	5 July 2023	15.39	Card payment to B	£4,800
		Total		£52,420

At a certain point Mr G was told he'd need to pay a fine for going against the rules of the project, and both his and the scammer's accounts were frozen. He was warned his account would be closed unless he could pay to "restore the project's liquidity". So Mr G applied for a £15,000 loan with a bank at the end of May 2023, to continue funding the investment. He was later hit with an 'operational maintenance fee' of £23,000 – and so he asked his wife to apply for loan too. Mr G also borrowed from their business account as well as friends to secure funds needed for the various charges requested.

Eventually B warned Mr G that the wallet he was sending cryptocurrency to was linked to a scam, which he queried with the scammers and was given a new wallet ID that he continued to send funds to. After making the payments on 5 July 2023 the scammers told Mr G there was an 'imbalance in the wallet' that needed correcting before payment of his profits could be made. He checked that requirement with one of the cryptocurrency exchanges (C), who advised that wasn't a real thing – and he was likely dealing with scammers. Mr G queried what C had told him with the scammers, but ultimately didn't send any more money to them.

Mr G reported the fraud to Revolut in August 2023. Revolut attempted recovery via chargeback, as all the transactions were debit card payments. But those were unsuccessful because the payments were authorised, and Mr G had received what he'd paid for from B (but had just sent the cryptocurrency purchased onto a scammer). So Mr G complained about the outcome through a professional representative. He argued that if there had been an impactful intervention from Revolut, and it had spoken to him to provide warnings, he wouldn't have gone through with the payments.

Revolut's final response to the complaint said it didn't think it was liable to refund the transactions as there were no chargeback rights under the card scheme rules. So, because the transactions were authorised, it believed it had considered the fraud claim fairly. Unhappy with the response, Mr G referred the complaint to our service for review.

One of investigators considered everything and recommended the complaint be upheld in part. In his view, Revolut ought to have done more after it recognised the first card payment of £5,000 presented a scam risk. It was a large payment going to a cryptocurrency provider, after a year of inactivity on the account. Mr G had also told Revolut he was falling for a 'safe account' scam via the automated questions it asked. So, the investigator thought Revolut should have spoken to Mr G about the payment, via its chat function, before allowing it – and had that happened the scam would have been uncovered. The investigator felt Mr G should

share responsibility for the loss, though, as several red flags that the opportunity might not be legitimate had been missed.

Mr G accepted the investigator's recommendation, but Revolut did not. It said (among other things) that Mr G had provided inaccurate information about the purpose of the initial declined payments, so it felt he would likely have done the same if it had queried the payments to B. So the true circumstances involved wouldn't have come to light. The investigator's opinion remained the same, so the complaint was passed to me (an ombudsman) for a final decision on the matter.

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.

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 its 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 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;
- 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.

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

Revolut did recognise Mr G was at risk of financial harm prior to processing the first payment, for £5,000 on 23 May 2023, and intervened to ask automated questions. It provided a warning based on Mr G's answers, but I don't think that was proportionate in the circumstances. There were lots of concerning factors present by the time Mr G attempted the £5,000 payment in question. Revolut had intended to speak to him about a far larger payment being attempted twice to a different cryptocurrency exchange, for £12,500. But it didn't question him further after he cancelled the transfers. Then two separate conversation threads were started, where both discussed unblocking the account at some length. Mr G appeared desperate to get it operational again, and gave conflicting answers around why.

He initially told Revolut he was travelling in Europe and urgently needed to use his card abroad, which already sounds incongruous in the context of the very large cryptocurrency transactions that had caused the account to be blocked. Mr G then says to the agent in the same conversation on the same day, sitting in the same chair (going by the various selfies he sent) that the local time here in the UK is 9.34pm.

Mr G then tried to send £5,000 through B, as he thought the account had been unblocked, but that was also declined. So he continued to message the chat threads with Revolut to sort out the block on his account. As soon as the blocks were lifted Mr G tried the £5,000 payment to B again – and by that point Revolut ought to have been concerned about what was going on. He'd given incorrect information about what he was using the account for, he'd tried to put through several large transactions, of different sizes, to different cryptocurrency exchanges, and then cancelled them – all seemingly to try and circumvent the firm's fraud controls and avoid speaking to Revolut. It does ask Mr G some automated questions about payment 1, but those answers ought to have increased Revolut's concerns. Mr G essentially said he was falling for a safe account scam. So Revolut ought to have spoken to him prior to allowing the transaction – and, given all of the above factors, the bar for satisfying Revolut that was he was doing was legitimate would have been high.

Mr G misled the originating bank, H, about what he was doing – but ultimately it added so much friction to the process of sending money to cryptocurrency that he gave up, and switched to Revolut. He also misled the bank about the transactions to Revolut from H, but that lie wouldn't have been available to him if he'd spoken to Revolut (sending money abroad to support a sick family member). Mr G is adamant he'd have been honest with Revolut if it had questioned him about the payments, as he believed it was 'crypto-friendly' compared with his bank. I'm not so sure, as he'd already begun to evade Revolut's controls as far as I can tell – and it had put in place just as much friction as his bank had for the initial cryptocurrency transactions.

But I don't think it matters. Revolut ought to have needed to see something to corroborate what he was doing, given how risky it looked. Even if all Revolut had asked to see was his wallet statement at B, to evidence he had control over it (to guard against him potentially falling for a safe account scam – as he'd indicated with his answers he might be) that would have shown he was sending on the cryptocurrency elsewhere. So once that was discovered then Revolut would have needed something to evidence where it was going or details of any investment. Mr G would have had to come clean at that point, or any lie he tried to tell would have unravelled with the need for supporting evidence – and his account would have remained blocked until Revolut was satisfied he wasn't at risk. The circumstances involved were so obviously indicative of a scam, that any details Mr G did share about the opportunity, and how he found it, would have alerted Revolut to what was happening. So I find that Revolut ought to have been able to prevent the loss in this case from the first payment, through a probing conversation with him.

Is it fair and reasonable for Revolut to be held responsible for Mr G's loss?

I have taken into account that Mr G remained in control of his money after making the payments from Revolut. It wasn't lost until he took further steps. But Revolut should still have recognised that Mr G was at risk of financial harm from fraud, made further enquiries about the first payment in the table, and ultimately prevented Mr G's loss from that point. So I think Revolut can fairly be held responsible for Mr G's loss in such circumstances. Our service also looked at a complaint about H, where the funds originated, and the investigator's view was that it wasn't at fault in what happened. That opinion was accepted by Mr G. But I have factored in the evidence from that case when deciding this one though. As I've decided

Revolut should have been able to prevent the loss, I think it can't fairly be held responsible – subject to a consideration of Mr G's responsibility in matters.

Should M G bear any responsibility for his losses?

I've thought about whether Mr G should bear any responsibility for his 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. That includes taking into account Mr G's own actions and responsibility for the losses he has suffered.

I recognise that there were sophisticated aspects to this scam, including a platform that looked very professional. I've no doubt the scammer's friendly demeanour lured Mr G in. R was also a real bank, and cloning that legitimate firm, with its genuine online presence, probably added to the air authenticity. I don't want to underestimate the level of social engineering involved here either – as these scammers will have been experts at extorting people, and persuading them to take risks they never usually would. But I've also found there were clear warnings signs that this wasn't a legitimate opportunity, that I think Mr G either missed or didn't pay sufficient attention to.

Mr G understandably had lots of questions about the opportunity when it was first explained, and was keen to see some documentation about it. But I don't think any of his questions were really answered by the scammer, except to say it was an internal project which is why there wasn't more public information about it. I don't think it was reasonable to commit such large amounts to an investment so quickly without understanding the mechanics of it, or why such an unrealistic level of interest was being offered. Particularly given the scammer had cold called him, and then almost immediately began discussing a seemingly covert opportunity – that should have struck Mr G as odd at best.

It also wasn't clear how the scammer was able to get involved in such a lucrative venture – and she oscillated between saying her sister introduced and trained her, to shortly afterwards saying her uncle was the one that got her involved. I think the vagueness of the offering and the inconsistencies in the back story ought to have been a red flag. Mr G quite rightly has doubts, and even asks (somewhat jokingly) is this a scam, but unfortunately doesn't follow through on those instincts. Mr G does seem to look up R, and found the website for the genuine bank, but doesn't question why the branding was very different on the platform shown to him by the scammer.

Mr G does spot other red flags – and questions the scammers around why the project is seemingly holding more than the globally circulating amount of USDT (a cryptocurrency). He also queried why profits were paid according to UK time, when it's supposedly an Austrian company – and why the agents' phone numbers appear to be US based ones. But Mr G doesn't get, to my mind, satisfactory explanations to any of those questions, and continues to invest.

I think the biggest warning signs came later, and the multiple requests for fees or fines – which seem to strike Mr G as both unfair and unexplained. He also had to take out loans to cover those costs, and putting himself in such a financially precarious position, for dubious reasons, ought to have caused him to pause. Finally, being warned by B that the wallet he was sending cryptocurrency to was linked to scams, and then continuing to send money after that, wasn't reasonable. I appreciate the scammer had an explanation for B's warning – but given the other alarms that ought to have sounding loudly by that point, I think ignoring B's advice amounts to negligence on his part.

For the reasons I've given, I've decided Mr G should fairly contribute to the overall loss, from payment 1 onwards (same as Revolut), as he ought to realised it might not be a legitimate

investment opportunity from the start. So I'm applying a 50% reduction to the total refund due, meaning Revolut and Mr G both equally share responsibility for the loss.

I don't think the deduction made to the amount reimbursed to Mr G should be greater than 50% taking into account all the circumstances of this case. I recognise that Mr G did have a role to play in what happened, and it could be argued that he should have had greater awareness than he did that there may be something suspicious about the opportunity. But I have to balance that against the role that Revolut, an EMI (at the time) subject to a range of regulatory and other standards, played in failing to intervene proportionately (or at all after the first payment). Just as Mr G's negligence increased as the scam went on, and the warnings signs stacked up, so did Revolut's liability – and it didn't carry out any further checks, despite a clearly escalating situation occurring on the account. I therefore think the parties had equal opportunity and responsibility for the preventing the loss. The mandatory reimbursement scheme rules aren't relevant to these transactions either – so 'gross negligence' isn't the standard to consider Mr G's actions against.

Mr G was taken in by a cruel scam – he was tricked into a course of action by a fraudster and his actions must be seen in that light. I don't think it would be fair to suggest that he is mostly to blame for what happened, taking into account Revolut's failure to recognise the risk that he was at financial harm from fraud, and given the extent to which I am satisfied that a business in Revolut's position should have been familiar with a fraud of this type. Overall, I remain satisfied that 50% is a fair deduction to the amount reimbursed in all the circumstances of the complaint.

I've thought about whether Revolut could have done more to recover the payments, and I'm satisfied it couldn't have. Mr G received what he purchased from B with the card payments (he just sent the cryptocurrency to the scammer), and so chargebacks wouldn't be successful on those. I also haven't seen any service issues that I consider would warrant a further award. Mr G was certainly given the runaround after his account was blocked, but given Mr G's own role in why it had been blocked, along with his own delays in responding to some of the messages, I don't think separate compensation is due for inconvenience. The interest applied to the redress will also fairly compensate Mr G for the time he was deprived of use of those funds – and I think that's sufficient in the circumstances.

Putting things right

Revolut should:

- refund 50% of all the disputed transactions (payments 1-13 in the table).
- apply 8% simple interest yearly to the above refunds (calculated from the date of the transactions to the date of settlement).

If Revolut considers that it's required by HM Revenue & Customs to deduct income tax from that interest, it should tell Mr G how much it's taken off. It should also give Mr G a tax deduction certificate if he asks for one, so he can reclaim the tax from HM Revenue & Customs if appropriate.

My final decision

I've decided to uphold Mr G's complaint about Revolut Ltd in part, and I direct it to settle the complaint as I've set out above (in the 'putting things right' section).

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr G to accept or reject my decision before 14 August 2025.

Ryan Miles
Ombudsman